MUNICÍPIO DE CAMPO BOM

ESTADO DO RIO GRANDE DO SUL - BRASIL

DIVISÃO DE LICITAÇÕES E CONTRATOS

RETIFICAÇÃO

REF.: PREGÃO ELETRONICO Nº 128/2022

OBJETO: Contratação de empresa especializada na prestação de serviços de instalação, configuração, manutenção, locação de equipamentos firewall (Appliance) e gerenciamento dos sistemas de segurança, para o Datacenter da Prefeitura Municipal de Campo Bom.

A Prefeitura Municipal de Campo Bom/RS torna público aos interessados que fica retificado o presente Edital, nos termos que seguem:

1) *Inclui-se o item 7.1.5.4 referente à capacidade técnica.*

Leia-se

> *"7.1.5.4 Comprovação de aptidão da empresa por meio de, no mínimo, 1 (um) atestado de capacidade técnica, comprovando serviços de Suporte, Atualização, Fornecimento do Next-Generation Firewall (NGFW) e de consultoria especializada."*

2) *Altera-se o item 1.1 do Anexo VII, Modelo de Proposta de Preços, do edital:*

leia-se:

ITEM	SUBITEM	DESCRIÇÃO	UNID	QTDE	VALOR UNIT.	VALOR TOTAL
01	1.1	Contrato de Firewall de Próxima Geração - Solução composta de 1 (um) appliance conforme termo de referência. Pacote de licenças da Console de Gerência Administrativa e Centralização de Logs e Relatórios. Pacote de licenças de Firewall, IPS, Anti-spyware, Filtro de Web, Proteção contra ameaças avançadas e firewall de aplicação web para appliance de Firewall de Próxima Geração Tipo 1 - (02 equipamentos)	MÊS	12		
	1.2	Instalação, configuração e treinamento profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento, Centralização e Monitoração de Logs Centralizado.	UN	01		
	1.3	Consultoria especializada. Banco de horas para execução de atividades especializadas de Segurança da Informação. Item 26 do Termo de Referência- Anexo I	HORA	10		

	TOTAL	

3) <u>Altera-se o Anexo I, Anexo I-A e Anexo I-B do edital</u>

Leia-se:

ANEXO I

PREGÃO ELETRÔNICO Nº 128/2022
TERMO DE REFERÊNCIA

FIREWALL

Contratação de empresa especializada na prestação de serviços de instalação, configuração, manutenção, locação de equipamentos firewall (Appliance) e gerenciamento dos sistemas de segurança, para o Datacenter da Prefeitura Municipal de Campo Bom.

1. OBJETOS:

1.1. Contratação de serviços técnicos especializados, sob demanda, com o objetivo de garantir a plena utilização da solução contratada, bem como sua instalação e adequação ao ambiente tecnológico da CONTRATANTE; ITEM 26 Banco de Horas, ANEXO I – Termo de Referência.

1.2. Locação de equipamentos firewall (Appliance) baseada em gerenciamento unificado de ameaças (UTM) com serviço de instalação, para proteção de todos os computadores, sistemas e redes instalados no Centro Administrativo, Secretarias e Órgãos Municipais. Além de possibilitar o gerenciamento centralizado de acessos à internet, proteção AntiSpam e antivírus, conforme itens abaixo e descritivo detalhado dos itens constante no Termos de referência do edital:

2. JUSTIFICATIVA:

2.1. A Prefeitura Municipal de Campo Bom possui um parque computacional de processamento de porte significativo, disponibilizando serviços de TI, na área administrativa, em servidores com médio grau de complexidade de manutenção.

2.2. O serviço a ser contratado requer profissionais habilitados e, até o momento, a Prefeitura Municipal de Campo Bom não possui quantitativo suficiente em seu quadro pessoal de técnicos especializados e certificados para a realização de alguns serviços críticos de suporte e manutenção do ambiente em questão.

2.3. Em razão da complexidade dos serviços necessários, propõe-se a contratação de serviço técnico especializado cuja equipe seja devidamente qualificada e certificada pelos órgãos competentes e/ou pelos próprios fabricantes, que possuem programas de capacitação e certificação específica para esses produtos, a fim de

possibilitar a restauração da operação normal dos serviços com o mínimo de impacto nos processos da Prefeitura Municipal de Campo Bom.

3. DO FUNDAMENTO LEGAL:

Os objetos aqui enunciados estão fundamentados nos seguintes dispositivos:

3.1. Lei 13.709 /2018

3.2. Lei 8.666 /1993

3.2.1. II, do art. 57, que possibilita a prorrogação de contratos de serviços contínuos por prazos de 48 (quarentas e oito meses), aplicando-a aos contratos de fornecimento, que via de regra se sujeitam ao crédito orçamentário, conforme prevê o caput do mesmo dispositivo.

3.3. Ao aluguel de equipamentos e à utilização de programas de informática, podendo a duração estender-se pelo prazo de até 48 (quarenta e oito) meses após o início da vigência do contrato.

3.4. Termo de referência- Anexo I e Termo de Vistoria – Anexo II

4. DA DOCUMENTAÇÃO RELATIVA À QUALIFICAÇÃO TÉCNICA

4.1. Comprovação, para o fornecimento de suporte e atualizações para estrutura a empresa responsável pela execução dos serviços deve possuir as seguintes certificações;

4.2. No mínimo 1 (um) técnicos Nível Engineer Next Generation Firewall

4.3. No mínimo 1 (um) técnicos Nível Architect Next Generation Firewall

4.4. No mínimo 01 (um) técnico com Certificação MCSA Windows Server 2008 ou superior.

4.5. No mínimo 1 (um) técnico com certificação LPI-2.

4.6. No mínimo 01 (um) DPO Data Protection Officer ou Encarregado de Dados.

4.7. Comprovação de aptidão da empresa por meio de, no mínimo, 1 (um) atestado de capacidade técnica, comprovando serviços de Suporte, Atualização, Fornecimento do Next-Generation Firewall (NGFW) e de consultoria especializada.

4.8. Comprovação de aptidão da empresa por meio de, no mínimo, 1 (um) atestado ou declaração pelo fabricante, para Suporte, Atualização e Fornecimento do Next-Generation Firewall (NGFW).

4.9. Comprovação de Localização em um raio máximo de 150 km (cento e cinquenta) quilômetros da sede do município de Campo Bom, ou declaração de que compromete a se instalar neste raio se declarado vencedor, no prazo de 60 dias.

4.10. Atestado de visita técnica emitido pela Divisão de informática do Município de Campo Bom, atestando que a licitante visitou o local onde serão executados os serviços, objeto desta licitação ou declaração da licitante de que tem pleno conhecimento acerca das estruturas e necessidade que poderão ser apresentadas, atendendo ao que solicita o anexo II – Termo de Vistoria.

5. DOS PRAZOS E DO RECEBIMENTO

5.1. O licitante vencedor se obriga a entregar o objeto (pag.1- itens 1.2) deste certame no prazo máximo de 45 (quarenta e cinco) dias, contados da assinatura do contrato.

5.2. A empresa vencedora deverá fazer a entrega do material Na Divisão de Informática de, localizado na Av. Independência, 800, Centro Administrativo, Bairro Centro, Campo Bom, sem ônus para o município.

5.3. O recebimento do material será de segunda a quinta-feira das 7h30min às 11h30min e das 13h às 17h30min.

5.4. A entrega do material deverá ser agendada pelo e-mail- informatica@campobom.rs.gov.br

5.5. Se dentro do prazo, o convocado não fizer a entrega, a Administração convocará os licitantes remanescentes, na ordem de classificação para execução do fornecimento em igual prazo e nas mesmas condições propostas pelo primeiro classificado.

