SC 01891/2024 (PC)

Solicitado em:	**09/09/2024**	Solicitante:	**JOYCE DA SILVA CORDEIRO - SAAE.JOYCEC**
Aprovado em:	**16/09/2024**	Aprovador:	**ERIC DOS SANTOS BURGOMEISTER - SAAE.ERICSANTOS**
Unidade solicitante:	**SAAE - JACAREI - (1)**		
Centro de consumo:	**Unidade de Tecnologia da Informação - (55)**		
Tipo de entrega:	**Única**	Prazo de entrega:	

Justificativa

A informação é um dos principais ativos das organizações e instituições públicas, tratando-se de um elemento fundamental para a tomada de decisões em todos os níveis, sendo determinante para a gestão governamental. Nesse sentido, os gestores precisam promover ações para garantir a segurança de tais informações. Os constantes ataques cibernéticos, a necessidade de continuidade do negócio e a evolução de ameaças das mais variadas espécies criam a necessidade de contratação de uma solução que proteja as informações da Autarquia e diminua os riscos de acesso indevido às mesmas.

Inseridos dentro de um contexto muito dinâmico de evolução constante de tecnologia, em um curto intervalo de tempo, os equipamentos destinados à segurança da informação podem se tornar obsoletos a tal ponto de não suportarem o aumento do tráfego de internet e dados, o crescente número de novos usuários e as novas ameaças e tentativas de invasões das redes corporativas. Dentro do contexto analisado, o firewall representa um quesito de segurança fundamental, uma vez que regula o tráfego de dados entre redes distintas e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede.

PEDIDO DE PRÉ-EMPENHO Nº: 0 | **PRÉ-EMPENHO Nº:** | **SITUAÇÃO DO PRÉ-EMPENHO: Aprovado**

TIPO DE EMPENHO:	**Estimativo** DESEMBOLSO: **0**
FICHA:	**55**
UNIDADE ORÇAMENTARIA:	**0305 - DEPARTAMENTO ADMINISTRATIVO**
UNIDADE EXECUTORA:	**030501 - GABINETE DO DIRETOR ADMINISTRATIVO E DEPENDÊNCIAS**
FUNCIONAL PROGRAMÁTICA:	**04.122.0011.2243 - Manutenção do Departamento Administrativo**
CONTA:	**3.3.90.40.00 - Serviços de Tecnologia da Informação e Comunicação - PJ**
ELEMENTO:	**3.3.90.40.99 - Outros Serviços de Tecnologia da Informação e Comunicação - PJ**
FONTE DE RECURSO:	**04 - Recursos Próprios da Administração Indireta**
APLICAÇÃO:	**110.0000**
FICHA DE CONTAS A PAGAR:	**0 - 000000.000 - Contas a pagar**
CENTRO DE CUSTO:	**SERVIÇOS DE TERCEIROS DIVERSOS P/ DIVISÃO**
TIPO DE DESPESA:	**GERAL**
ORDENADOR:	**EDER CAMPOS OLIVEIRA**

ITEM	LIB.	CLASSIFICAÇÃO E DESCRIÇÃO DO *SERVIÇO*	QUANTIDADE	VALOR ESTIMADO UNITÁRIO	VALOR ESTIMADO TOTAL
0001	✓	511.110011 **PJ - LOCAÇÃO DE SOTWARE - CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM FORNECIMENTO DE SOLUÇÃO DE HARDWARE E SOFTWARE DE SEGURANÇA DE REDES, COM TECNOLOGIA AVANÇADA DE FIREWALL, IPS,VPN, FILTRO WEB E PROTEÇÃO CONTRA AMEAÇAS** *ESPECIFICAÇÃO:* Conforme termo de referencia em anexo *LOCAL DE ENTREGA:* Rua Miguel Leite do Amparo, 121 - Jd. Pereira do Amparo - Jacarei	---	---	1,00

LIB. = Liberado

TOTAL: 1,00

SALDO DISPONÍVEL NA FICHA NA ELABORAÇÃO DO PRÉ-EMPENHO:	**0,00**
VALOR DO PRÉ-EMPENHO:	**0,00**
SALDO DISPONÍVEL NA FICHA APÓS A ELABORAÇÃO DO PRÉ-EMPENHO:	**0,00**

