CONTRATO DE PRESTAÇÃO DE SERVIÇOS, QUE ENTRE SI, FAZEM A CENTRAIS DE ABASTECIMENTO DE CAMPINAS S/A - CEASA/CAMPINAS E A EMPRESA BLUEPEX CONTROLE E SEGURANÇA EM TI S/A.

PROTOCOLO N.º 2018/16/1257
DISPENSA DE LICITAÇÃO N.º 260/2018
CONTRATO N.º 025/2018

Por este Termo de Contrato de Prestação de Serviços, de um lado como **CONTRATANTE**, a **CENTRAIS DE ABASTECIMENTO DE CAMPINAS S/A - CEASA/CAMPINAS**, sociedade de economia mista de âmbito municipal, inscrita no CNPJ/MF sob o n.º 44.608.776/0001-64, estabelecida na Rodovia D. Pedro I, SP - 065, Km 140,5 - Pista Norte, Campinas/SP, neste ato representada por seu **DIRETOR PRESIDENTE - WANDER DE OLIVEIRA VILLALBA**, brasileiro, casado, Fisioterapeuta, portador do RG n.º 18.337.851-9 SSP/SP, e do CPF n.º 141.089.938-10, por seu **DIRETOR ADMINISTRATIVO E FINANCEIRO - MIGUEL JORGE NICOLAU FILHO**, brasileiro, solteiro, Tecnólogo em Obras de Solos, portador do RG n.º 8.723.774-X SSP/SP, e do CPF n.º 724.291.868-53, e por seu **DIRETOR TÉCNICO OPERACIONAL - CLAUDINEI BARBOSA**, brasileiro, casado, Advogado, portador do RG n.º 18.406.151 SSP/SP, e do CPF n.º 079.624.198-81, todos residentes e domiciliados na cidade de Campinas/SP, e de outro lado, como **CONTRATADA: BLUEPEX CONTROLE E SEGURANÇA EM TI S/A**, empresa devidamente inscrita no CNPJ sob o n.º 02.227.843/0001-50, estabelecida na Rua Wilson Vitorio Coletta, n.º 157, no bairro Jardim Maria Buchi Modeneis, na cidade de Limeira/SP - CEP: 13.482-225, por seu representante legal, **NILTON SILVA FERNANDES DE SOUZA**, portador do RG n.º 11.225.073-3 SSP/RJ, e do CPF n.º 080.763.007-11, residente e domiciliado na cidade de Campinas/SP, ajustam e convencionam as obrigações e compromissos recíprocos que assumem em consonância com a Lei Federal nº. 13.303/2016 e tudo mais que consta do processo administrativo epigrafado.

CLÁUSULA PRIMEIRA
DO OBJETO

1.1. Constitui objeto do presente instrumento a contratação de empresa especializada para a prestação de serviços aplicados à tecnologia da informação, compreendendo a locação de 02 (duas) unidades de Appliance de Firewall com Gerenciamento Unificado de Ameaças (UTM - Unified Threat Management), entendendo-se como tais, o conjunto de hardware e software e serviços, dedicados para o controle e proteção de tráfego de dados, VPN, balanceamento de links, controle de rede proxy e cluster de equipamentos, incluindo serviços de instalação, configuração inicial e treinamento (opcional) para capacitação de equipe técnica da Centrais de Abastecimentos de Campinas S/A - Ceasa/campinas, de acordo com as condições aqui estabelecidas.

CLÁUSULA SEGUNDA
DA VIGÊNCIA DO CONTRATO

2.1. O prazo de vigência do Contrato será de 12 (doze) meses, **iniciando-se** em **01/12/2018** e se **encerrando** em **30/11/2019**, podendo ser prorrogado por acordo

BANCO MUNICIPAL DE ALIMENTOS
CEASA - Mariana Romão - Jurídico
OAB/SP nº 263.559

entre as partes, observadas as disposições da Lei Federal n.º 13.303/2016, mediante justificativa e autorização e desde que não haja denúncia das partes protocolada com antecedência mínima de **120** (**cento e vinte**) **dias**, do término do período inicial ou do prorrogado.

CLÁUSULA TERCEIRA
DOS REQUISITOS GERAIS PARA A SOLUÇÃO EM APPLIANCE DE FIREWALL UTM

3.1. Solução integrada em um único equipamento, porém, de forma duplicada para a realização de cluster (cópia em trilha), para que em caso de falha de um equipamento, o outro entre em operação. A redundância deverá ser realizada através da interligação dos equipamentos de forma que em caso de indisponibilidade de um, o outro assumirá as mesmas propriedades e configurações diminuindo eventuais indisponibilidades. Para isto a Contratada deverá fornecer a solução sempre em duplicidade de equipamentos, softwares e serviços.

3.2. O sistema deverá estar licenciado para até, no mínimo, 1.000 (um mil) usuários conectados a ele e 200 (duzentas) VPNs, Webfilter, assinatura layer 7, gerador de relatórios gerenciais, IPS, antivírus de navegação, garantia de hardware e cluster e todos os demais recursos disponíveis no sistema que estiver sido ofertado na proposta comercial.

3.3. Não serão aceitas soluções baseadas em PC de uso geral.

3.4. Ser capaz de controlar permanentemente o tráfego de informações na rede de dados da Contratante, através da interligação dos links de internet.

3.5. Ser capaz de realizar o balanceamento de cargas dos links, tanto para o tráfego de entrada quanto para o tráfego de saída, permitindo que em caso de indisponibilidade de um link, os pacotes saiam ou entrem por outros links de internet disponíveis, além de permitir a otimização dos recursos de link.

3.6. Possibilitar a configuração das portas e dos protocolos de internet e regras de qualidade em no mínimo 10 (dez) portas de rede.

3.7. Fornecer suporte ao serviço de VPN - VPN IPsec ponto a ponto e VPN de acesso remoto - com boa performance e estabilidade.

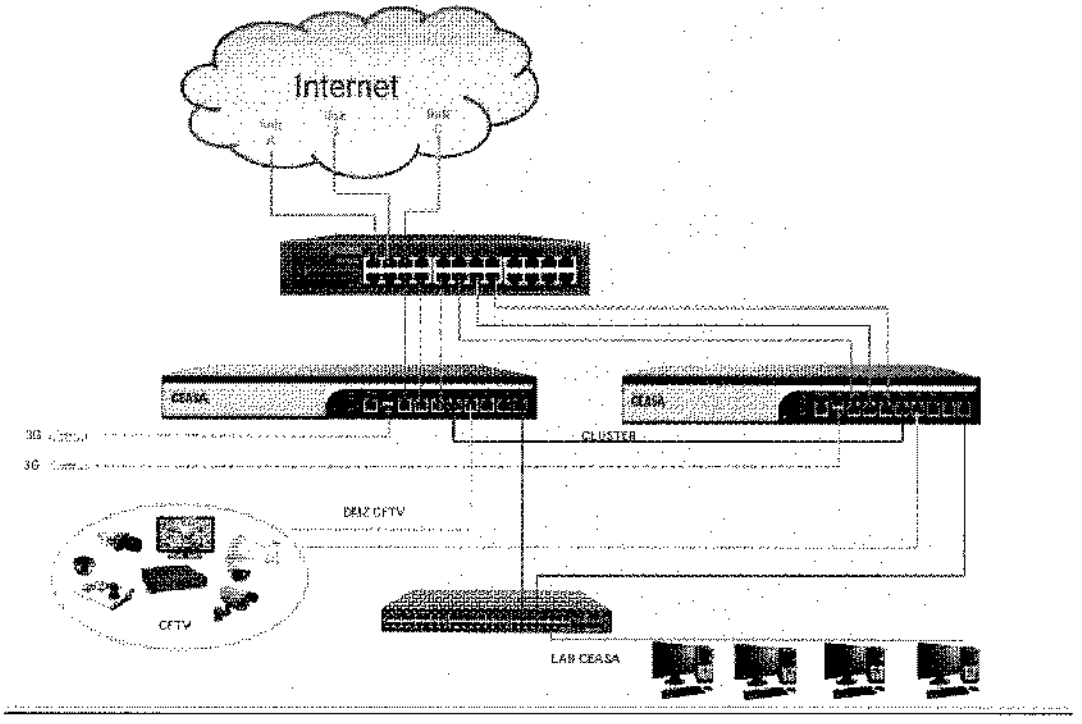
3.8. Fornecer suporte ao serviço de proxy, com integração com o Active Directory para facilitar o gerenciamento.

3.9. Possibilitar a geração de relatórios de utilização por usuários ou grupos, informando em tempo real ou períodos específicos, os endereços mais acessados, o tempo de navegação e consumo de tráfego da rede.

3.10. A Contratada deverá realizar toda a instalação e configurações iniciais na rede da Contratante, configurando as VPNs, NAT, DMZs, links, Load Balance, Fail Clustes, QoS, bem

como todas as regras de Firewall e proxy necessárias para o funcionamento adequado da solução.