ANEXO I -A

PREGÃO ELETRÔNICO Nº 128/2022
FIREWALL

1. CARACTERISTICAS GERAIS DA APPLIANCE:

1.1. Solução de segurança (APPLIANCE) baseada em gerenciamento unificado de ameaças (UTM):

1.2. O fabricante do software da appliance deverá estar enquadrado no quadrante mágico do Gartner na categoria Leader, Challengers, Niche Playes ou Visionaries no ano de 2018 ou 2019.

1.3. Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL, criptografia de e-mail, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em hardware específico ou virtualizado.

1.4. Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos novos, sem uso anterior.

1.5. Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.

1.6. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

1.7. Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.

1.8. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

2. CARACTERISTICAS DE HARDWARE:

2.1. Suportar no mínimo 140.000 (cento e quarenta mil) novas conexões por segundo;

2.2. Suportar no mínimo 6.500.000 (seis milhões e quinhentos mil) conexões simultâneas;

2.3. Performance mínima de 6.000 (seis mil) Mbps de performance de NGFW.

2.4. Possuir no mínimo 31.000 (trinta e um mil) de rendimento (throughput) do Firewall;

2.5. No mínimo 6.200 (seis mil e duzentos) Mbps de rendimento (throughput) do IPS;

2.6. Possuir no mínimo 13000 (treze mil) Mbps de throughput de VPN IPsec;

2.7. Suporte a, no mínimo, 1700 túneis SSL VPN;

3. A solução proposta deve corresponder aos seguintes critérios de throughput em mundo real:

3.1. Entende-se como mundo real, testes realizados pelo fabricante que tenham sido feitos com o appliance utilizando até 50% da capacidade de processamento, utilizando um mix de protocolos usados no mundo corporativo.

3.2. Performance mínima de 6,2 Gbps de throughput de IPS.

3.3. Entende-se como mundo real, testes realizados utilizando ambientes e protocolos usados no mundo corporativo.

3.4. A solução proposta deve possuir licenças baseado nos recursos de hardware.

3.5. A solução proposta deve suportar a configuração de políticas baseadas em usuários para segurança e gerenciamento de internet.

3.6. A solução proposta deve fornecer os relatórios diretamente no Appliance, baseados em usuário, não só baseado em endereço IP.

3.7. A solução proposta deve possuir no mínimo 120 GB de espaço em disco SSD para o armazenamento de eventos e relatórios.

3.8. Possuir slot de FleXi Port

3.9. Possuir ao menos uma porta COM (RJ45).

3.10. Possuir painel de LCD na parte frontal do appliance com funcionalidades básicas para ajudar na gerência do equipamento.

3.11. Número irrestrito de usuários/IP conectados.

3.12. Appliance com 1 U para montagem em rack.

3.13. Possuir no mínimo 8GB de memória RAM.

3.14. Possuir no mínimo 8 (oito) interfaces de rede 1000Base-TX.

3.15. Possuir 1 (uma) interface do tipo console ou similar.

3.16. Possuir 1 (uma) fonte 100-240VAC.

4. PROTEÇÃO WEB

4.1. Filtragem e Segurança Web

4.2. Proporcionar transparência total de autenticação no proxy, provendo segurança anti- malware e filtragem web.

4.3. Possuir uma base de dados com mais de 1.000.000 (um milhão) de URLs reconhecidas e categorizadas agregadas a pelo menos 92 categorias oferecidas pela solução.

4.4. Realizar autenticação dos usuários nos modos transparente e padrão.

4.5. As autenticações devem ser feitas via NTLM.

4.6. Possuir sistema de quotas aplicado por usuários e grupos.

4.7. Permitir criar políticas por horário aplicado a usuários e grupos

4.8. Possuir sistema de malware scanning que realize as seguintes ações;

4.9. Bloquear toda forma de vírus

4.10. Bloquear malwares web

4.11. Prevenir infecção de malwares, trojans e spyware em tráfegos HTTPS, HTTP, FTP e e-mails baseados em acesso web (via navegador).

4.12. Proporcionar proteção de web malware avançado com emulação de Java script.

4.13. Prover proteção em tempo real de todos os acessos web.

4.14. A proteção em tempo real deve consultar constantemente a base de dados na nuvem do fabricante que deverá se manter atualizada prevenindo novas ameaças.

4.15. Prover pelo menos duas engines diferentes de anti-malware para auxiliar na detecção de ataques e ameaças realizadas durante os acessos web realizados pelos usuários.

4.16. Fornecer Pharming Protection.

4.17. Possuir pelo menos dois modos diferentes de escaneamento durante o acesso do usuário.

4.18. Permitir criação de regras customizadas baseadas em usuário e host.

4.19. Permitir criar exceções de URLs, usuários e host para que não sejam verificados pelo proxy.

4.20. Validação de certificado.

4.21. Prover cache de navegação, contribuindo na agilidade dos acessos à internet.

4.22. Realizar filtragem por tipo de arquivo, mime-type, extensão e tipo de conteúdo (exemplo: Activex, applets, cookies, etc.)

4.23. Integração com o youtube for schools.

4.24. Prover funcionalidade que força o uso das principais ferramentas de pesquisa segura (SafeSearch): Google, Bing e Yahoo.

4.25. Permitir alterar a mensagem de bloqueio apresentada pela solução para os usuários finais.

4.26. Permitir alterar a imagem de bloqueio que é apresentado para o usuário quando feito um acesso não permitido.

4.27. Permitir a customização da página HTML que apresenta as mensagens e alertas para os usuários finais.

4.28. Especificar um tamanho em Kbytes de arquivos que não devem ser escaneados pela proteção web.

4.29. Range aceitável de 1 a 25600KB.

4.30. Bloquear trafego que não segue os padrões do protocolo HTTP.

4.31. Permitir criar exceções de sites baseados em URL Regex, tanto para HTTP quanto para HTTPS.

4.32. Nas exceções, permitir definir operadores “AND” e “OR”.

4.33. Permitir definir nas exceções a opção de não realizar escaneamento HTTPS.

4.34. Permitir definir nas exceções a opção de não realizar escaneamento contra malware.

4.35. Permitir definir nas exceções a opção de não realizar escaneamento de critérios especificado por políticas.

4.36. Permitir criar regras de exceções por endereços IPs de origem.

4.37. Permitir criar regras de exceções por endereços IPs de destino

4.38. Permitir criar exceções por grupo de usuários.

4.39. Permitir criar exceções por categorias de sites.

4.40. Permitir a criação de agrupamento de categorias feitas pelo administrador do equipamento.

4.41. Ter grupos de categorias pré-configuradas na solução apresentando nomes sugestivos para tais agrupamentos, por exemplo: “Criminal Activities, Finance & Investing, Games and Gambling”, entre outras.

4.42. Permitir editar grupos de categorias preestabelecidos pela solução.

5. Deve ter sistema que permita a criação de novas categorias com as seguintes especificações:

5.1. Nome da regra;

5.2. Permitir criar uma descrição para identificação da regra.

6. Ter a possibilidade de classificação de pelo menos:

6.1. Produtivo;

6.2. Não produtivo;

6.3. Permitir aplicar Traffic shaping diretamente na categoria;

6.4. Na especificação das URLs e domínios que farão parte da regra, deve-se permitir cadastrar por domínio e palavra-chave;

6.5. Deve permitir importar uma base com domínios e palavras chaves na hora da criação da categoria, a base com informações de domínios e palavras chaves deverá aceitar pelo menos as seguintes extensões;

6.6. Permitir importar a base citada no item anterior de forma externa, ou seja, especificar uma URL externa que contenha as informações com a lista domínios que poderá ser mantida pelo administrador ou um terceiro.