SC 01891/2024 (PC)

Joyce da Silva Cordeiro
SOLICITANTE
JOYCE DA SILVA CORDEIRO

APROVADOR
ERIC DOS SANTOS BURGOMEISTER

Eric dos S. Burgomeister
Diretor de Departamento Administrativo

ORDENADOR
EDER CAMPOS OLIVEIRA

Controle Orçamentário - Financeiro:

Data:____/____/_____

Ass:_____

Controlador Orçamentário e Financeiro

Data:____/____/_____ ( ) Aprovado ( ) Não Aprovado

Francisco José Monteiro

Unidade de Licitações e Compras
16/09/24
09:41 Horas
Nazare

TERMO DE REFERÊNCIA

1. ***OBJETO: Contratação de Empresa especializada em fornecimento de solução de hardware e software de segurança de redes, com tecnologia avançada de firewall, IPS, VPN, filtro web e proteção contra ameaças.***

2. ***JUSTIFICATIVA:***
Devido a problemas com o processo de licitação de mesmo objeto em andamento, faz-se necessária a compra direta de 4 (quatro) meses de serviço de firewall afim de garantir a segurança de rede da autarquia durante o período já que é um dos principais ativos das organizações e instituições públicas, tratando-se de um elemento fundamental para a tomada de decisões em todos os níveis, sendo determinante para a gestão governamental. Nesse sentido, os gestores precisam promover ações para garantir a segurança de tais informações. Os constantes ataques cibernéticos, a necessidade de continuidade do negócio e a evolução de ameaças das mais variadas espécies criam a necessidade de contratação de uma solução que proteja as informações da Autarquia e diminua os riscos de acesso indevido às mesmas. Dentro do contexto analisado, o firewall representa um quesito de segurança fundamental, uma vez que regula o tráfego de dados entre redes distintas e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede.

3. HABILITAÇÃO

3.1 Apresentar Atestado(s) de Capacidade Técnica comprovando que realizou serviços de características similares, ao objeto deste Termo de Referência, emitido(s) por empresa(s) pública(s) ou privada(s), o qual deverá constar no mínimo:

a) Nome da contratante;

b) Local da prestação dos serviços;

c) Período dos serviços atestados;

d) Objeto do contrato;

e) Serviços executados (com respectivos totais);

f) Nome do(s) responsável(eis) técnico(s);

3.2 A Licitante deverá informar na proposta comercial marca e modelo do(s) produto(s) ofertado(s);

4 DOS REQUISITOS COMUNS PARA TODOS OS ITENS

4.1 Os produtos que compõe a Solução de Segurança devem todos ser produzidos pelo mesmo fabricante;

4.2 A LICITANTE deve informar na proposta comercial e na tabela de formação de preços marca e modelo do(s) produto(s) ofertado(s);

4.3 A LICITANTE deverá realizar a instalação dos produtos de segurança contratados pelo presente certame, na rua Miguel Leite do Amparo, 121 – Jacareí -SP;

4.4 Deverão ser fornecidos todos os documentos e manuais técnicos, tais como, datasheet, manual de instalação e configuração em versão Português - Brasil e em formato digital, no mínimo, na versão em PDF.