3.11. A topologia da rede da CONTRATANTE está representada na figura abaixo:



CLÁUSULA QUARTA
DAS DESCRIÇÕES DOS SERVIÇOS

4.1. CONFIGURAÇÃO INICIAL:

4.1.1. A configuração inicial (setup) da solução consistirá na implantação dos equipamentos pela Contratada, nas dependências da Contratante, de forma a realizar a substituição dos sistemas atualmente em funcionamento na Contratante pelo sistema novo, sem impactos de indisponibilidade na rotina da Contratante.

4.1.2. A Contratada deverá encaminhar uma equipe técnica para avaliar previamente e organizar os trabalhos junto com a equipe de tecnologia da Contratante e, nas datas agendadas, realizar a implantação do sistema. A Contratada deverá realizar esta implantação com sua equipe técnica nas dependências da Contratante, não podendo alegar outros custos que não estejam apresentados no Contrato firmado entre as partes.

4.1.3. A solução será considerada implantada após ficar em execução pelo prazo de 15 (quinze) dias operacionais, sem interrupção na rotina da Contratante.

4.1.4. A configuração inicial deverá habilitar o sistema para funcionar conforme a topologia de rede apresentada, com as regras de Firewall, relatórios, QoS entre outras configurações.

Após o término do período de operação inicial, a equipe técnica da Contratante emitirá um Termo de Aceite para formalizar o término da implantação.

4.1.5. A Contratada não poderá apresentar quaisquer outros custos que não estejam definidos em contrato ou alegar desconhecimento de quaisquer eventuais impedimentos para a implantação.

4.2. DO TREINAMENTO (OPCIONAL):

4.2.1. Caso a Contratante julgue ser necessária a realização de treinamento, a Contratada deverá fornecer treinamento técnico sobre as soluções fornecidas, reconhecido pelo fabricante, conforme os requisitos a seguir:

4.2.1.1. O treinamento deverá ter parte teórica e prática, ser ministrado por profissional habilitado como instrutor e certificado para este fim, devidamente reconhecido pelo fabricante dos equipamentos.

4.2.1.2. A Contratada terá o prazo de 90 (noventa) dias consecutivos para realizar o treinamento, contados a partir da solicitação da Contratante.

4.2.1.3. O treinamento deverá ser ministrado para 02 (dois) funcionários da Coordenadoria de Informática da Contratante e deverá contemplar todo o conteúdo técnico necessário à certificação profissional, visando capacitá-los à instalação, configuração, gerenciamento, monitoramento, emissão de relatórios, suporte, diagnóstico, solução de problemas e incidentes aos equipamentos fornecidos.

4.2.1.4. Os certificados de participação deverão ser fornecidos pela Contratada em até 30 (trinta) dias após o treinamento.

4.2.1.5. O treinamento deverá ser realizado nas dependências da Contratada, ou em local por ela indicado;

4.2.1.6. Todas as despesas oriundas do treinamento (transporte, hospedagem, alimentação e material didático) são de inteira responsabilidade da empresa Contratada.

4.2.1.7. Caso a Contratante não venha utilizar o treinamento por qualquer motivo (opcional), o mesmo não poderá ser cobrado.

4.3. DO SUPORTE TÉCNICO:

4.3.1. Após a implantação inicial, a Contratada deverá fornecer suporte técnico, através de técnico remoto, via chat, telefone, acesso remoto, e-mail, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, durante a vigência do Contrato.

4.3.2. Em caso de indisponibilidade do sistema por causa de defeitos de peças ou outro problema em que a solução exija tempo superior a 24 (vinte quatro) horas, a Contratada deverá disponibilizar, em até 04 (quatro) horas, equipamento de backup, a ser retirado pela

Contratante, em local especificado pela Contratada, desde que não ultrapasse 120 (cento e vinte) quilômetros de distância da Contratante. Caso a distância seja superior a 120 (cento e vinte) quilômetros, a entrega do equipamento de backup será de responsabilidade da Contratada, sem custos adicionais para a Contratante, mesmo quando for necessário o transporte ou fretamento dos equipamentos, o translado e a estada de técnicos ou qualquer outro tipo de serviço necessário para garantir o cumprimento do serviço.

4.3.3. A Contratada tem o prazo de 24 (vinte e quatro) horas para disponibilizar o(s) equipamento(s) de backup após a abertura do chamado técnico.

4.3.4. Em caso de necessidade de visita técnica no local da Contratante, a empresa Contratada deverá apresentar orçamento prévio à Contratante e realizar o serviço somente após aprovação formal do orçamento.

4.4. DAS ESPECIFICAÇÕES TÉCNICAS:

4.4.1. DAS CARACTERÍSTICAS GERAIS DA SOLUÇÃO EM APPLIANCE DE FIREWALL/UTM:

4.4.1.1. Toda a solução de Firewall UTM e sistemas que possam ser necessários para atender esta especificação, deverá ser de um único fabricante. Não serão aceitas soluções oriundas de acordos (bundle) entre fabricantes distintos.

4.4.2. INTERFACE CLOUD:

4.4.2.1. A solução de Firewall UTM deverá permitir o acesso as informações do produto não somente através de um acesso direto ao seu painel, como também acesso à um servidor em Cloud que permita:

- ✓ Visualizar informações do produto em tempo real, como: processamento, memória, disco.
- ✓ Visualizar informações dos links conectados em tempo real como disponibilidade, latência e perda de pacotes.
- ✓ Visualizar em um painel único informações básicas de todos os Firewalls/UTM (em caso de existir mais de 1), em um mapa baseado no Google ou em formato de cartões.
- ✓ Ter funcionalidade de acessar o painel de login cada Firewall/UTM no momento que desejar.
- ✓ Ter possibilidade de ver informações de segurança, sendo uma delas referente a sua senha foi "vazada" em algum site que você possui cadastro usando o mesmo e-mail.
- ✓ Ter funcionalidade para cadastrar um website e/ou serviço e verificar se o mesmo está ativo (funcionamento) ou não.

4.4.3. INTERFACE WEB:

- ✓ Fornecer uma interface administrativa totalmente acessível via web (interface gráfica amigável).
- ✓ Configurar interface de rede.
- ✓ Configurar senha de acesso WEB.
- ✓ Reiniciar o equipamento com configuração padrão do fabricante.

- ✓ Reiniciar o sistema.
- ✓ Parar o sistema.
- ✓ Acessar o sistema operacional do equipamento (Shell).
- ✓ Lista de atividades do Firewall, tais como conexões, gateways nos quais as conexões estão saindo, regras que estão sendo aplicadas.
- ✓ Visualizar log de filtro do Firewall.
- ✓ Reiniciar serviço de acesso WEB.
- ✓ Acessar o sistema operacional como desenvolvedor (Developer Shell).
- ✓ Atualização via console.
- ✓ Habilitar acesso remoto via SSH.
- ✓ Efetuar download das dependências dos pacotes.
- ✓ Logout para acesso via SSH.
- ✓ Funcionalidade de ping.

4.4.4. DA PRIMEIRA INSTALAÇÃO:

4.4.4.1. A solução deverá permitir a utilização de um auxiliador de configuração (wizard) no caso de primeira instalação do sistema.

4.4.5. INTERFACE DE CONFIGURAÇÃO:

4.4.5.1. A interface administrativa deverá suportar o idioma português do Brasil.

4.4.5.2. Configuração do produto deverá ser através de interface WEB de fácil compreensão.

4.4.6. INTERFACES OU GRUPOS DE INTERFACES:

4.4.6.1. A solução deverá possuir grupos de interfaces administrativas (painéis de gerenciamento) que permitam a criação de regras que se aplicam a múltiplas interfaces sem duplicar as mesmas. Em caso de remoção de membros do grupo de interface, às respectivas regras do grupo não mais serão aplicadas àquela interface.

4.4.6.2. Deverá permitir a criação e uso de VLANs, no mínimo 4094 VLANs 802.1Q.

4.4.6.3. Deverá suportar o uso da tecnologia 3G conectados diretamente na solução firewall UTM, com as configurações de conexão das operadoras brasileiras pré-configuradas.

4.4.7. FIREWALL:

4.4.7.1. A solução terá que ter no mínimo as seguintes características relacionadas ao sistema de firewall:

- ✓ Filtragem por origem e IP de destino, porta de origem do protocolo, e destino IP para o tráfego TCP e UDP.
- ✓ Capacidade de limitar as conexões simultâneas com base em regras.
- ✓ Opção de gravar log do tráfego correspondente a cada regra.
- ✓ Possibilidade de alterar o gateway da regra de firewall para balanceamento de carga, failover, WAN múltipla.

4.4.7.2. Permitir agrupamento e designação de IPs, redes e portas para manter o conjunto de regras de firewall limpa e de fácil compreensão. Terá que atuar com espaços reservados para hosts, redes e portas reais.

4.4.7.3. Permitir a criação de regras para os mais diferenciados tipos de redes. Definir diversas interfaces e protocolos, como TCP, UDP, TCP/UDP, ICMP, ESP, AH, GRE, IGMP.