6.7. Ter função para criar grupos de URLs.

6.8. A base de sites e categorias devem ser atualizadas automaticamente pelo fabricante.

6.9. Permitir o administrador possa especificar um certificado autoritário próprio para ser utilizado no escaneamento HTTPS.

6.10. Deve permitir que em uma mesma política sejam aplicadas ações diferentes de acordo com o usuário autenticado.

6.11. Nas configurações das políticas, deve-se existir pelo menos as opções de: Liberar categoria/URL, bloquear e alarmar o usuário quando feito acesso a uma categoria não desejada pelo administrador.

6.12. Forçar filtragem diretamente nas imagens apresentadas pelos buscadores, ajudando na redução dos riscos de exposição de conteúdo inapropriado nas imagens.

7. Permitir criar cotas de navegação com os seguintes requisitos:

7.1. Tipo do ciclo, especificando se o limite será por duração de acesso à internet ou se será especificado uma data limite para o acesso.

8. CONTROLE E SEGURANÇA DE APLICAÇÕES

8.1. Reconhecer pelo menos 2.700 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer- to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.

8.2. Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Vídeo, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

8.3. Controlar aplicações baseadas em categorias, característica (Ex: Banda e produtividade consumida), tecnologia (Ex: P2P) e risco.

8.4. Permitir criar regras de controle por usuário e host.

8.5. Permitir realizar traffic shaping por aplicação e grupo de aplicações.

8.6. Possibilitar que as regras criadas baseadas em aplicação permitam;

8.7. Bloquear o trafego para as aplicações

8.8. Liberar o trafego para as aplicações

9. CRIAR CATEGORIZAÇÃO DAS APLICAÇÕES POR RISCO:

9.1. Risco muito baixo

9.2. Risco baixo

9.3. Risco médio

9.4. Risco alto

9.5. Risco muito alto

9.6. Permitir visualizar as aplicações por suas características, por exemplo: aplicações que utilizam banda excessiva, consideradas vulneráveis, que geram perda de produtividade, entre outras.

9.7. Permitir selecionar pela tecnologia, por exemplo: p2p, client server, protocolos de redes, entre outros.

9.8. Permitir granularidade na hora da criação da regra baseada em aplicação, como por exemplo: Permitir bloquear anexo dentro de um post do Facebook, bloquear o like do Facebook, permitir acesso ao youtube, mas bloquear o upload de vídeos, e etc.

9.9. Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, Linkedin (Company Search, Compose Webmail,Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Vídeo Search, Vídeo Streaming, Upload, Website).

9.10. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

9.11. Permitir agendar um horário e data especifico para a aplicação das regras de controle de aplicativos, podendo ser executadas apenas uma vez como também de forma recursiva.

9.12. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, Port hopping e túnel através de tráfego SSL encriptado.

9.13. Atualizar a base de assinaturas de aplicações automaticamente.

9.14. Reconhecer aplicações em IPv6.

9.15. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory.

9.16. Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

10. SEGURANÇA DE REDES WIFI

10.1. Fornecer gerencia dos access points do mesmo fabricante remotamente.

10.2. Plug and play no deploy dos access points.

10.3. Permitir criar SSIDs com bridge to LAN, bridge to VLAN e zona separada

10.4. Suporte a múltiplas SSIDs, incluindo hidden SSIDs.

10.5. Suporte WPA2 Personal e Enterprise.

10.6. Suporte a IEEE 802.1X (RADIUS authentication). Suporte a 802.11r (fast transition).

10.7. Suporte a hotspot, customização de voucher, senha do dia e termos de aceitação.

10.8. Acesso a rede wireless baseado em horário.

10.9. Escolha do melhor canal feita automaticamente pela ferramenta, buscando a melhor performance.

10.10. Suporte a login em HTTPS.

10.11. Detecção de Rogue AP.

10.12. O access point deve poder operar e ser gerenciado (tendo alteração de configurações) de forma independente de uma controladora central, onde em caso de interrupção de link isto não afetará sua gerência. Para isto deve-se ter uma controladora local e está controladora deve ser gerenciada de forma central.

11. PROTEÇÃO PARA E-MAILS

11.1. Possuir suporte para escaneamento dos protocolos SMTP, POP3 e IMAP.

11.2. Possuir serviço de reputação para monitoramento dos fluxos dos e-mails, sendo assim, o AntiSpam deverá bloquear e-mails considerados com má reputação na internet e pelo fabricante.

11.3. Bloquear SPAM e MALWARES durante a transação SMTP.

11.4. Possuir duas engines de antivírus para duplo escaneamento.

11.5. Ter proteção em tempo real, a solução deverá realizar consultas na nuvem para verificar a integridade e segurança dos e-mails que passam pela solução e assim tomar ações automáticas de segurança caso necessário.

11.6. Os updates das assinaturas e proteção deverão ser realizados de forma automática pelo fabricante.

11.7. Possuir funcionalidade que permite detectar arquivos por suas extensões e bloqueá-los caso estejam em anexo.

11.8. Usar conteúdo pré-definido pela solução para que seja possível criar regras baseadas neste conteúdo ou customizá-los de acordo com o desejado.

11.9. Ter suporte a criptografia TLS para SMTP, POP e IMAP.

11.10. Ter a possibilidade de agregar RBLs do fabricante e terceiras para ajudar composição de segurança da ferramenta.

12. AS AÇÕES DOS E-MAILS CONSIDERADOD SPAM DEVEM SER:

12.1. Drop

12.2. Warn

12.3. Quarantine

12.4. Poder definir um prefixo no subject de cada e-mail considerado SPAM, como por exemplo: [SPAM] Marketing etc.

12.5. Permitir visualizar os e-mails que se encontram na fila para serem enviadas.

12.6. Possuir funcionalidade que permita a adição de um banner no final dos E-mails analisados pela solução.

12.7. Possuir funcionalidade de allowlist e blocklist.

12.8. Possuir funcionalidade que rejeite e-mails com HELO invalido e/ou que não possuam RDNS.

12.9. Permitir que o escaneamento seja feito tanto para e-mails de entrada quanto para os de saída.

13. QUARENTENA DE E-MAIL

13.1. Possuir quarentena para os e-mails e opções de notificações para o administrador.

13.2. E-mails que possuem malwares e spam e foram quarentenados, devem ter a opção para serem pesquisados por filtros como: data, sender, recipient e subject, todos eles devem possuir a opção para realização do release da mensagem e a opção para remoção.

13.3. O usuário deve poder gerenciar sua quarentena de e-mails através de um portal disponibilizado pela própria solução, onde ele poderá visualizar e realizar release das mensagens em quarentena.

13.4. As regras do administrador não poderão ser ignoradas, o usuário tomará ações somente as quais for permitido.

13.5. Permitir o administrador agendar diariamente, semanalmente ou mensalmente o envio de relatório de quarentena para todos os usuários.

13.6. Possuir funcionalidade de criptografia de e-mails e DLP para os dados

13.7. Possuir funcionalidade de encriptação de e-mails que não necessite a configurações complexas que envolvam certificados entre outros requisitos.

13.8. Os e-mails criptografados poderão ter seu conteúdo armazenado em um arquivo PDF.

13.9. Ter como funcionalidade a possibilidade de o usuário pode registrar sua própria senha de segurança para que seja possível abrir os e-mails criptografados.