5 ESPECIFICAÇÕES TÉCNICAS – SOLUÇÃO DE SEGURANÇA "FIREWALL UTM"

5.1 ITEM A: APPLIANCE UTM DE 5 GBPS DE CAPACIDADE DE FIREWALL - CARACTERÍSTICAS DO HARDWARE

5.1.1 O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45mm) do referido rack;

5.1.2 Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

5.1.3 Possuir painel/led indicador on/off, disco e devices de rede;

5.1.4 Possuir throughput de no mínimo 5000 (cinco mil)Mbps para tráfego UDP;

5.1.5 Suportar no mínimo 900.000 (novecentos mil) conexões simultâneas;

5.1.6 Suportar no mínimo 50.000 (cinquenta mil) novas conexões por segundo;

5.1.7 Possuir throughput de no mínimo 1000 (mil) Mbps para tráfego HTTP/ HTTPS via proxy;

5.1.8 Possuir throughput de no mínimo 500 (quinhentos) Mbps para tráfego HTTP/ HTTPS com inspeção SSL via proxy;

5.1.9 Possuir throughput de no mínimo 400 (quatrocentos) Mbps para tráfego IPS;

5.1.10 Possuir throughput de no mínimo 1000 (mil) Mbps para tráfego VPN IPSEC com criptografia (AES-128);

5.1.11 Possuir throughput de no mínimo 800 (oitocentos) Mbps para tráfego VPN SSL com criptografia (AES-128);

5.1.11 Possuir throughput de no mínimo 800 (oitocentos) Mbps para tráfego VPN SSL com criptografia (AES-128);

5.1.12 Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

5.1.13 Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

5.1.14 Possuir no mínimo 1 (uma) porta console de conexão padrão RJ45 para acesso a interface de comando CLI especifica para esta finalidade, utilizando cabo do tipo serial RS-232/RJ-45;

5.1.15 Possuir no mínimo 2 (duas) portas USB para conexão de dispositivos externos;

6 ESPECIFICAÇÕES GERAIS DE SOFTWARE UTM PARA O ITEM A

6.1 FUNÇÕES BÁSICAS

6.1.1 Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;

6.1.2 VPN SSL, VPN IPSec (Client-to-site e Site-to-site);

6.1.3 Controle de Aplicações;

6.1.4 Proxy Web e Filtro de Conteúdo Web (URL Filtering);

6.1.5 Detecção e prevenção de intrusos – IPS;

6.1.6 Qualidade de serviço – QOS;

6.1.7 Anti-Malware;

6.1.8 SD-WAN;

6.1.9 Cluster.

6.2 CARACTERÍSTICAS GERAIS

6.2.1 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

6.2.2 Interface em português e inglês;

6.2.3 O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

6.2.4 O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.

6.2.5 Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.

6.2.6 Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.

6.2.7 A Solução deverá prover inspeção SSL:

6.2.8 A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho.

6.2.9 Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;

6.2.10 Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;

6.2.11 Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:

6.2.12 Endereço do servidor;

6.2.13 Porta do servidor;

6.2.14 Usuário;

6.2.15 Senha;

6.2.16 Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:

6.2.17 Desempenho total (throughput);

6.2.18 Conexões simultâneas;

6.2.19 Usuários autenticados;

6.2.20 Serviços habilitados ou desabilitados;

6.2.21 Quantidade de endereços distribuídos pelo DHCP.

6.3 DAS FUNCIONALIDADES DO FIREWALL:

6.3.1 Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;

6.3.2 Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

6.3.3 Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões do tipo Network File System, SSH e PenDrive;

6.3.4 Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.

6.3.5 Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;

6.3.6 O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.

6.3.7 As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

6.3.8 O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

6.3.9 Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

6.3.10 Deve permitir habilitar ou desabilitar o registro de log por política de firewall.

6.3.11 Possuir controle de acesso à internet por endereço IP de origem e destino;

6.3.12 Possuir controle de acesso à internet por sub-rede;

6.3.13 Possuir suporte a tags de VLAN (802.1q);

6.3.14 Suportar agregação de links, segundo padrão IEEE 802.3ad;

6.3.15 Possuir ferramenta de diagnóstico do tipo tcpdump;

6.3.16 Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;

6.3.17 Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

6.3.18 Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.

6.3.19 Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

6.3.20 Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;

6.3.21 Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.

6.3.22 Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;

6.3.23 Possuir funcionalidades de DHCP Cliente, Servidor e Relay;

6.3.24 Deverá suportar aplicações multimídia como: H.323, SIP;

6.3.25 Possuir tecnologia de firewall do tipo Stateful;

6.3.26 Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;

6.3.27 Permitir o funcionamento em modo transparente tipo "bridge";

6.3.28 Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;

6.3.29 Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);

6.3.30 Deverá suportar forwarding de multicast;

6.3.31 Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;

6.3.32 Permitir o agrupamento de serviços;

6.3.33 Permitir o filtro de pacotes sem a utilização de NAT;

6.3.34 Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

6.3.35 Possuir mecanismo de anti-spoofing;

6.3.36 Permitir criação de regras definidas pelo usuário;

6.3.37 Permitir o serviço de autenticação para HTTP e FTP;

6.3.38 Possuir a funcionalidade de balanceamento e contingência de links;

6.3.39 Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY.