4.4.7.4. Permitir fonte OS, Diff code point (mecanismo para fornecer qualidade de serviço), TCP Flags, Tipo de estado.

4.4.7.5. Camada 2 transparente com as seguintes opções:
- ✓ Permitir fazer bridge das interfaces.
- ✓ Permitir normalização de pacote, a fim de garantir que não haja ambiguidades na interpretação pelo destino final do pacote. Também remonta pacotes fragmentados, protegendo alguns sistemas operacionais de algumas formas de ataque e descartando pacotes TCP que têm combinações de flag inválidas.

4.4.7.6. State Table com as seguintes opções:
- ✓ Permitir controle granular (ou regular) da tabela de estado (State Table) com estados e tamanhos ajustáveis, baseado em regras.
- ✓ Limite de conexões simultâneas de cliente.
- ✓ Limite de estados por host.
- ✓ Limite de novas conexões por segundo.
- ✓ Tempo limite de estado.
- ✓ Por tipo de estado.

4.4.7.7. Tipo do Estado com as seguintes opções:
- ✓ Manter estado ativo - Funcionando com todos os protocolos.
- ✓ Modular o estado - Funcionando apenas com o TCP.
- ✓ Synproxy - Filtrando conexões TCP para ajudar a proteger servidores de inundações SYN TCP.

4.4.7.8. State Table - tem que permitir as seguintes opções de otimização:
- ✓ Normal.
- ✓ Alta latência.
- ✓ Expirar conexões ociosas com maior tempo
- ✓ Expirar conexões inativas mais rapidamente.
- ✓ Tenta evitar o descarte de conexões legítimas.

4.4.7.9. Bloqueio por país/região:
- ✓ Permitir efetuar bloqueio a conexões recebidas por determinada região.
- ✓ O bloqueio terá que ser feito por país selecionando através de uma interface WEB e os países separados por continentes, não precisando selecionar os IPs de cada país.
- ✓ Exibir a quantidade de bloqueios que foi efetuado de cada país através de um Dashboard.

- ✓ Permitir no mínimo as seguintes configurações:
  - Opção para habilitar log.
  - Configurar interface de entrada.
  - Ação a ser feita na interface de entrada (block ou reject).
  - Configurar interface de saída.
  - Ação a ser feita na interface de saída (block ou reject).

- ✓ Para configuração de listas personalizadas terá que permitir no mínimo definir:
  - Nome do alias, descrição, inserção de uma lista no formato ".gz" ou ".txt" proveniente de um link na internet.
  - Ações permitidas na lista, tais como: bloqueio de entrada, bloqueio de saída, bloqueio de entrada e saída, permitir entrada, permitir saída ou nenhuma ação.
  - Frequência de atualização: nunca, a cada 1 hora, a cada 4 horas, a cada 12 horas ou uma vez por dia.
  - Permitir inserir as faixas de rede manualmente.
  - Permitir configuração tipo "Top Spammers" e o produto terá que listar um ranking com os países conhecidos como os maiores Spammers da internet. Esta configuração terá que permitir o selecionar o país e a ação como: bloqueio de entrada, bloqueio de saída, bloqueio de entrada e saída, permitir entrada, permitir saída ou nenhuma ação.
  - Possuir opção de configuração para cada continente tal como: África, Ásia, Europa, América do Norte, Oceania, América do Sul com a lista de países e quantidade de range de IPs de cada país.
  - Configuração como opcional sincronismo destas regras no caso de Cluster.

4.4.8. REDIRECIONAMENTO DE PORTAS:

4.4.8.1. Permitir criar regras de redirecionamento de portas. Uma forma de informar ao equipamento, que destino dar aos pacotes.

4.4.9. NAT (Network Address Translator):

4.4.9.1. O equipamento deverá fazer a comunicação entre os hosts da rede interna e a internet, traduzindo os IPs, com as seguintes características:

- ✓ Encaminhamento de portas incluindo faixas de rede e o uso de múltiplos IPs públicos.
- ✓ NAT para IPs individuais ou sub-redes inteiras.
- ✓ NAT de saída.
- ✓ NAT de saída avançado - permitindo que seu comportamento padrão seja desativado e permitindo a criação de múltiplas flexões de regras de NAT.
- ✓ NAT Reflection - possibilitando que os serviços possam ser acessados por IP público a partir de redes internas.

4.4.10. RULES OU REGRAS:

4.4.10.1. Permitir criação de regras para os mais diferenciados tipos de redes. Definir diversas interfaces e protocolos, como TCP, UDP, TCP/UDP, ICMP, ESP, AH, GRE, IGMP, entre outros.

4.4.11. IGMP PROXY:
4.4.11.1. Permitir fazer proxy do protocolo IGMP entre segmentos de rede.

4.4.11.2. Permitir configurar as redes, bem como interface de upstream e downstream.

4.4.12. RECURSOS AVANÇADOS DE CRITÉRIOS DE REGRAS DE FIREWALL:
4.4.12.1. Permitir fonte OS, Diff code point (mecanismo para fornecer qualidade de serviço), TCP Flags, Tipo de estado, Layer7, entre outros.

4.4.13. UPNP & NAT-PMP:
4.4.13.1. Permitir suporte ao protocolo Universal Plug and Play (UPnP) e NAT Port Mapping Protocol (NAT-PMP), podendo configurar download e upload máximo caso necessário.

4.4.14. WAKE ON LAN:
4.4.14.1.1 Possuir suporte para ser configurado o serviço de Wake on LAN, através de suporte no hardware, com objetivo de ligar o computador através de um pacote específico de rede.

4.4.15. AUTO UPDATE:
4.4.15.1. Possuir suporte para atualização automática, da base do sistema, sempre que existir alguma disponível.

4.4.16. AGENDAMENTOS DE REGRAS:
4.4.16.1. Permitir criação de tabela de horários para agendamento de regras.

4.4.16.2. Permitir vincular uma regra a uma agenda definida para que as mesmas vigorem a partir de ou durante datas e horários previamente especificados.

4.4.16.3. Permitir a criação das tabelas de horários pelo administrador do sistema, bem como suas variações.

4.4.17. TRAFFIC SHAPER / QoS / GERENCIAMENTO DE BANDA:
4.4.17.1. Fornecer uma suíte de gerência de tráfego de rede.

4.4.17.2. Possibilitar a criação de regras dos seguintes tipos:
- ✓ Priorização de tráfego, definindo quais protocolos possui prioridade.
- ✓ Limite de tráfego por protocolo, definindo qual limite máximo de um protocolo.
- ✓ Reserva de tráfego com empréstimo em caso de não estar sendo utilizado em seu limite.

4.4.17.3. Permitir a criação de diversas filas onde cada fila tem seu grupo de configuração.

4.4.17.4. A configuração poderá ser definida por interface, por fila ou layer7.

4.4.17.5. Permitir a verificação e consumo de filas em tempo real através do painel WEB, ou modo texto acessando por SSH.

4.4.18. DHCP RELAY:
4.4.18.1. Oferecer serviço de DHCP sem necessariamente possuir um servidor DHCP instalado em sua rede.

4.4.18.2. Permitir que o DHCP Relay encaminhe requisições para um servidor definido em outro segmento.

4.4.19. DHCP SERVER:
4.4.19.1. Dispor de servidor DHCP.

4.4.19.2. Atribuir endereços IPs e configurações relacionadas aos dispositivos da rede.

4.4.19.3. Permitir DNS Forwarder para auxiliar o servidor DNS a consultar nomes na internet.

4.4.20. DNS DINÂMICO:
4.4.20.1. Permitir uso de DNS dinâmico para que você possa registrar seu endereço IP público com um número de prestadores de serviços de DNS dinâmico comumente usados para conectar-se à VPNs, Web Servers e Mail Servers, podendo ser usado conta em serviço de terceiros no mínimo as seguintes opções: DynDNS, No-IP, OpenDNS, ZoneEdit e DyNS.

4.4.20.2. Um cliente também terá que ser disponibilizado para RFC 2136 com atualizações dinâmicas de DNS, para uso com servidores DNS BIND que suportam este meio de atualização.