13.10. Possuir também funcionalidade para geração de senhas aleatória para desencriptação do conteúdo.

13.11. Permitir enviar anexos junto aos e-mails criptografados.

13.12. Para o usuário final o uso desta criptografia deve ser completamente transparente, ou seja, não se deve utilizar qualquer software adicional, plugin, ou client instalado no equipamento.

13.13. Possuir funcionalidade de DLP nos E-mails

13.14. A engine de DLP deve ser automática na hora de escanear os e-mails e anexos, assim identificando todos os dados sensíveis encontrados no e-mail sem qualquer intervenção.

13.15. Possuir templates de dados considerados sensíveis preestabelecidos pelo fabricante (CCLs) com os padrões PII, PCI, HIPAA, com a intenção de ajudar o administrador na criação das regras desejadas e seguir as principais normas do mercado, elas deverão ser mantidas pelo fabricante.

13.16. Ter a opção de criar exceções individuais para cada tipo de situação.

13.17. As regras devem corresponder para as redes de origem e alvos específicos como a especificados por URLs.

13.18. Suporte a operadores lógicos

13.19. Poder definir tamanho máximo para escaneamento.

13.20. Permitir bloquear e liberar ranges IP.

13.21. Suporte para utilização de Wildcards

13.22. Anexar automaticamente um prefixo/sufixo para autenticação.

14. ESPECIFICAÇÕES DA ADMINISTRAÇÃO, AUTENTICAÇÃO E CONFIGURAÇÕES EM GERAL

14.1. A solução proposta deve suportar administração via comunicação segura (HTTPS, SSH) e console.

14.2. A solução proposta deve ser capaz de importar e exportar cópias de segurança (backup)das configurações, incluindo os objetos de usuário.

14.3. O backup pode ser realizado localmente, enviado pela ferramenta para um ou mais e-mails pré-definidos e via FTP, deve-se também ser feito sob demanda, ou seja, agendar para que este backup seja realizado, por dia, semana, mês e ano.

14.4. A solução proposta deve suportar implementações em modo Router (camada 3) e transparente (camada 2) individualmente ou simultâneos.

14.5. A solução proposta deve suportar integrações com Active Directory, LDAP, Radius, e Directory, TACACS+ e Banco de Dados Local para autenticação do usuário.

14.6. A solução proposta deve suportar em modo automático e transparente “Single Sign On” na autenticação dos usuários do active directory e eDirectory.

14.7. Os tipos de autenticação devem ser, modo transparente, por autenticação Kerberus/NTLM e cliente de autenticação nas máquinas.

14.8. 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.

14.9. Deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.

14.10. Certificados de autenticação para iOS e Android.

14.11. A solução proposta deve suportar integração com Dynamic DNS de terceiros

14.12. A solução proposta deve ter gráficos de utilização de banda em modos diários, semanais, mensais ou anuais para os links de forma consolidada ou individual.

14.13. solução proposta deve suportar Parent Proxy com suporte a IP / FQDN.

14.14. solução proposta deve suportar NTP.

14.15. solução proposta deverá suportar a funcionalidade de unir usuário/ip/mac para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança.

14.16. solução proposta deve ter suporte multilíngue para console de administração web.

14.17. solução proposta deverá suportar fazer um roll back de versão.

14.18. solução proposta deve suportar a criação de usuário baseada em ACL para fins de administração.

14.19. A solução proposta deve suportar instalação de LAN by-pass no caso do appliance

14.20. estar configurado no modo transparente.

14.21. solução proposta deve suportar cliente PPPOE e deve ser capaz de atualizar automaticamente todas as configurações necessárias, sempre que PPPOE trocar.

14.22. A solução proposta deve suportar SNMP v1, v2c.

14.23. A solução proposta deve suportar SSL/TLS para integração com o Active Directory ou LDAP.

14.24. A solução proposta deve possuir serviço de “Host Dynamic DNS” sem custo e com segurança reforçada.

14.25. A solução proposta deve ser baseada em Firmware ao contrário de Software e deve ser capaz de armazenar duas versões de Firmware ao mesmo tempo para facilitar o retorno “rollback” da cópia de segurança.

14.26. A solução proposta deve fornecer uma interface gráfica de administração flexível e granular baseado em perfis de acesso.

14.27. A solução proposta deve fornecer suporte a múltiplos servidores de autenticação para diferentes funcionalidades (Exemplo: Firewall um tipo de autenticação, VPN outro tipo de autenticação)

14.28. A solução proposta deve ter suporte a ambientes de terminais (Microsoft e Citrix);

14.29. Suportando autenticação de usuário de diferentes sessões originando do mesmo endereço IP.

15. A SOLUÇÃO PROPOSTA DEVE SUPORTAR:

15.1. Serviço de DHCP/DHCPv6;

15.2. Serviço de DHCP/DHCPv6 Relay Agent;

15.3. Suporte a DHCP sobre VPN IPSec;

15.4. A solução proposta deve trabalhar como DNS/DNSv6 Proxy.

15.5. Gráficos, relatórios e ferramentas avançadas de o poio para troubleshooting.

15.6. Permitir exportar informações de troubleshooting para arquivo PCAP.

15.7. Permitir o factory reset e troca do idioma via interface gráfica.

15.8. Atualização de firmware de forma automatizada;

15.9. Reutilização de definições de objetos de rede, host, serviços, período de tempo, usuários, grupos, clientes e servers.

15.10. Portal de acesso exclusivo para usuários poderem realizar atividades administrativas que envolve apenas funcionalidades específicas a ele.

15.11. Controle de acesso e dispositivos por zoneamento.

15.12. Integrar com ferramenta de gerenciamento centralizado disponibilizado pela própria fabricante.

15.13. Opção de habilitar acesso remoto do appliance para suporte diretamente com o fabricante através de um túnel seguro, esta funcionalidade deve estar embarcada dentro do próprio appliance ofertado.

15.14. Traps SNMP ou e-mail para notificações do sistema.

15.15. Suportar envio de informações via Netflow e possuir informações via SNMP.

15.16. Suporte a TAP mode para POCs e trials.

15.17. Ter funcionalidade que permita que o administrador manualmente atribua e/ou distribua cores do CPU para uma interface em particular, dessa forma, todo trafego que passar por esta interface, será tratado unicamente pelos núcleos definidos.

15.18. Possuir funcionalidade de Fast Path para realizar a otimização no tratamento dos pacotes.

16. ESPECIFICAÇÕES DE BALANCEAMENTO DE CARGA E REDUNDÂNCIA PARA MÚLTIPLOS PROVEDORES DE INTERNET

16.1. A solução proposta deve suportar o balanceamento de carga e redundância para mais de 2 (dois) links de Internet.

16.2. A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário e aplicação.

16.3. A solução proposta deve suportar algoritmo “Round Robin” para balanceamento de carga.

16.4. A solução proposta deve fornecer opções de condições em caso de falha “Failover” do link de Internet através dos protocolos ICMP, TCP e UDP.

16.5. A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway.

16.6. A solução proposta deve ter ativo/ativo utilizando algoritmo de “Round Robin” e ativo/passivo para o balanceamento de carga do gateway e suporte a falha (Failover).

16.7. A solução proposta deve fornecer o gerenciamento para múltiplos links de Internet bem como tráfego IPv4 e IPv6.

17. ESPECIFICAÇÕES DE ALTA DISPONIBILIDADE

17.1. A solução proposta deve suportar Alta Disponibilidade (High Availability) ativo/ativo e ativo/passivo.

17.2. A solução proposta deve notificar os administradores sobre o estado (status) dos gateways mantendo a Alta Disponibilidade.