6.4 IDENTIFICAÇÃO DE USUÁRIO

6.4.1 Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;

6.4.2 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

6.4.3 Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;

6.4.4 Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);

6.4.5 A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

6.4.6 Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;

6.4.7 A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;

6.4.8 A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;

6.5 DAS FUNCIONALIDADES DA VPN:

6.5.1 VPN baseada em appliance;

6.5.2 Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

6.5.3 Suporte a certificados PKI X.509 para construção de VPNs;

6.5.4 Possuir suporte a VPNs IPSec site-to-site:

6.5.4.1 Criptografia, 3DES, AES128, AES256, AES-GCM-128
6.5.4.2 Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
6.5.4.3 Algoritmo Internet Key Exchange (IKE) versões I e II;
6.5.4.4 AES 128 e 256 (Advanced Encryption Standard);
6.5.4.5 Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30;

6.5.5 Possuir suporte a VPN SSL;

6.5.6 Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

6.5.7 Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços: RDP, VNC,SSH,WEB e SMB

6.5.8 Deve permitir a arquitetura de vpn hub and spoke;

6.5.9 Suporte a VPNs IPSec client-to-site;

8.5.9.1 Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.

6.5.10 Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);

6.5.11 Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;

6.5.12 A funcionalidade de AD-VPN deve suportar criar no mínimo os seguintes tipos de tuneis: Site-to-Site, Full-Mesh e Star

6.6 DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO:

6.6.1 A Detecção de Intrusão deverá ser baseada em appliance:

6.6.2 Capacidade de detecção de mais de 22.000 ataques;

6.6.3 O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;

6.6.4 Possuir tecnologia de detecção baseada em assinatura;

6.6.5 Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;

6.6.6 Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass;

6.6.7 O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;

6.6.8 Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.

6.6.9 Possuir capacidade de remontagem de pacotes para identificação de ataques;

6.6.10 Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;

6.6.11 Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

6.6.12 Mecanismos de detecção/proteção de ataques;

6.6.13 Reconhecimento de padrões;

6.6.14 Análise de protocolos;

6.6.15 Detecção de anomalias;

6.6.16 Detecção de ataques de RPC (Remote procedure call);

6.6.17 Proteção contra ataques de Windows ou NetBios;

6.6.18 Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

6.6.19 Proteção contra ataques DNS (Domain Name System);

6.6.20 Proteção contra ataques a FTP, SSH , Telnet e rlogin;

6.6.21 Proteção contra ataques de ICMP (Internet Control Message Protocol);

6.6.22 Alarmes na console de administração;

6.6.23 Alertas via correio eletrônico;

6.6.24 Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

6.6.25 Capacidade de resposta/logs ativa a ataques;

6.6.26 Terminação de sessões via TCP resets;

6.6.27 Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

6.6.28 O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;

6.6.29 Possuir filtros de ataques por anomalias;

6.6.30 Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

6.6.31 Permitir filtros de anomalias de protocolos;

6.6.32 Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

6.6.33 Suportar verificação de ataque nas camadas de aplicação;

6.7 DAS FUNCIONALIDADES DE QOS

6.7.1 Adotar solução de Qualidade de Serviço baseada em appliance;

6.7.2 Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

6.7.3 Permitir modificação de valores DSCP para o DiffServ;

6.7.4 Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;

6.7.5 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

6.7.6 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

6.7.7 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

6.7.8 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;

6.7.9 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

6.8 DAS FUNCIONALIDADES DO ANTIVÍRUS

6.8.1 Possuir funções de Antivírus, Anti-spyware;

6.8.2 Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;

6.8.3 Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)