4.4.21. LOGS:
4.4.21.1. Permitir gravar logs separando pelas seguintes categorias:

- ✓ Log do sistema
- ✓ Firewall
- ✓ DHCP
- ✓ Autenticação
- ✓ IPSec
- ✓ PPP
- ✓ VPN
- ✓ Load Balancer
- ✓ OpenVPN
- ✓ NTP

4.4.21.2. Permitir gravar logs em servidor externo, podendo configurar até 03 (três) servidores.

4.4.22. ENVIO DE INFORMAÇÕES POR E-MAIL:

4.4.22.1. Permitir o envio pré-programado de informações referente ao status do link permitindo selecionar o gráfico.

4.4.22.2. Permitir enviar e-mail informando quando houver queda de link.

4.4.23. GERENCIAMENTO DE CERTIFICADOS:

4.4.23.1. Permitir o gerenciamento de certificados através de modo gráfico.

4.4.23.2. Permitir criar novos certificados através do painel web, caso necessário.

4.4.23.3. Permitir revogar certificados existentes través do painel web.

4.4.24. CONTROLE DE PERMISSÃO DE ACESSO:

4.4.24.1. Permitir efetuar controle de permissão para acesso a algumas funcionalidades.

4.4.25. MÓDULO DE DIAGNÓSTICO:

4.4.25.1. Possuir um módulo de diagnóstico com no mínimo as seguintes ferramentas:

- ✓ Verificação da tabela ARP
- ✓ Autenticação
- ✓ Backup/Restore
- ✓ Histórico de configurações
- ✓ DNS Lookup
- ✓ Edição de arquivo
- ✓ Voltar configuração do fabricante
- ✓ Desligar sistema
- ✓ Informações referentes a limites do sistema
- ✓ Captura de pacotes
- ✓ Tabela de roteamento e tabela de estado
- ✓ Atividades do sistema (CPU, Memória, Throughput)
- ✓ Ping
- ✓ Traceroute

4.4.26. GERENCIAMENTO DE LINK/BANDA DE INTERNET:

4.4.26.1. Load Balance - Balanceamento de Saída:

- ✓ Permitir distribuir carga entre duas ou mais interfaces WAN.
- ✓ O número de interfaces Wan que podem ser usadas para Load balancing deve ser limitada a quantidade de interfaces do equipamento.
- ✓ Não limitar o número de interfaces para serem balanceadas.
- ✓ O serviço de Load Balancer também terá que prover automaticamente serviço de Failover.
- ✓ Fornecer balanceamento de carga de saída com múltiplas conexões WAN para fornecer balanceamento de carga e failover.
- ✓ Permitir o direcionamento do tráfego para o gateway desejado ou para o pool de balanceamento de carga em uma base de regras por firewall.

- ✓ Permitir configurar sensibilidade para definição de queda ou não do link com no mínimo opção de latência ou perda de pacotes.
- ✓ Permitir configurar qual será o ponto de verificação para análise da latência do link ou queda.
- ✓ Permitir configurar a tolerância de perda de pacotes e latência do link para considerar o link como "down".
- ✓ Permitir configurar o peso de cada link no momento do balanceamento para decisão de quantos pacotes enviar para cada link.

4.4.26.2. Load Balance - Balanceamento de Entrada:

- ✓ Permitir balanceamento de carga de entrada ou failover.
- ✓ Permitir distribuir a carga entre vários servidores, podendo ser usado com servidores web, servidores de e-mail e outros.
- ✓ Permitir que os servidores que não respondem às solicitações ping ou conexões de porta TCP sejam removidos do pool.

4.4.27. OPENNTPD:

4.4.27.1. Possibilitar a sincronização de horário do equipamento utilizando protocolo NTP.

4.4.27.2. Possibilitar a instalação de um servidor NTP dentro do Firewall, permitindo selecionar as redes no qual ele irá monitorar o serviço.

4.4.28. OLSR:

4.4.28.1. Possuir suporte, através de um serviço do sistema operacional para Optimized Link State Routing Protocol.

4.4.29. NETFLOW:

4.4.30. Permitir a utilização do protocolo Netflow versão 1, 5 ou 9 para envio de informações referente à tráfego/link, permitindo configurar no mínimo: IP de destino, porta, IP de origem e restrição de direção.

4.4.31. RIP:

4.4.31.1. Permitir a utilização do protocolo RIP 1 e 2, permitindo configurar a interface e a senha.

4.4.32. OSPF:

4.4.32.1. Permitir a utilização do protocolo OSPF caso necessário, permitindo configurar a área ou não do padrão RFC 1583.

4.4.33. SNMP:

4.4.33.1. Suportar a utilização do protocolo SNMP.

4.4.34. GRÁFICOS:

4.4.34.1. Possuir no mínimo os seguintes gráficos:

- ✓ Sistema - Gráficos diários, semanais, mensais e anuais de:

- Memória
- Throughput
- Processador

✓ Tráfego - Gráficos diários, semanais, mensais e anuais de:
- Links
- VPNs
- Consumo total

✓ Qualidade dos links - Gráficos diários, semanais, mensais e anuais de:
- Latência
- Perda de pacote
- Quedas

✓ Pacotes:
- Customização de gráficos, caso necessário.

4.4.35. PPPOE SERVER:

4.4.35.1. Permitir a configuração de um servidor PPPoE Server no equipamento.

4.4.35.2. Permitir uso de servidor PPPoE com base local de dados de usuários podendo ser usada para autenticação.

4.4.35.3. Permitir autenticação RADIUS por conta fixando IP por usuário autenticado.

4.4.35.4. Permitir caso necessário acessar um servidor PPPoE para ativar algum link.

4.4.36. VPN:

4.4.36.1. Permitir no mínimo as seguintes opções de VPN: IPsec, OpenVPN, PPTP e o L2TP:

✓ IPsec
- Permitir uso de VPN IPsec.

✓ OpenVPN
- Permitir configuração de OpenVPN.
- Permitir uso de VPN com outros equipamentos.
- Permitir uso de OpenVPN através de cliente instalado em estações de trabalho Windows.
- No caso de uso das estações de trabalho Windows, a solução terá que gerar de maneira simples e via console de administração o software cliente.
- No caso do uso do cliente acima citado, o mesmo terá que ser gerado sem custo de licença e sem limites de quantidades.
- Permitir o modo servidor de OpenVPN com no mínimo as seguintes variações: Peer to Peer (SSL/TLS), Peer to Peer (chave compartilhada), Acesso remoto

(SSL/TLS), Acesso Remoto (Autorização Usuário), Acesso Remoto (SSL/TLS + Autorização Usuário).
- Permitir pelo menos 60 (sessenta) algoritmos de criptografia.
- Permitir compactação de pacotes utilizando algoritmo LZO.
- Fornecer suporte a VPN L2TP.
- Fornecer suporte a VPN PPTP Server com opção de base local ou autenticação Radius.
- Possuir a funcionalidade de enviar e-mail sempre que:
  - Algum usuário se conectar na VPN utilizando protocolo OPENVPN;
  - Algum usuário desconectar na VPN utilizando protocolo OPENVPN;
  - Permitir a gravação de logs das conexões VPNs, em banco de dados, informando o endereço IP de origem, tempo de conexão e tráfego total.

4.4.37. REDUNDÂNCIA DE EQUIPAMENTOS (CLUSTER):

4.4.37.1. Todos os equipamentos deverão suportar o funcionamento em modo "Cluster" e todas as licenças para seu uso deverão estar inclusas no fornecimento.

4.4.37.2. Permitir a configuração de 02 (dois) ou mais firewalls como um grupo de "failover", se uma interface falhar no primário ou ficar "off-line" completamente, o secundário se torna ativo, sem qualquer prejuízo de parada ou interrupções de atividade de operação (quantidade de usuários, conexões simultâneas, troughput, etc.) especificadas no dimensionamento.

4.4.37.3. Possuir capacidade de sincronização de configuração, para que as alterações de configuração no firewall UTM primário sincronizem automaticamente com o firewall UTM secundário.

4.4.37.4. Garantir que a tabela de estado do "firewall" seja toda replicada para todos os firewalls configurados de "failover", isso significa que as conexões existentes serão mantidas, no caso de falha, o que é importante para prevenir interrupções de rede.

4.4.37.5. Permitir que seja configurado quais os módulos serão sincronizados através do protocolo de cluster.

4.4.37.6. Permitir que em caso de queda de um firewall UTM, o outro assuma de modo que as conexões não sejam interrompidas.

4.4.38. BACKUP/RESTORE:

4.4.38.1. Fornecer uma ferramenta para realizar cópias seguras de seus dados, com no mínimo as seguintes configurações:
- ✓ Selecionar qual a área de backup (todos, sistema, regras de firewall, NAT, etc).
- ✓ Fazer ou não backup das configurações de pacotes instalados no equipamento.
- ✓ Permitir fazer backup dos gráficos do sistema.
- ✓ Permitir efetuar backups agendados.

BANCO MUNICIPAL ALIMENTOS CAMPINAS
DEPARTAMENTO JURÍDICO DA CEASA CAMPINAS
ISA
CEASA - Mariana Romão - Jurídico OAB/SP nº 163.859

4.4.39. GRÁFICOS ESTATÍSTICOS, MONITORAMENTO E RELATÓRIOS:

4.4.39.1. Fornecer tela de Dashboard na qual o administrador de redes poderá ter uma visão geral de todas as funcionalidades do equipamento.

4.4.39.2. O Dashboard terá que ser totalmente customizável e na forma de Widgets como monitoramento de diversos serviços.

4.4.39.3. Fornecer relatório e gráficos de pelo menos os seguintes itens:

- ✓ Gráficos de uso de CPU
- ✓ Gateways
- ✓ Gráficos de tráfego e Throughput total da rede
- ✓ Status dos serviços e estados do firewall
- ✓ Serviços instalados
- ✓ Load Balancer
- ✓ Throughput individual para cada interface
- ✓ Taxa de pacotes por segundo para todas as interfaces
- ✓ Tempo de resposta de ping do Gateway da interface WAN
- ✓ Filas de Traffic Shapper em sistemas com o serviço habilitado
- ✓ Bloqueio por país
- ✓ Quantidade de dispositivos conectados em tempo real
- ✓ Informações em tempo real:
  - Disponibilizar gráficos e mostrar o throughput em tempo real para cada interface.
  - Fornecer para usuários com traffic shaper a tela de status de filas QoS em tempo real de uso de fila, usando medidores atualizados.
  - O Dashboard terá que exibir medidores em tempo real do uso da CPU, memórias swap e utilização do disco e tamanho da tabela de estado.
  -
- ✓ Relatórios de Web Filter:
  - Disponibilizar, em tempo real, o relatório dos sites acessados pelos usuários, mostrando informações como horário do acesso, URL acessada, ação do Proxy, categoria da URL, nome do usuário e grupo do usuário.
  - Permitir filtro por palavra chave e também marcação dos itens liberados ou bloqueados, para facilitar a análise.