17.3. O tráfego entre os equipamentos em Alta Disponibilidade deverá ser criptografado.

17.4. A solução deverá detectar falha em caso de Link de Internet, Hardware e Sessão.

17.5. A solução proposta deve suportar sincronização automática e manual entre os appliances em “cluster”.

17.6. A solução deve suportar Alta Disponibilidade (HA) em “Bridge Mode” e Mixed Mode" (Gateway + Bridge).

18. PROTEÇÃO BÁSICA DE FIREWALL

18.1. Especificações do Firewall e roteamento;

18.2. A solução deve ser Standalone Appliance e com Sistema Operacional fortalecido “Hardening” para aumentar a segurança.

18.3. Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

18.4. Suporte a objetos e regras IPV6.

18.5. Suporte a objetos e regras multicast.

18.6. A solução proposta deve suportar "Stateful Inspection" baseado no usuário "oneto-one", NAT Dinâmico e PAT.

18.7. A solução proposta deve usar a "Identidade do Usuário" como critério de Origem/Destino, IP/Subnet/Grupo e Porta de Destino na regra do Firewall.

18.8. A solução proposta deve unificar as políticas de ameaças de forma granular como Antivírus/AntiSpam, IPS, Filtro de Conteúdo, Políticas de Largura de Banda e Política de Balanceamento de Carga baseado na mesma regra do Firewall para facilitar de uso.

18.9. A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.

18.10. Deve permitir o bloqueio de vulnerabilidades.

18.11. Deve permitir o bloqueio de exploits conhecidos.

18.12. A solução proposta deve suportar arquitetura de segurança baseado em Zonas

18.13. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

18.14. A solução proposta deve ter predefinido aplicações baseadas na "porta/assinatura" e também suporte à criação de aplicativo personalizado baseado na "porta/número de protocolo".

18.15. A solução proposta deve suportar balanceamento de carga de entrada (Inbound NAT) com diferentes métodos de balanceamento como First Alive, Round Robin, Random, Sticky IP e Failover conforme a saúde (Health Check) do servidor por monitoramento (probe) TCP ou ICMP.

18.16. A solução proposta deve suportar 802.1q (suporte a marcação de VLAN).

18.17. A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, OSPF, BGP4.

18.18. A solução proposta deve possuir uma forma de criar roteamento Estático/Dinâmico via shell.

18.19. O sistema proposto deve prover mensagem de alertas no Dash Board (Painel de Bordo) quando eventos como: a senha padrão não foi alterada, acesso não seguro está permitindo ou a licença expirará em breve.

18.20. O sistema proposto deve prover Regras de Firewall através de endereço MAC (MAC Address) para prover segurança na camada de rede 2 até 7 do modelo OSI.

18.21. A solução proposta deve suportar IPv6.

18.22. IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.

18.23. A solução proposta deve suportar implementações de IPv6 Dual Stack.

18.24. A solução proposta deve suportar tuneis 6in4,6to4,4in6,6rd.

18.25. A solução proposta deve suportar toda a configuração de IPv6 através da Interface Gráfica.

18.26. A solução proposta deve suportar DNSv6;

18.27. A solução proposta deve oferecer proteção DoS contra ataques IPv6;

18.28. A solução proposta deve oferecer prevenção contra Spoof em IPv6;

18.29. A solução proposta deve suportar 802.3 ad para Link Aggregation;

18.30. A solução proposta deve suportar gerenciamento de banda baseado em Aplicação que permite administradores criarem políticas de banda de utilização de link baseado por aplicação;

18.31. Flood protection, DoS, DDoS e Portscan;

18.32. Bloqueio de Países baseados em GeoIP;

18.33. Suporte a Upstream proxy;

18.34. Suporte a VLAN DHCP e tagging;

18.35. Suporte a Multiple bridge.

18.36. Funcionalidades do portal do usuário

18.37. Autenticação de dois fatores (OTP) para IPSEC e SSL VPN, portal do usuário, e administração web (GUI).

18.38. Download dos clientes de autenticação disponibilizados pela ferramenta.

18.39. Download do cliente VPN SSL em plataformas Windows.

18.40. Download das configurações SSL em outras plataformas.

18.41. Informações de hotspot.

18.42. Autonomia de troca de senha do usuário.

18.43. Visualização do uso de internet do usuário conectado.

18.44. Acesso a mensagens quarentenadas.

18.45. Opções base de VPN

18.46. A VPN IPsec deve suportar: DES e 3DES, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128,192 e 256 (Advanced Encryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).

18.47. L2TP e PPTP.

18.48. VPN SSL, IPSEC.

18.49. Proporcionar através do portal do usuário uma forma de conexão via HTML5 de acesso remoto com suporte aos protocolos, RDP, HTTP, HTTPS, SSH, Telnet e VNC.

18.50. Suportar autenticação via AD/LDAP, Token e base de usuários local.

18.51. Funcionalidades base de QoS e Quotas

18.52. QoS aplicado a redes e usuários de download/Upload em tráfegos baseados em serviços.

18.53. Otimização em tempo real do protocolo Voip.

18.54. Suporte a marcação DSCP.

18.55. Regras associadas por usuário.

18.56. Criar regras que limitem e garantam upload e download.

18.57. Permitir criar regra de QoS individualmente e compartilhada.

19. PROTEÇÃO DE REDES

19.1. Prover funcionalidade de Intrusion Prevention System (IPS) Proporcionar alta performance na inspeção dos pacotes

19.2. Possuir mais de 7000 mil assinaturas conhecidas.

19.3. Suportar a customização de assinaturas, permitindo o administrador agregar novas sempre que desejado.

19.4. Proporcionar flexibilização na criação das regras de IPS, ou seja, permitir que as regras possam ser aplicadas tanto para usuários quanto para redes, permitindo total customização.

19.5. Possuir funcionalidade Anti-DoS.

19.6. Ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP Flood, etc.

20. DEVE-SE PERMITIR CUSTOMIZAR OS VALORES DAS SEGUINTES FUNCIONALIDADES DE DOS:

20.1. SYN Flood;

20.2. UDP Flood;

20.3. TCP Flood;

20.4. ICMP Flood;

20.5. IP Flood;

20.6. Possuir templates pré-configurados pelo fabricante havendo sugestões de fluxo dos pacotes, exemplo: LAN to DMZ, WAN to LAN, LAN to WAN, WAN to DMZ, e etc.

20.7. Possuir proteção contra spoofing.

20.8. Poder restringir IPs não confiáveis, somente aqueles que possuírem MAC address cadastrados como confiáveis.

20.9. Possuir funcionalidade para o administrador poder criar by-pass de DoS.

20.10. Permitir o administrador clonar templates existentes para ter como base na hora da criação de sua política customizada.

20.11. Possuir proteção avançada contra ameaças persistentes (APT)

20.12. Deve detectar e bloquear trafego de pacotes suspeitos e maliciosos que trafegam pela rede onde tentam realizar comunicação com servidores de comando externo(C&C), usando técnicas de multicamadas, DNS, AFC, Firewall e outros.

20.13. Possuir logs e relatórios que informem todos eventos de APT.

20.14. Permitir que o administrador possa configurar entre apenas logar os eventos ou logar e bloquear as conexões consideradas ameaças persistentes.