6.8.4 Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

6.8.5 Permitir o bloqueio de download de arquivos por tamanho.

6.9 DAS FUNCIONALIDADES DO PROXY E FILTRO DE CONTEÚDO WEB

6.9.1 Possuir solução de filtro de conteúdo web integrado a solução de segurança

6.9.2 Possuir pelo menos 75 categorias para classificação de sites web

6.9.3 Possuir base mínima contendo, 40 milhões de sites internet web já registrados e classificados;

6.9.4 Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:

6.9.4.1 Webmail;
6.9.4.2 Instituições de Saúde;
6.9.4.3 Notícias;
6.9.4.4 Pornografia;
6.9.4.5 Restaurante;
6.9.4.6 Mídias Sociais;
6.9.4.7 Esporte;
6.9.4.8 Educação;
6.9.4.9 Games;
6.9.4.10 Compras;

6.9.5 Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

6.9.6 Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;

6.9.7 Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;

6.9.8 Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;

6.9.9 Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;

6.9.10 Possibilitar a integração com servidores de cache WEB externos;

6.9.11 Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update®, Youtube®, MSN Vídeos®, Facebook®, Google Maps®;

6.9.12 Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;

6.9.13 Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

6.9.14 Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

6.9.15 Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;

6.9.16 Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;

6.9.17 Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;

6.9.18 Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

6.9.19 Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;

6.9.20 Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;

6.9.21 Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

6.9.22 Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

6.9.23 Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;

6.9.24 Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;

6.9.25 Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e URLs originadas de Spam;

6.9.26 Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

6.9.27 Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;

6.9.28 Deverá permitir configurar a porta do Proxy Explícito.

6.10 DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES

6.10.1 As funcionalidades abaixo devem ser baseadas em appliance:

6.10.2 Deverá reconhecer no mínimo 700 aplicações;

6.10.3 Deverá possuir pelo menos 10 categorias para classificação de aplicações;

6.10.4 Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:

6.10.4.1 P2P;
6.10.4.2 Web;
6.10.4.3 Transferência de arquivos;
6.10.4.4 Chat;
6.10.4.5 Social;

6.10.5 Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

6.10.6 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

6.10.7 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

6.10.8 Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

6.10.9 Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

6.10.10 Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

6.10.11 Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;

6.10.12 Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

6.11 SISTEMA DE PROTEÇÃO AVANÇADA CONTRA AMEAÇAS - ATP

6.11.1 Possuir sistema de proteção avançada contra ameaças (ATP) nativo;

6.11.2 O sistema de ATP deve monitorar e analisar o tráfego da rede, identificar aplicativos e ameaças de ataques direcionados e persistentes e efetuar os respectivos bloqueios.

6.11.3 Deve ser baseado em uma lista de assinaturas eletrônicas que atue em tempo real analisando a camada de aplicação, capaz de identificar o conteúdo dos pacotes, fazer log (registros) das assinaturas trafegadas, inspecionar os pacotes e efetuar o descarte automático do pacote quando identificado assinaturas de pacotes maliciosos, inapropriados para o uso no ambiente corporativo;

6.11.4 A base de assinaturas do sistema de ATP nativo deverá ser fornecida pelo período do contrato;

6.11.5 Possuir um mínimo de 31 mil (trinta e um mil) assinaturas;

6.11.6 Dever permitir a identificação de aplicativos e ameaças independente das portas e protocolos;

6.11.7 Deve permitir a atualização automática das assinaturas por meio de agendamento diário;

6.11.8 Possuir capacidade de inspecionar e bloquear em tempo real, ameaças do tipo: activex, malware, malware-backdoors, ataques P2P, trojans, worms, user_agents, pua (adware, p2p, toolbars) malwares para mobile, blacklist, botcc, exploits-kits, file-executable, file-flash, file-identify, file-image, file-java, file-multimedia, file-office, file-other, file-pdf, games, inappropriate e vulnerabilidades conhecidas;

6.11.9 Possuir uma ferramenta de bloqueio de execução de aplicativos, integrado a base de Antivírus e Antimalware;

6.11.10 Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos do tipo: ads, cloud, colaboração, download, e-mail, games, mobile, p2p, proxy, remote, redes sociais; storage, streaming, update, voip e web.