4.4.40. UPGRADE / ATUALIZAÇÃO:

4.4.40.1. Permitir a atualização através da interface administrativa WEB ou através da interface Console, de maneira simples e intuitiva.

4.4.40.2. Permitir a atualização de:

- ✓ Pacotes considerados estáveis;
- ✓ Pacotes considerados como versão BETA, com objetivo de aplicação de correções rápidas para resolução de bugs críticos.

4.4.41. GERENCIAMENTO SIMPLIFICADO:

4.4.41.1. Possuir módulo de gerenciamento simplificado que possua sistemas pré-configurados e atualizados diariamente, comuns para liberação ou bloqueio em uma rede considerada comum, tais como: Apple, Banco do Brasil, Conectividade Social, Java, Microsoft, NFE, Microsoft Remote Desktop, VPN PPTP, VPN IPSEC, MP3 Streaming, IRC, JABBER, DNS, www (HTTP/HTTPS), Email (SMTP), Email (POP3), Ping (ICMP), Email (IMAP), Microsoft SMB, Realtime Streaming Protocol (RTSP), Simple network management protocol (SNMP), virtual network control (VNC), ICQ, Lotus Notes, MSN Messenger, Server Database (Mysql), NNTP, Symantec PC Anywhere, Team Speak, CVS, HBCI, SlingBox, File Transfer Protocol (FTP).

4.4.41.2. O mesmo terá que ocorrer para configurações de QoS para protocolos como VOiP, ERP TOTVs entre outros.

4.4.41.3. O módulo terá que alterar configurações de Webfilter e Firewall ao mesmo tempo, caso necessário.

4.4.42. CAPTIVE PORTAL / ADMINISTRAÇÃO DE VISITANTES:

4.4.42.1. Permitir gerenciamento de visitantes para acesso à rede via hot spot ou redes sem fio.

4.4.42.2. Solicitar autenticação para usuários visitantes.

4.4.42.3. Permitir a criação de regras específicas para esse grupo de visitantes.

4.4.42.4. Permitir a criação de regras de firewall, bloqueios e controles diferentes da rede para usuários autenticados como visitantes.

4.4.42.5. Permitir no mínimo os seguintes recursos para o Portal Captive:

- ✓ Máximo de conexões simultâneas;
- ✓ Tempo limite de ociosidade;
- ✓ Tempo limite rígido;
- ✓ Logon por janela de pop-up;
- ✓ Redirecionamento de URL após a autenticação onde os usuários podem ser redirecionados para a URL definida;
- ✓ Filtragem MAC.

4.4.42.6. Opções de Autenticação - fornecer pelo menos as seguintes opções de autenticação:

- ✓ Nenhuma autenticação;
- ✓ Gerenciador de usuários locais;
- ✓ De autenticação RADIUS - Pode ser usado para autenticar a partir do Microsoft Active Directory e vários outros servidores RADIUS.

4.4.42.7. Capacidades de RADIUS:
- ✓ Forçar a re-autenticação;
- ✓ Capacidade de enviar atualizações às contas;
- ✓ RADIUS MAC para permitir que o Captive Portal autentique em um servidor RADIUS usando o endereço MAC do cliente como nome de usuário e senha;
- ✓ Permitir a configuração de servidores RADIUS redundantes;
- ✓ Permitir a configuração da página inicial do Captive Portal para usar HTTP ou HTTPS;
- ✓ Permitir a passagem de endereços MAC e IP - MAC e endereços IP devem poder ser listados para ignorarem o portal;
- ✓ Permitir o upload de imagens para uso em páginas do portal.

4.4.43. SERVIÇOS:
4.4.43.1. Permitir a instalação de serviços conforme demanda.

4.4.43.2. Será definido pelo administrador se deseja ou não instalar um serviço a fim de economizar recursos de hardware.

4.4.43.3. Permitir no mínimo as seguintes funcionalidades referentes a serviços:
- ✓ Instalação;
- ✓ Reinstalação total do pacote;
- ✓ Remoção do pacote;
- ✓ Atualização do pacote.

4.4.44. WEBFILTER / PROXY:
4.4.44.1. Permitir a escolha de trabalhar com proxy transparente ou autenticado.

4.4.44.2. Permitir que o equipamento utilize um proxy externo.

4.4.44.3. Gerenciar a política de cache com: tamanho de espaço em disco utilizável, sistema de cache utilizado, localização do diretório do cache, quantidade de memória utilizável pelo cache, tamanho mínimo e máximo de arquivo de cache, tamanho máximo de arquivo alocado na memória RAM para o cache e não armazenar cache.

4.4.44.4. Permitir exceções e bloqueios para o proxy, como: sub-redes permitidas, IPs que não serão filtrados, IPs banidos pelo proxy e sites que terão acesso liberado pelo proxy.

4.4.44.5. Limitar banda para hosts ou extensões como: tamanho máximo de arquivo para download, tamanho máximo para upload, limite de banda global para os hosts e limite de banda para determinadas extensões de arquivos.

4.4.44.6. Permitir autenticação dos usuários através de: base local, LDAP, Active Directory (AD), RADIUS, NTdomain e Single-Sign-on.

4.4.44.7. Permitir gerenciamento de acesso a páginas por categoria.

4.4.44.8. Fornecer listas de categoria atualizadas diariamente.

4.4.44.9. A alimentação das URL´s pertinentes a cada categoria terá que ser automática e no mínimo diária.

4.4.44.10. A base de URL´s deve conter no mínimo 2 bilhões de sites catalogados.

4.4.44.11. A base de URL´s deve conter no mínimo 48 categorias.

4.4.44.12. Permitir a criação de categorias personalizadas sem limite de quantidades.

4.4.44.13. Permitir a criação de lista brancas/negras como exceções.

4.4.44.14. Redirecionar as páginas bloqueadas para uma URL específica e personalizada da instituição, bem como pode manter a página padrão do equipamento.

4.4.44.15. Permitir de forma simples o agendamento de período em que uma regra entrará em vigor, definindo data e horário o para que isto aconteça.
Fornecer a possibilidade de armazenar log em um servidor de banco de dados externo MySQL.

4.4.44.16. Permitir o agendamento de backup dos logs e das configurações do webfilter.

4.4.44.17. Permitir o agendamento da limpeza dos logs do webfilter.

4.4.44.18. Possuir módulo de diagnóstico de bloqueio ou liberação de URL por usuário, mostrando qual regra está permitindo ou bloqueando o acesso.

4.4.44.19. Permitir o bloqueio ou liberação do múltiplo login por usuário.

4.4.44.20. Permitir visualizar através do painel administrativo os acessos em tempo real, mudando a cor do acesso de acordo com a ação (bloqueio ou liberação).

4.4.44.21. Possuir uma opção de liberação de acesso em caso de justificativas no momento do bloqueio do acesso ao usuário. Caso o usuário deseje, acessar mesmo após o bloqueio, o mesmo terá que justificar. O equipamento terá que:

- ✓ Liberar automaticamente caso esteja configurado para o mesmo;
- ✓ Inserir a justificativa em uma "fila" de desejos de acesso pelo usuário, que somente o administrador poderá liberar ou manter bloqueado o acesso.

4.4.45. RELATÓRIOS - RELATÓRIOS DE NAVEGAÇÃO (PROXY):

4.4.45.1. Fornecer uma suíte de relatórios simples e de fácil utilização para ser acessado ou disponibilizado para administradores da solução.

4.4.45.2. Permitir a personalização da marca estampada no cabeçalho do relatório.

4.4.45.3. Será permitido suíte de relatórios na mesma interface desde que com acesso restrito e de fácil utilização.

4.4.45.4. Em caso da suíte de relatórios for um aplicativo a parte o mesmo terá que ser multiplataforma, sendo possível ser instalado em Windows, Linux e MAC com funcionamento externo ao produto.