20.15. Em casos de falso positivo, permitir o administrador criar exceções para o fluxo considerado como APT.

21. PROTEÇÃO PARA SERVIDORES WEB (WAF)

21.1. Possuir funcionalidade de proxy reverso

21.2. Possuir engine de URL hardening e prevenção a directory traversal.

21.3. Possuir engine Form hardening.

21.4. Proteção contra SQL injection

21.5. Proteção contra Cross-site scripting

21.6. Possuir duas engines de antivírus disponíveis para análise de malware.

21.7. Permitir definir o fluxo que o antivírus atuará, se será no upload ou download.

21.8. Permitir limitar o tamanho máximo em que o antivírus atuará.

21.9. Permitir bloquear conteúdo considerado unscannable.

21.10. Possuir HTTPS (SSL) encryption offloading.

21.11. Proteção para cookie signing com assinaturas digitais.

21.12. Possuir Path-based routing.

21.13. Suporte ao protocolo do Outlook anywhere.

21.14. Possuir autenticação reversa para acesso aos servidores web.

21.15. Permitir criar templates de autenticação, onde o administrador poderá configurar uma página em HTML para autenticação.

21.16. Ter abstração de servidores virtuais e físicos.

21.17. Proporcionar função de load balancer para que os visitantes possam ser jogados para diversos servidores de forma transparente.

21.18. Permitir definir qual modo o WAF deve operar, tendo como opção modo de monitoramento apenas e modo para rejeitar as conexões consideradas maliciosas.

21.19. Bloquear clients com má reputação.

21.20. Bloquear protocolos com anomalias.

21.21. Limitar número de requisições.

22. FERRAMENTAS DE RELATÓRIOS CENTRALIZADO

22.1. Permitir que todos os appliances do fabricante possam centralizar seus relatórios em um único appliance especializado para esta função.

22.2. Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.

22.3. Permitir a customização dos relatórios padrão da solução, permitindo o administrador criar relatórios de acordo com as necessidades do ambiente e informações desejadas.

22.4. Permitir que o administrador realize agendamentos destes relatórios para que estes sejam enviados via e-mail para todos os e-mails cadastrados.

22.5. Ter relatórios customizados e em conformidade com, pelo menos, estes órgãos; HIPAA, SOX, PCI.

22.6. Ter fácil identificação das atividades de rede e ataques em potencial.

22.7. Armazenar histórico dos relatórios em disco local.

22.8. Possuir relatórios únicos para cada um dos módulos ofertados pela solução.

22.9. Possuir multiformato de relatórios, pelo menos tabular e gráfico.

22.10. Permitir exportar relatórios para: PDF, Excel.

22.11. Possuir relatórios sobre as pesquisas realizadas pelos usuários nos principais buscadores: Yahoo, Bing, Wikipédia, Google.

22.12. Possuir relatórios que informem principais atividades em cada módulo.

22.13. Ter logs em tempo real.

22.14. Ter logs arquivados para consulta posterior.

22.15. Permitir que o administrador consiga realizar pesquisas dentro dos logs arquivados.

22.16. Possuir logs de auditoria.

22.17. Ter sua gerência totalmente baseada em acesso web.

22.18. Permitir que o administrador crie regras baseadas em usuários onde cada usuário criado poderá ter acesso a funcionalidades específicas na ferramenta.

22.19. Deve-se detectar automaticamente um equipamento do mesmo fabricante quando este se reportar ao centralizador de relatórios, onde o administrador do sistema poderá dar um aceite ou não neste appliance que está realizando a tentativa de integração.

22.20. Permitir agrupamento dos equipamentos por tipo do dispositivo e modelo do equipamento.

22.21. O administrador deve poder acessar estes relatórios de qualquer lugar através de apenas um navegador.

22.22. Possuir gerenciamento somente de appliances favoritos.

22.23. Ter total gerencia sobre a retenção dos dados armazenados neste equipamento.

22.24. Ter disponibilidade em appliance virtual e software caso necessário instalar o appliance em um hardware baseado em Intel.

23. POSSUIR SUPORTE NO MINIMO AOS VIRTUALIZADORES:

23.1. VMware

23.2. Hyper-V

23.3. Citrix

23.4. KVM

23.5. Proxmox

23.6. Possuir capacidade de armazenamento ilimitado, tendo apenas o disco como limitador.

23.7. Devem ser fornecidas soluções virtuais ou via appliance desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 1TB de dados.

23.8. Deve possuir mecanismo de procura de logs arquivados.

23.9. Deve ter acesso baseado em Web com controles administrativos distintos.

24. SERVIÇOS DE INSTALAÇÃO

24.1. Instalação do equipamento no rack 19 “

24.2. Ativação do sistema operacional, com instalação da licença e demais particularidades do equipamento.

24.3. Criação de usuários para administração e gerência do equipamento.

24.4. Configuração de 2 (dois) links de internet, configurações de endereços IPv4 e IPV6 públicos dos respectivos links.

24.5. Redirecionamento de 15 portas da rede externa para rede DMZ, mais o redirecionamento de um range de portas para o serviço de telefonia VOIP.

24.6. Criação de 4 (quatro) perfis de navegação, bloqueando conteúdo específicos por determinado perfil.

24.7. Integração com Microsoft Active Directory, autenticando o usuário automaticamente com as credenciais de acesso ao computador. Ativar a funcionalidade de Proxy SSL.

24.8. Ativar proteção AntiSpam, IPS e anti-DDOS.

24.9. Ativar proteção de servidores WEB.

24.10. Bloquear aplicações como TOR e Torrents.

24.11. Criar uma regra de QOS.

24.12. Configuração do sistema AntiSpam no servidor de E-mail Zimbra 8.0

25. A CONTRATADA deverá ministrar treinamento relativo à instalação, operacionalização, manuseio, configuração e utilização da solução de segurança, visando garantir a transferência de conhecimento para até 4 (quatro) pessoas indicadas pela CONTRATANTE:

25.1. O treinamento deverá possuir carga horária mínima de 8 (oito) horas, observando- se que o treinamento deverá conter todo o conteúdo sobre a solução.

25.2. As datas e horários para realização dos treinamentos serão definidos pela CONTRATANTE em comum acordo com a CONTRATADA.

25.3. O treinamento deverá ser oficial e autorizado pelo fabricante da solução, devendo ser apresentado.

25.4. O instrutor deverá possuir experiência em treinamentos desta natureza e pleno conhecimento da solução de segurança.

25.5. Deverá ser emitido certificado aos participantes do treinamento que cumprirem frequência mínima de 80%.

25.6. Treinamento deve ser ministrado por um técnico Nível Architect Next Generation Firewall.

26. BANCO DE HORAS:

26.1. De acordo com a necessidade apresentada, será passível a contratação de serviços técnicos especializados com o objetivo de garantir a plena utilização da solução contratada, bem como sua instalação e adequação ao ambiente tecnológico da CONTRATANTE;

26.2. Principais serviços cobertos pelo banco de horas:

26.3. Consultoria em sistema de Firewall UTM e demais componentes;

26.4. Instalação e ajustes de ambiente e instalação de novas funcionalidades perfeito funcionamento dos serviços;

26.5. Todo o material para os serviços do item acima, deverão estar inclusos;

26.6. O serviço de operação assistida a ser demandado somente será executado pela CONTRATADA mediante Ordem de Serviço (OS);

26.7. Este método de trabalho baseado no conceito de Delegação de Responsabilidade atribui a CONTRATANTE a gestão qualitativa dos resultados, a serem obtidas por meio da execução dos serviços dentro dos prazos e pela obtenção dos produtos previstos, e à CONTRATADA as responsabilidades da execução operacional dos serviços, por meio da disponibilização e gerência de todos os recursos humanos necessários à execução dos serviços;

26.8. As Ordens de Serviço serão consideradas como adendos ao Contrato e deverão descrever, entre outros itens, os serviços de forma detalhada, contemplando: a identificação do tipo de serviço, complexidade, prazos, requisitos de qualidade, e responsável pelo atesto;

26.9. O aceite e o posterior pagamento dos serviços e artefatos (produtos) executados e entregues pela CONTRATADA não a exime das responsabilidades quanto às garantias específicas associadas a cada produto desenvolvido e estabelecido na O.S., ficando a CONTRATADA responsável pela correção de todos os erros, defeitos, bugs, falhas e quaisquer outras irregularidades, pelo período mínimo de 02 (dois) meses, contado a partir de emissão do Termo de Aceite;

26.10. Cada Ordem de Serviço deverá ser dimensionada em conjunto com o Gestor de Contrato e equipe técnica designada pelo CONTRATANTE.