6.11.11 Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de VoIP tais como: Hotline, Asterisk, Linphone, SIP, Skype, Xlite SIP, X-Pro SIP, Cisco SIP, OpenSIP, Bria, ClearSea e Nero SIP;

6.11.12 Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos de Redes Sociais tais como: Aol Instant Messenger, Badoo, BaiduHi, Airtime, Blogger, BoldChat, ChatON, China.com, Facebook, Flickr, FC2, Fring, Google Analytics, Google App, ICQ, Linkdin, Meetup, MSM Messenger, Netlog, Skype, Tinder, Tuenti, Twitter, WhatssApp, WeChat e Zoho Chat;

6.11.13 Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) tais como: BitTorrent, Gnutella, FastTrack, IceShare, Napster, Shareman e de Storages, tais como: Dropbox, Easy-share, Google Drive, Megashare, MegaUpload, Rapidshare, OneDrive, Yahoo Box, SoundCloud e Filemail, DivShare;

6.11.14 Suportar exceção de ameaças por assinatura; IP de origem ou IP de destino;

6.11.15 Suportar exceção de aplicativos por assinatura; IP de origem ou IP de destino;

6.11.16 Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre as "ameaças detectadas" e as "ameaças bloqueadas";

6.11.17 Deve possuir mecanismos para gerar gráfico do histórico da relação de eventos entre os "aplicativos detectados" e os "aplicativos bloqueados";

6.11.18 Deve possuir mecanismos para gerar log dos registros das incidências, classificados em pelo menos 3 (três) níveis de impacto: "baixo; médio e alto";

6.11.19 Gerar registro do tipo Top Level, dos 10(dez) mais, inclusive da relação de eventos entre usuários e ameaças, usuário e aplicativos, aplicativos e ameaças identificados e bloqueados;

6.12 SD-WAN:

6.12.1 Possuir funcionalidades de SD-WAN, não se limitando aos recursos solicitados abaixo;

6.12.2 Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;

6.12.3 Permitir utilizar VPN IPsec para interligar unidades remotas;

6.12.4 Possuir recurso de "persistência de link" para impedir a queda de conexões em aplicações que não suportam o load balance de link;

6.12.5 O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;

6.12.6 Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos relacionado ao recurso SD-WAN;

6.12.7 Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações:

6.12.8 Consumo de banda;

6.12.9 Perda de pacotes;

6.12.10 Jitter;

6.12.11 Latência.

6.13 ALTA DISPONIBILIDADE

6.13.1 Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.

6.13.2 Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.

6.13.3 O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat;

7 ITEM B: SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE FIREWALL - FUNCIONALIDADES DE GERENCIAMENTO

7.1 Como boa prática de segurança e de mercado, a solução de gerência deverá ser separada do gateway de segurança, onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto;

7.2 A solução de gerenciamento centralizado deve possibilitar o gerenciamento de todos os Firewall contratados.

7.3 O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance fisíco deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual, deverá ser compatível com VMware ESXi e todo custo da infraestrutura necessária para suportar o appliance virtual é responsabilidade da CONTRATANTE;

7.4 Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;

7.5 A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS ou console gráfica;

7.6 Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;

7.7 A solução deve incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;

7.8 A solução de gerência deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho.

7.9 Deve possibilitar a realização de "backup" e restauração de dados.

7.10 Deve possibilitar o envio dos "logs" gerados a outro concentrador de "logs" externo a solução.

7.11 Deve possibilitar a gerência de "logs", realizando as configurações de relatórios de todos os "firewalls" integrados.

7.12 Deve permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet.

7.13 O gerenciamento deve permitir/possuir:

7.14 Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas;

7.15 Monitoração de logs;

7.16 Debugging;

7.17 Acesso concorrente de administradores;

7.18 Deve permitir usar palavras chaves para facilitar identificação de regras;

7.19 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

7.20 Autenticação integrada à base de dados local;

7.21 Deve possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, subrede) na base de regras;

7.22 Criação de regras que fiquem ativas em horário definido;

7.23 Backup das configurações e rollback de configuração para a última configuração salva;

7.24 Habilidade de upgrade via interface de gerenciamento;

7.25 Deverá ter a capacidade de gerar um relatório gráfico, que permita visualizar as mudanças na utilização de aplicações na rede, no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao passado;

7.26 Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções;