4.4.45.5. Permitir cadastrar quantos Firewall/UTM desejar.

4.4.45.6. Gerar relatórios de navegação referentes a usuários, domínios ou relatórios resumidos com pelo menos as seguintes características:

- ✓ Acessos por Usuários - Sintético;
- ✓ Acessos por Usuários - Analítico;
- ✓ Consumo de Link por Usuário;
- ✓ Acessos por IP - Sintético;
- ✓ Acessos por IP - Analítico;
- ✓ Consumo de Link por IP;
- ✓ Atividades por Usuários;
- ✓ Atividades por IP;
- ✓ Sites mais acessados - Sintético;
- ✓ Sites mais acessados - Analítico;
- ✓ Consumo de Link por Site e Sites por usuários;
- ✓ Acessos por categoria e Consumo de link por categoria;
- ✓ Quantidade de acessos por IP sintético ou analítico;
- ✓ Duração da conexão de VPN por usuário;
- ✓ Consumo de banda por usuário de VPN;
- ✓ Duração da conexão de VPN por IP;
- ✓ Consumo de banda por IP de VPN;
- ✓ Informações gerais;
- ✓ Relatório resumido que informa o consumo total de banda utilizado pelo Proxy;
- ✓ Todos os relatórios anteriores podem ser gerados pelo menos nos seguintes formatos: PDF, RTF, DOCX, XLSX, CVS, Jasper Reports (jrprint), HTML e HTM, ODT e XML;
- ✓ Todos os relatórios devem permitir gerar gráficos (pizza e barra).

4.4.46. IDS/IPS:

4.4.46.1. Fornecer um sistema de detecção e prevenção de intrusão com capacidade de inspecionar o payload do pacote, fazendo o registro dos pacotes, além de detectar as invasões. Capaz de detectar quando um ataque está sendo realizado e, baseado nas características do ataque, alterar ou remodelar sua configuração de acordo com as necessidades, além de permitir a configuração de avisos ao administrador do ambiente sobre o ataque.

4.4.46.2. A solução de IDS/IPS terá que permitir configurar limite de log.

4.4.46.3. A solução de IDS/IPS terá que permitir configurar alertas.

3.4.46.4. Permitir registrar através de um cadastro denominado Whitelist as redes ou IPs dos computadores que o IDS/PS não aplicará as suas regras de bloqueio.

4.4.47. MÓDULO DE GARANTIA DE DISPONIBILIDADE ENTRE MATRIZ E FILIAIS:
4.4.47.1. Possuir um módulo com objetivo de automatizar as regras necessárias para conexão da matriz com filiais garantindo alta disponibilidade.

4.4.47.2. Possuir uma interface na matriz que permita visualizar todas as VPNs conectadas entre a matriz e todas as filiais, com sinalizações fáceis para identificar status das conexões.

4.4.48. SUPORTE A PROTOCOLO BGP:
4.4.48.1. Fornecer suporte ao protocolo BPG segundo RFC 4271.

4.4.48.2. O protocolo BGP terá que ser capaz de trabalhar até mesmo sob túneis VPN caso necessário.

4.4.48.3. Em caso de failover configurado através do protocolo BGP, o sistema terá que manter conexões ativas caso ocorra queda em algum link e o outro link esteja em perfeito funcionamento e possua tamanho de banda.

4.4.48.4. As conexões de alguns protocolos tais como: VoiP e alguns sistemas de banco de dados e ERP deverão permanecer ativas mesmo em caso de queda de um dos links.

4.4.49. ANTIVÍRUS DE NAVEGAÇÃO:
4.4.49.1. HTTP Antivírus para scanner vírus para todo download que for efetuado.

4.4.49.2. A solução deverá fornecer todas as licenças para o antivírus embarcado no equipamento.

4.4.50. USO DE REDE:
4.4.50.1. Fornecer modo interativo, onde mostra o status da rede no terminal do usuário. No modo web, atuando como servidor web, criando um dump em HTML do status da rede.

4.4.50.2. Suportar NetFlow/sFlow emissor/coletor em uma interface cliente baseada em HTML para criar aplicações de monitoramento ntop-centric, e RRD para estatísticas de tráfego de armazenamento persistentes.

4.4.51. HARDWARE:
Deverão ser disponibilizadas 02 (duas) unidades de Appliance de Firewall com Gerenciamento Unificado de Ameaças (UTM - Unified Threat Management) para suportar os serviços acima descritos e os mesmos devem possuir as seguintes características técnicas mínimas:

Item	Quantidade	Descrição Técnica
Tamanho	Rack 19"	Com acessórios para fixação inclusos
Altura	1U	Máximo
Memória RAM	4GB	DDR3
Número de Interface de Rede	10 (dez)	Giga
Processador	1 (um)	2.4GHz - Núcleo Duplo
Interfaces USB para modens externos	2 (duas)	3.33 ou superior
Interface USB para outros usos (frontal)	2 (duas)	2.0 ou superior
Fonte de Alimentação	1 (uma) Interna	Full Range 110/220V
Conector VGA	1 (um)	
Display de cristal líquido com informações de estado e IP do equipamento	1 (um)	
Slot de Expansão PCI	1 (um)	Adaptador Riser
Botão de Power no painel frontal ou traseiro	1 (um)	-
Storage	1 (um)	500GB para disco único ou 100GB com servidor de log remoto instalado e configurado sem ônus adicionais para a Contratante.
Capacidade de usuários conectados simultaneamente e licenciado	1000 (um mil)	Fornecimento das licenças

<u>OBS.:</u> Não serão aceitos hardwares montados e/ou customizados com interfaces de rede que não sejam integradas a motherboard.

4.4.52. TOPOLOGIA DE REDE:

4.4.52.1. A solução deverá ser configurada inicialmente nas dependências da Contratante da seguinte forma:

- ✓ LINKS DE ENTRADA
  - Link Privado Dedicado Full
  - Link Rádio
  - Link ADSL
  - Link Modem

- ✓ DMZ
  - DMZ - CFTV
  - DMZ - DVR
  - DMZ - SERVIDORES

- ✓ Preservação das regras atuais
  - A solução deverá aceitar e ser configurada com as regras atuais da Contratante.

4.4.53. SUPORTE, INSTALAÇÃO E LICENCIAMENTO:

4.4.53.1. Todas as soluções que envolvam hardware e software, a serem implementadas no ambiente tecnológico da Ceasa/Campinas deverão ser fornecidas com garantia do fabricante dos produtos, por um período mínimo de 12 (doze) meses, a partir da data da entrega, mediante a assinatura do Termo de Recebimento emitido pela Contratada.

4.4.53.2. A garantia contratual cobre o reparo e a substituição gratuita das partes, peças e componentes do produto que venham apresentar defeitos e/ou vícios; defeitos decorrentes de projeto, fabricação, construção ou montagem, inclusive atualizações corretivas dos softwares (firmwares e drivers) fornecidos com os equipamentos, compreendidas aquelas disponibilizadas pelo fabricante durante o período de garantia.

4.4.53.3. A Contratada irá reinstalar ou substituir por outro novo, sem custos adicionais para a Contratante, qualquer equipamento defeituoso, objeto deste contrato, no prazo de 10 (dez) dias úteis contados do recebimento de carta emitida pela Contratante.

4.4.53.4. A Contratada disponibiliza canal de comunicação com o fabricante dos produtos para abertura e acompanhamento de chamados em tempo integral (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados), possibilitando suporte a dúvidas e esclarecimentos relativos à utilização e configuração das funcionalidades relacionadas a cada software e componentes da solução.

4.4.53.5. A Contratante poderá efetuar um número ilimitado de chamados de suporte técnico durante a vigência do Contrato para suprir suas necessidades de utilização dos softwares, sem ônus adicional.

4.4.53.6. Caso necessário, a Contratada poderá fazer atendimento on-site e o mesmo poderá ser cobrado mediante aviso prévio a ser encaminhado e aprovado pela Contratante.

CLÁUSULA QUINTA
DO PRAZO DE ENTREGA

5.1. Os equipamentos deverão ser instalados e configurados nas dependências da Contratante no prazo máximo de 60 (sessenta) dias corridos a partir da data de assinatura do Contrato.

5.2. Caso os equipamentos sejam rejeitados, a Contratada deverá, no prazo máximo de 15 (quinze) dias úteis, contados da notificação pelo Gestor do Contrato - Coordenadoria de Informática - AII, para nova entrega livre das causas de rejeição.

5.2.1. Caso novos equipamentos entregues em substituição aos rejeitados sejam também objeto de rejeição, ficará demonstrada a incapacidade técnica da Contratada de prestar o serviço nas condições e especificações contratuais pactuadas e sujeitá-la-á as penalidades

previstas na letra d do item 13.1 deste Contrato.

4.2.2. Caso não ocorra o atendimento de maneira satisfatória no prazo acima determinado, estará a Contratada incorrendo em atraso na entrega, sujeita à aplicação de penalidades.

4.3. Os custos dos ajustes do serviço e/ou material rejeitado correrão exclusivamente às expensas da Contratada.

CLÁUSULA SEXTA
DAS OBRIGAÇÕES DA CONTRATADA

6.1. A Contratada se compromete a empregar seus recursos disponíveis para desenvolver os serviços contratados, atendendo as especificações da legislação vigente e/ou normas técnicas utilizadas.

6.2. A Contratada se obriga a manter, durante toda a execução do Contrato, as obrigações assumidas, relativas à habilitação e qualificação exigidas no processo de contratação.

6.3. A Contratada não poderá transferir direitos e/ou obrigações, no todo ou em parte, decorrentes da contratação.

6.4. A Contratada deve guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com a Contratante.

6.5. A Contratada deve se abster de veicular publicidade acerca do Contrato, salvo se houver prévia autorização da Contratante.