27. FORMULÁRIO PARA PROPOSTA DE PREÇO

Item	Qtd.	Unid.	Especificações do Objeto	Marca	Valor Unitário	Valor Mensal	Valor Total
01	2	Unid.	Contrato de Firewall de Próxima Geração - Solução composta de 1 (um) appliance conforme termo de referência. Pacote de licenças da Console de Gerência Administrativa e Centralização de Logs e Relatórios. Pacote de licenças de Firewall, IPS, Anti-spyware, Filtro de Web, Proteção contra ameaças avançadas e firewall de aplicação web para appliance de Firewall de Próxima Geração Tipo 1 pelo prazo de 48 meses.				

02	01	Unid	Instalação, configuração e treinamento profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento, Centralização e Monitoração de Logs Centralizado.				
03	10	Horas	Banco de horas para execução de atividades especializadas de Segurança da Informação. Item 26 do Termo de Referência- Anexo I				

28. INFORMAÇÕES:

A licitante vencedora se obriga a fornecer soluções em Appliance de Firewall com Gerenciamento Unificado de Ameaças (UTM – Unified Threat Mangement), entendendo-se como tais, o conjunto de hardware e software dedicados, necessários e suficientes para o funcionamento da solução, atualização e treinamento para capacitação técnica da equipe da Prefeitura Municipal de Campo Bom, de acordo com as especificações descritas no ANEXO I – Termo de Referência.

I. A licitante vencedora deverá iniciar a instalação dos equipamentos em até 45 (quarenta e cinco) dias após a assinatura do contrato.

II. Os equipamentos deverão ser entregues em até 45 (quarenta e cinco) dias após a assinatura do contrato.

III. A instalação e entrega deverá ocorrer junto ao Divisão de Informática, no centro administrativo da Prefeitura Municipal e Campo Bom.

IV. As especificações gerais do objeto, constam no ANEXO I – Termo de Referência, deste Edital.

V. A licitante vencedora deverá ministrar treinamento relativo à instalação, operacionalização, manuseio, configuração e utilização da solução de segurança, para os funcionários indicados pela Prefeitura Municipal de Campo Bom. As datas e horários para a realização do treinamento deverão ser combinados previamente entre as partes.

VI. O treinamento deverá ter carga horária mínima de 08 (oito) horas, observando-se que o treinamento deverá conter, de forma integral, o conteúdo da solução.

VII. O treinamento deverá ser oficial e autorizado pelo fabricante da solução. Além disso, o instrutor deverá possuir experiência em treinamento desta natureza e conhecimento da solução de segurança.

VIII. Deverá ser emitido certificado aos participantes do treinamento que cumprirem 80% da carga horária do treinamento.

IX. A licitante vencedora deverá prover a instalação e configuração de todas as atualizações fornecidas pelo fabricante do produto, sem custos à Prefeitura Municipal de Campo Bom.

X. O fabricante deverá fornecer garantia dos equipamentos pelo período de vigência das licenças.

XI. A vigência contratual será de 12 (doze) meses, contados da data de assinatura do Contrato.

XII. Todas as despesas (de qualquer natureza), sejam elas tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais), fornecimento de mão-de-obra especializada, leis sociais, administração, lucros, equipamentos e ferramentas, transporte de material e de pessoal, acomodações e despesas com os funcionários da contratada que executarão os serviços (alojamento, transporte, refeição, encargos sociais, trabalhistas, etc.) e demais despesas referentes à execução do objeto da presente licitação, ficarão a cargo da licitante vencedora.

ANEXO I - B

PREGÃO ELETRÔNICO Nº 128/2022
FIREWALL

1. ATIVIDADES DE SUPORTE E MANUTENÇÃO:

1.1. Problemas, correções, aplicações de patches, mudanças de configuração e eventos ocorridos no período;

1.2. Inventário lógico de ativos de segurança;

1.3. Chamados abertos no período, ações corretivas tomadas, tempos para execução das atividades;

1.4. Diagnóstico dos ambientes monitorados, obtido por meio do cruzamento das informações obtidas nos logs coletados;

2. Relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a qualidade e desempenho dos serviços prestados em relação ao atingimento ou não dos níveis mínimos de serviço, com pelo menos, as seguintes informações:

2.1. Atualizações de software realizadas no período;

2.2. Sites com maior volume de dados acessados por esses usuários;

2.3. Sites acessados por determinados usuários, classificado por username;

2.4. Ataques e tentativas de ataques à rede Prefeitura Municipal de Campo Bom;

2.5. Análise e mitigação de ameaças (quantidade, estudo, mitigação, priorização);

2.6. Plano de ações sobre vulnerabilidades identificadas;

2.7. Definição e implantação das rotinas de backup de todos os equipamentos componentes dos serviços. Nesse sentido, será responsabilidade da contratada o backup realizado pela própria, bem como a execução das configurações necessárias para realização de um backup secundário pelo software em uso atualmente pela Divisão de Informática da Prefeitura Municipal de Campo Bom.

2.8. Definição e implementação dos mecanismos permanentes de monitoramento dos equipamentos componentes da solução, inclusive com envio de informações de monitoramento para a solução em uso pelo Centro de Operação de Redes da Prefeitura Municipal de Campo Bom (software Zabbix);

2.9. Procedimento operacional para recuperação em caso de indisponibilidade do datacenter (disaster recovery);

2.10. Análise e implantação de ajustes nas permissões de acesso de usuários aos componentes da solução, mediante autorização prévia da Prefeitura Municipal de Campo Bom;

2.11. Integração à base de usuários de rede da Prefeitura Municipal de Campo Bom (Active Directory) ou à plataforma de autenticação em uso pela Divisão de Informática da Prefeitura Municipal de Campo Bom (Radius) dos componentes da solução, nos casos previstos na especificação técnica;

2.12. Mapeamento, junto à Prefeitura Municipal de Campo Bom, dos processos necessários ao cumprimento dos requisitos deste Termo;

2.13. Para todos os equipamentos, produtos ou peças utilizadas na prestação dos serviços, a contratada deverá identificar, em local visível, por meio de etiqueta de material resistente, os equipamentos utilizados e os cabos de rede a eles conectados;

3. Para todos os equipamentos, produtos ou softwares utilizados no atendimento aos requisitos destas Especificações Técnicas, deverão ser criadas:

3.1. Conta de usuário com controle total para que a equipe de servidores designados pela Divisão de Informática da Prefeitura Municipal de Campo Bom de forma a possibilitar a atuação nos equipamentos em casos de indisponibilidade dos serviços da contratada, por quaisquer motivos;

3.2. Contas de usuários para acesso pelos funcionários da contratada, mantidas em base de usuários local.

3.3. As contas de usuários com controle total, somente serão utilizadas pela Divisão de Informática da Prefeitura Municipal de Campo Bom, em momentos de indisponibilidade dos serviços da contratada, ou ainda, em situações de emergência em que a contratada viole os níveis mínimos de serviço contratado;

3.4. Para todos os equipamentos, produtos ou softwares utilizados no atendimento aos requisitos deste Termo, deverão ser autorizados grupos de usuários (do Active Directory da Prefeitura Municipal de Campo Bom) para que a equipe possa monitorar e consultar informações nos equipamentos;

3.5. Quaisquer componentes adicionais que se fizerem necessários para que os produtos descritos ofereçam todas as características expostas, bem como para a perfeita instalação e utilização dos produtos, deverão ser providos pela contratada;

3.6. No momento do envio da proposta comercial ajustada, o licitante deverá apresentar planilha de composição de custos detalhada de forma a permitir a repactuação futura do contrato;

4. CONDIÇÕES DE EXECUÇÃO DOS TREINAMENTOS:

4.1. Deverão ser previamente agendados pela Divisão de Informática da Prefeitura Municipal de Campo Bom;

4.2. A alteração dos prazos de início/término dos treinamentos somente será possível mediante apresentação, pela contratada, de relatório de impacto contendo justificativas plausíveis, devidamente aceitas pela Divisão de Informática da Prefeitura Municipal de Campo Bom;

4.3. Os treinamentos só serão considerados concluídos após a avaliação do treinamento realizado ser feita pela Divisão de Informática da Prefeitura Municipal de Campo Bom;

4.4. Os treinamentos serão avaliados pelos participantes com nota de 1 a 5, considerando notas abaixo de (3) como “treinamento insatisfatório", devendo ser repetido neste caso;

4.5. Os treinamentos poderão ser online ou presencial conforme o caso e a temática; em caso de treinamento presencial deverá ser realizado nas dependências da Prefeitura Municipal de Campo Bom;

4.6. A contratada deverá providenciar material didático individual que abranja todo o conteúdo do curso. Não será exigido material oficial do fabricante nem impresso, entretanto este será avaliado pela equipe técnica da Prefeitura Municipal de Campo Bom antes da realização do curso, e caso seja considerado insuficiente, deverá ser readaptado para as condições exigidas pela Divisão de Informática da Prefeitura Municipal de Campo Bom;

4.7. Para a realização da parte prática do treinamento, deverão ser utilizados equipamentos similares aos ofertados, além de todos os softwares que fizerem parte da solução;

4.8. A contratada deverá fornecer, ao final do curso, certificado individual de conclusão com carga horária e conteúdo do curso;

5. DA ENTREGA / EXECUÇÃO:

5.1. A execução do objeto deverá ser iniciada imediatamente após a assinatura do contrato e do termo de confidencialidade.

5.2. A contratada deverá seguir todas as diretivas do Licitante (Controlador) atendendo as hipóteses legais da Lei 13.709/2018.

5.3. Todas as despesas de deslocamento, alimentação serão por conta da Licitada, devendo compreender o seu custo na hora de suporte.

5.4. O serviço deverá estar disponível durante o horário de expediente da Prefeitura Municipal de Campo Bom (das 7:30 hs às 18:30 hs), de segunda a sexta-feira, eventualmente após o expediente e finais de semana.

5.5. As atualizações dos sistemas operacionais devem ser realizadas mediante aprovação do corpo técnico da Prefeitura Municipal de Campo Bom, bem como previsão de horas para a demanda.

5.6. O período excedente além das horas previstas deverá ser comunicado com antecedência ao corpo técnico da Prefeitura Municipal de Campo Bom para obtenção de aprovação prévia junto à Diretoria de Informática.

5.7. Customizações serão desenvolvidas segundo cronograma aprovado pelo corpo técnico do Prefeitura Municipal de Campo Bom.

Severidade	Descrição	Tempo de resposta máximo
CRÍTICA	Indisponibilidade total dos serviços	1 Hora
ALTA	Indisponibilidade parcial dos serviços	4 Horas
MÉDIA	Esclarecimento de dúvidas, alteração de configurações não críticas ou configuração de novas implementações.	24 Horas

5.8. A empresa contratada deve monitorar: logs, espaços disponíveis, violação de segurança, atualizações de softwares e pacotes disponíveis, interrupção de serviços, eventos críticos, tentativas de invasão, permitir a inclusão de outras variáveis de monitoramento.

6. ATENDIMENTO DE SUPORTE TÉCNICO DEVERÁ OCORRER:

6.1. Via telefone: O serviço telefônico deverá ficar à disposição de 08h00min as 18h00min, devendo ser prestado em português, sem custo adicional para a Prefeitura Municipal de Campo Bom;

6.2. O Ticket: Através da abertura de ordem de serviço (OS) em sistema de registro de chamados acessível de forma online disponibilizado em site da Licitante, deverá ser fornecido treinamento ao cliente sobre o uso da ferramenta.

6.3. Acesso remoto: Quando permitido, via acesso remoto (VPN) pela Licitante nos servidores da Empresa, sem a necessidade de aquisição de licenças de software pela Prefeitura Municipal de Campo Bom para realização do acesso independentemente do canal de comunicação utilizado para acionar um pedido de suporte, todas as solicitações devem ser registradas em sistema de Ticket no site da Licitante.

6.4. Os acessos às estatísticas e números de atendimentos devem estar disponíveis para Prefeitura Municipal de Campo Bom.

6.5. Independente da forma como for aberto o chamado, a contratada deverá registrar o chamado no Help Desk, mesmo que este se resolva por telefone, com o registro da hora de abertura e fechamento.

6.6. Os eventos devem ser acompanhados pela contratada e enviados para a equipe de suporte de TI da Prefeitura Municipal de Campo Bom via e-mail.

6.7. Os técnicos de Informática da Prefeitura Municipal de Campo Bom, não possuem números de celulares coorporativos, bem como contas de WhatsApp vinculados ao órgão público, portanto, esse meio de comunicação não será aceito para abertura de chamados e acompanhamento dos mesmos.

7. PENALIDADES

7.1. Sem prejuízo das demais disposições legais, em caso de inexecução, total ou parcial, do objeto, bem como falhas ou atrasos em sua execução, poderão ser aplicadas as seguintes sanções e penalidades:

7.2. Advertências, quando da ocorrência de faltas consideradas leves, assim entendidas, aquelas que não acarretarem danos e/ou prejuízos à Prefeitura Municipal de Campo Bom;

8. MULTAS

8.1. no percentual de até 5% (cinco por cento) sobre o valor da ordem de compra, em caso de atraso injustificado na execução do objeto contratado;

8.2. no percentual de até 5% (cinco por cento) sobre o valor da ordem de compra, em caso de execução do objeto em desacordo com as especificações do contrato e deste Termo de Referência;

8.3. no percentual de até 5% (cinco por cento) sobre o valor da ordem de compra, em caso de atraso injustificado na conclusão da execução do objeto;

8.4. no percentual de até 5% (cinco por cento) sobre o valor da ordem de compra, em caso de não execução parcial do objeto;

8.5. no percentual de até 5% (cinco por cento) sobre o valor do contrato, em caso de infringência injustificada de quaisquer outras cláusulas previstas no instrumento convocatório e ou contratual;

8.6. rescisão antecipada da contratação;

MUNICÍPIO DE CAMPO BOM
ESTADO DO RIO GRANDE DO SUL - BRASIL

Altera-se a data de abertura do certame para o dia 28/12/2022 às 13:30min. As demais cláusulas permanecem inalteradas.

Campo Bom, 16 de dezembro de 2022.

Luciano Libório Baptista Orsi
Prefeito Municipal