6.6. A Contratada deve se responsabilizar, direta e indiretamente, por todas as despesas decorrentes, por todos os impostos, taxas, emolumentos, seguros e contribuições fiscais e parafiscais que incidam ou venham a incidir, direta ou indiretamente, sobre todas as atividades decorrentes deste Contrato, de forma a que os pagamentos constantes na cláusula oitava, representem a única e exclusiva contraprestação pelos serviços prestados.

6.7. A Contratada deve ressarcir os eventuais prejuízos diretos ou indiretos causados à Contratante e/ ou a terceiros provocados por culpa, dolo, ineficiência ou irregularidades cometidas por seus empregados e/ ou profissionais autônomos contratados na execução dos serviços, não excluindo ou reduzindo desta responsabilidade a fiscalização ou o acompanhamento realizado pela Contratante.

6.8. A Contratada deve responder pelos danos de qualquer natureza que venham sofrer seus empregados e terceiros, em razão de acidentes ou de ação, ou de omissão dolosa ou culposa, de prepostos da empresa ou de quem a represente.

6.9. A Contratada deve prestar todos os esclarecimentos que forem solicitados pela Contratante, obrigando-se a atender todas as reclamações a respeito da qualidade dos serviços prestados.

6.10. É vedado à Contratada negociar duplicatas ou qualquer outro título cambial emitido contra a Contratante.

6.11. Assumir inteira e total responsabilidade técnica pela execução dos serviços.

6.12. Disponibilizar os serviços para uso da Contratante dentro dos parâmetros e rotinas estabelecidas, implantando de forma adequada, a supervisão permanente dos mesmos, de modo a obter uma operação correta e eficaz.

6.13. Responder, em relação aos seus empregados, por todas as despesas decorrentes da execução dos serviços, tais como: salários, seguros de acidente, taxas, impostos e contribuições, indenizações, vale-refeição, vales-transportes, e outras que eventualmente venham a ser criadas e exigidas pelo Governo.

CLÁUSULA SÉTIMA
DAS OBRIGAÇÕES DA CONTRATANTE

7.1. A Contratante deverá efetuar os pagamentos nas condições e preços pactuados desde que cumpridas todas as formalidades e exigências deste Contrato, do objeto contratado, podendo rejeitar no todo ou em parte a prestação dos serviços que estejam em desacordo às especificações deste Contrato.

7.2. Acompanhar a execução dos serviços objeto do Contrato através de fiscal nomeado para este fim e indicado pela Contratante, assegurando-se do bom desempenho e qualidade dos serviços prestados.

7.3. Fiscalizar a execução dos serviços prestados pela Contratada, inclusive quanto à continuidade da prestação dos serviços, que, ressalvados os casos de força maior, justificados e aceitos pela Contratante, não devem ser interrompidos.

7.4. A Contratante deverá proporcionar todas as condições para que a Contratada possa desempenhar seus serviços de acordo com as determinações do Contrato.

7.5. A Contratante deverá zelar para que durante a vigência do Contrato sejam mantidas, em compatibilidade com as obrigações assumidas pela Contratada, todas as condições de habilitação e qualificação exigidas no processo de contratação.

7.6. Comunicar à Contratada, o mais prontamente possível, qualquer anormalidade observada na prestação dos serviços.

7.7. Proporcionar todas as facilidades necessárias ao bom andamento do serviço desejado.

7.8. Prestar as informações e os esclarecimentos necessários que venham ser solicitados pela Contratada, durante a vigência e execução dos serviços.

CLÁUSULA OITAVA
DO VALOR CONTRATUAL

8.1. Pela realização dos serviços objeto deste Contrato, fará jus a Contratada o valor mensal de **R$ 4.161,58 (quatro mil, cento e sessenta e um reais e cinquenta e oito centavos)**, perfazendo o total anual de **R$ 49.938,96 (quarenta e nove mil, novecentos e trinta e oito reais e noventa e seis centavos)**, para os 12 (doze) meses de Contrato, conforme proposta acostada aos autos do processo de Dispensa de Licitação n.º 260/2018 (Protocolo 2018/16/1257).

8.2. Para os efeitos legais, considera-se o valor estabelecido nesta cláusula, como líquido e sem mais acréscimo de qualquer natureza, considerando-se ainda incluso todos os custos e benefícios decorrentes de trabalhos executados em horas extraordinárias, trabalhos noturnos, dominicais, e em feriados, de modo a constituir a única contraprestação pela execução dos serviços.

8.3. A Contratada não poderá realizar qualquer cobrança adicional de valores que não constem na proposta e nem alegar posterior desconhecimento de causas que impeçam a execução dos serviços.

8.4. No pagamento a ser efetuado, a Contratante providenciará a retenção do ISSQN e, o posterior recolhimento do valor correspondente junto à Prefeitura Municipal de Campinas, nos termos da legislação municipal vigente, bem como, das demais retenções aplicáveis, se cabíveis para o tipo de contratação.

8.5. Os recursos disponíveis para a aquisição do objeto do presente instrumento provêm do orçamento financeiro previsto no orçamento executivo do exercício do ano de 2018, devidamente aprovado pelo conselho de administração, identificado pelo n.º 196/2018, constante da planilha orçamentária que integra os autos do processo licitatório.

CLÁUSULA NONA
DA FISCALIZAÇÃO/CONTROLE DA EXECUÇÃO DOS SERVIÇOS

9.1. A Contratante nomeia o Coordenadoria de Informática - AII, para ser o Gestor do presente Contrato.

9.2. No desempenho de suas atividades é assegurado ao Gestor o direito de verificar a perfeita execução do presente ajuste em todos os termos e condições.

9.3. A ação ou omissão total ou parcial do Gestor não eximirá a Contratada de total responsabilidade de executar os serviços em questão, com toda cautela e boa técnica.

9.4. Não obstante a Contratada seja a única e exclusiva responsável pela prestação dos serviços, à Contratante fica reservado o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização sobre os serviços, por prepostos designados.

9.5. A presença da Fiscalização da Contratante durante a execução dos serviços, quaisquer que sejam os atos praticados no desempenho de suas atribuições, não implicará na solidariedade ou corresponsabilidade com a Contratada, que responderá única e integralmente pela execução dos serviços, inclusive pelos serviços executado por suas subcontratadas, se aplicável ao caso, na forma da legislação em vigor.

9.6. O gestor do Contrato deverá:
9.6.1. Promover o acompanhamento e a fiscalização dos serviços contratados, sob os aspectos quantitativo, anotando, em registro próprio, as falhas detectadas e comunicando à Contratada as ocorrências de quaisquer fatos que, a seu critério, exijam corretivas por parte da mesma.

CLÁUSULA DÉCIMA
DAS CONDIÇÕES DE PAGAMENTO

10.1. A Contratada deverá emitir nota fiscal/fatura correspondente aos serviços prestados à Contratante até o dia 25 (vinte e cinco) do mês correspondente ao da execução dos serviços, e entregá-la no prazo de 01 (um) dia útil ao gestor do Contrato, juntamente com o relatório dos serviços prestados e da respectiva Ordem de Serviço (OS), quando houver.

10.2. Na nota fiscal/fatura a Contratada deverá discriminar a nomenclatura do serviço prestado, com o valor correspondente à somatória dos serviços ativos. Estes valores devem contemplar custos com impostos, além dos demais elementos habituais fiscais e legais.

10.3. Os dados cadastrais para emissão da nota fiscal/fatura são os seguintes:

- Nome/Razão Social: **Centrais de Abastecimento de Campinas S/A**
- CNPJ/MF: **44.608.776/0001-64**
- Inscrição Estadual: **Isenta**
- Endereço: Rodovia Dom Pedro I - Km 140,5 - SP 065 - Pista Norte
- Bairro: Barão Geraldo
- Município: Campinas
- Estado: São Paulo
- CEP: 13.082-902
- Nome do departamento para receber cópia da Nota Fiscal Eletrônica: departamento financeiro
- E-mail: ***nfe@ceasacampinas.com.br***

10.4. O gestor terá o prazo de até 01 (um) dia útil, a contar da apresentação do documento fiscal, para aprová-lo ou rejeitá-lo.

10.5. O documento fiscal não aprovado pelo gestor será devolvido à Contratada para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo estabelecido no item anterior, a partir da data da reapresentação da nota fiscal/fatura o que, consequentemente, provocará a prorrogação do pagamento sem qualquer ônus adicional a Contratante.

10.6. A devolução do documento fiscal não aprovado pelo gestor em hipótese alguma servirá de pretexto para que a Contratada suspenda a execução dos serviços.

10.7. Caso os serviços constantes do objeto deste Contrato sofram algum tipo de retenção na fonte de impostos ou contribuições, a Contratante providenciará a retenção e o recolhimento, nos termos da legislação vigente, aplicável ao caso.

10.7.1. Se a Contratada estiver estabelecida na cidade de Campinas/SP, a Contratante irá reter e recolher na fonte o valor correspondente ao ISSQN, por substituição tributária, de acordo com a legislação municipal em vigor, bem como, das demais empresas que independente da sede, a lei estabeleça que o ISSQN seja recolhido no local da prestação do serviço.

10.7.2. Para as empresas estabelecidas fora do município de Campinas/SP, deverá a mesma possuir situação cadastral **ativa** no CENE (Cadastro de Empresas Não Estabelecidas em Campinas), observadas as disposições do art. 2º da INSTRUÇÃO NORMATIVA DRM/SMF N.º 002, DE 06 DE DEZEMBRO DE 2017. O não cumprimento desta orientação, acarretará a retenção do ISSQN a favor do erário de Campinas/SP.

10.8. A falta da apresentação de qualquer documento obrigatório pelas leis em vigor acarretará a suspensão do pagamento da respectiva nota fiscal/fatura e das seguintes, até que a pendência seja sanada, sem que se aplique, neste caso, o disposto na cláusula décima primeira do Contrato.

10.9. Se aplicável ao caso, juntamente com a nota fiscal/fatura a Contratada deverá encaminhar:
a) Certidão Conjunta Negativa de Débitos ou Positiva com efeito de Negativa, relativa a tributos federais (inclusive as contribuições sociais) e dívida ativa da União;
b) Certidão de regularidade de débito para com o Fundo de Garantia por Tempo de Serviço (FGTS);
c) Certidão Negativa de Débitos Trabalhistas - CNDT ou Positiva de Débitos Trabalhistas com Efeitos de Negativa, em cumprimento à Lei n.º 12.440/2011 e à Resolução Administrativa TST n.º 1.470/2011;
d) Certidão de regularidade de débito com o Município - ISSQN, da sede ou do domicílio da Contratada.

10.10. Verificada qualquer irregularidade na emissão da nota fiscal/fatura, perante a incidência do ICMS, o serviço não será recebido pela Ceasa/Campinas uma vez que, o Decreto Estadual n.º 52.118/2007 veda a utilização de carta de correção em itens que possam incidir no valor do imposto.

10.11. A Contratante providenciará **o pagamento da nota fiscal/fatura à Contratada até o 5º (quinto) dia útil do mês subsequente ao da emissão da nota fiscal.**

10.12. Os pagamentos serão efetuados exclusivamente através de depósito bancário em

conta corrente da Contratada, de acordo com os dados constantes da proposta de preços.

10.13. A Contratante deduzirá quaisquer valores faturados indevidamente, bem como, poderá deduzir quaisquer valores provenientes de aplicação de penalidades.

CLÁUSULA DÉCIMA PRIMEIRA
DO REAJUSTAMENTO DE PREÇO

11.1. O valor contratual previsto na cláusula oitava, se por acordo entre as partes, o Contrato for prorrogado, poderá ser reajustado tendo como base o índice ICV - Dieese ou outro que vier a substituí-lo, sendo que a periodicidade de reajuste será anual.

CLÁUSULA DÉCIMA SECUNDA
DA RESCISÃO CONTRATUAL

12.1. O Contrato poderá ser rescindido, de pleno direito, nos seguintes casos:
a) o descumprimento ou o cumprimento irregular ou incompleto de cláusulas contratuais, especificações ou prazos;
b) o atraso injustificado no início do serviço;
c) a subcontratação do objeto contratual;
d) a fusão, cisão, incorporação, ou associação da Contratada com outrem, não admitidas no Contrato e sem prévia autorização da Contratante;
e) o desatendimento das determinações regulares do gestor e/ou do fiscal do Contrato;
f) o cometimento reiterado de faltas na sua execução, anotadas em registro próprio;
g) a decretação de falência ou a instauração de insolvência civil;
h) a dissolução da sociedade ou o falecimento da Contratada;
i) razões de interesse da Contratante, de alta relevância e amplo conhecimento, justificadas e exaradas no processo interno;
j) a ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do Contrato;
k) a suspensão de sua execução, por ordem escrita da Contratante, por prazo superior a 120 (cento e vinte) dias, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra;
l) o atraso superior a 90 (noventa) dias dos pagamentos devidos pela Contratante, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado à Contratada o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;
m) o descumprimento da proibição de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e de qualquer trabalho a menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos;
n) o perecimento do objeto contratual, tornando impossível o prosseguimento da execução da avença.

12.2. A rescisão do Contrato poderá ser:
a) amigável, reduzida a termo no processo que originou esta contratação, desde que haja conveniência para a Contratante;
b) judicial, nos termos da legislação.

CLÁUSULA DÉCIMA TERCEIRA
DAS SANÇÕES ADMINISTRATIVAS

13.1. O não cumprimento dos serviços constantes deste Contrato e ainda a prática de qualquer transgressão das condições estabelecidas neste instrumento contratual sujeitarão à Contratada as seguintes sanções:

a) advertência, sempre que forem constatadas irregularidades de pouca gravidade, para as quais tenha a Contratada concorrido diretamente;

b) multa de 1,0% (um por cento) por dia até o 5º dia de atraso e 2% (dois por cento) ao dia a partir do 6º dia de atraso indicados nos itens 5.1 e 5.2 até o limite de 25% (vinte e cinco por cento);

c) multa de 10% (dez por cento) aplicada sobre o valor total do Contrato, para qualquer transgressão cometida que não seja atraso na prestação de serviços;

d) multa de 10% (dez por cento) aplicada sobre o valor total do Contrato, na ocorrência da situação indicada no item 5.2.1, além de sua rescisão unilateral; e

e) rescisão unilateral do Contrato pela Ceasa, no caso de ser excedido o limite de 25% (vinte e cinco por cento) estabelecido na letra b.

13.2. As multas serão, após regular processo administrativo, descontadas dos créditos da Contratada ou, se for o caso, cobradas administrativa ou judicialmente.

13.3. As penalidades previstas neste item têm caráter de sanção administrativa, consequentemente, a sua aplicação não exime a Contratada da reparação das eventuais perdas e danos que seu ato punível venha acarretar a Contratante.

13.4. As penalidades são independentes e a aplicação de uma não exclui a das demais, quando cabíveis.

13.5. As sanções previstas neste item poderão ser aplicadas desde que facultada a defesa previa da Contratada no respectivo processo no prazo de 10 (dez) dias uteis, conforme art. 83, § 2.º da Lei Federal n.º 13.303/2016.

13.6. Sem prejuízo da aplicação de penalidades, a Contratada é responsável pelos danos causados à Administração ou a terceiros, na forma disposta no art. 76 da Lei Federal n.º 13.303/2016, não excluindo ou reduzindo essa responsabilidade, a fiscalização ou acompanhamento pelo órgão interessado.

CLÁUSULA DÉCIMA QUARTA
DA FUNDAMENTAÇÃO LEGAL

14.1. A presente contratação será por Dispensa de Licitação - artigo 29, inciso II, da Lei Federal n.º 13.303/2016, cujos atos se encontram junto ao Protocolo n.º 2018/16/1257.

CLÁUSULA DÉCIMA QUINTA
DA SUSPENSÃO DO PAGAMENTO

15.1. A Contratante poderá suspender o pagamento de qualquer fatura apresentada pela Contratada, no todo ou em parte, nos seguintes casos:

a) execução defeituosa dos serviços;
b) descumprimento de obrigação relacionada com os serviços contratados;
c) débito da Contratada para com a Contratante, proveniente deste Contrato ou de qualquer outra obrigação entre as partes;
d) não cumprimento de obrigação contratual, hipótese em que o pagamento ficará retido até que a Contratada atenda à cláusula infringida;
e) havendo prejuízo à Contratante pelo descumprimento da obrigação contratual, a Contratada arcará com perdas e danos, bem como com eventuais gastos assumidos pela Contratante para reparar a ineficiência dos serviços contratados;
f) obrigações da Contratada com terceiros que, eventualmente, possam prejudicar a Contratante;
g) paralisação do serviço por culpa da Contratada.

CLÁUSULA DÉCIMA SEXTA
DO FORO

16.1. Os contratantes elegem o Foro da Comarca de Campinas/SP, com renúncia de qualquer outro, por mais privilegiado que seja, para dirimir dúvidas ou questões não resolvidas administrativamente.

E, por estarem assim justas e contratadas, firmam as partes este instrumento em 04 (quatro) vias de igual teor e único fim, para que produza os efeitos de direito.

Campinas, 14 de novembro de 2018.

Pela **CEASA/CAMPINAS**:

WANDER DE OLIVEIRA VILLALBA
Diretor Presidente

MIGUEL JORGE NICOLAU FILHO
Diretor Administrativo e Financeiro

CLAUDINEI BARBOSA
Diretor Técnico Operacional

Pela Contratada: **BLUEPEX CONTROLE E SEGURANÇA EM TI S/A**

NILTON SILVA FERNANDES DE SOUZA

Testemunha 1:

Nome/RG: Vlissi de Oliveira Portado
RG. 27.385.011-4

Testemunha 2:

Nome/RG: Danuza Savala
25.470.945-X

Danuza Savala
Chefe de Setor - Licitações e Contratos
CEASA - Campinas

BANCO MUNICIPAL DE ALIMENTOS
DA CEASA/CAMPINAS

CEASA - Mariana Romão - Jurídico
OAB/SP nº 203.559