7.27 Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção;

7.28 Deve permitir a criação de objetos e políticas compartilhadas;

7.29 Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

7.30 Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

7.31 FUNCIONALIDADES DE ANALISE DE LOG

7.32 Deverá prover análise de tráfego de rede de modo centralizado;

7.33 Deve possuir análise de tráfego de rede e ameaças por geolocalização;

7.34 Deverá ser capaz de receber os logs e eventos com o objetivo de prover os seguintes tipos de análises:

7.35 Análise de ameaças e incidentes de segurança;

7.36 Análise de tráfego e uso de categorias Web;

7.37 Análise de tráfego e uso de aplicativos;

7.38 Análise de tráfego e ameaças por usuário;

7.39 Análise de desempenho de políticas de segurança;

7.40 A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de logs, consolidação de logs, arquivamento de logs, busca avançada de logs;

7.41 Deverá possuir ferramenta para salvar consultas avançadas;

7.42 Deve possuir relatórios personalizados;

7.43 Deverá ser capaz de efetuar o arquivamento de relatórios;

7.44 Deve possuir agendamento de relatórios;

7.45 Os Relatórios deverão, no mínimo, serem exportados em formatos flexíveis (PDF, CSV);

8 ITEM C: SERVIÇO DE INSTALAÇÃO

8.1 O prazo para execução do serviço de instalação será de até 7 dias após emissão de ordem de serviço.

8.2 Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da contratada;

8.3 Entende-se por serviços de instalação, as atividades de fornecimento dos materiais, planejamento, instalação, integração e pré-operação.

8.4 Os serviços de instalação deverão ser executados pela CONTRATADA nas dependências da CONTRATANTE.

8.5 Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário de expediente da Contratante, compreendido das 8h30 às 16h30, de segunda-feira a sexta-feira, devendo eventualmente e previamente agendado, atender à CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de atividades que necessitem ser executados nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente, e de comum acordo entre as partes, sem ônus adicional para a CONTRATANTE.

8.6 Todos os instrumentos/equipamentos necessários para a execução dos serviços e testes de aceitação do serviço e produtos serão fornecidos pela CONTRATADA.

8.7 O projeto de planejamento e execução das atividades de instalação e configuração deverão ser executados por profissionais com certificação em gerenciamento de projetos – PMP (Project Management Professional) e com experiência no objeto licitado;

8.8 A equipe técnica da CONTRATADA deverá trabalhar sob orientação e supervisão direta do profissional responsável pela coordenação das atividades de instalação (gestor de projetos da CONTRATADA), com o acompanhamento do responsável técnico da CONTRATANTE.

8.9 A CONTRATADA deverá elaborar e manter relatório de atividades (RA), contendo anotações das atividades realizadas, irregularidades encontradas e outras ocorrências relativas à execução do contrato de modo a subsidiar reunião periódica de acompanhamento do projeto a ser realizada com a participação mínima do responsável técnico da CONTRATANTE e pelo gestor de projetos da CONTRATADA.

8.10 Quando aprovado o funcionamento dos produtos, esses serão considerados instalados e aptos a serem utilizados. Isso deverá ser confirmado em termo de recebimento emitido pela CONTRATANTE, após execução completa dos serviços de instalação.

8.11 Quando não aprovado o funcionamento de qualquer produto ou serviço sob responsabilidade da CONTRATADA, esta deverá anotar no relatório de atividades as ocorrências e suas origens, e tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus à CONTRATANTE e sem prejudicar o tempo previsto de implantação.

8.12 O relatório de atividades não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento dos produtos, o qual deverá ser estendido ao longo de todo o período de garantia.

8.13 Todas as informações manuseadas pela CONTRATADA são de uso exclusivo e restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da

CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE.

8.14 A CONTRATADA, após concluído o serviço de instalação dos produtos no site da CONTRATANTE, deverá realizar, com o acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para constatar que os produtos foram instalados e configurados de acordo com o cenário requerido pela CONTRATANTE e conforme definido no Projeto de Implantação desenvolvido.

9 ITEM D: SERVIÇOS DE PRESTAÇÃO DE SUPORTE TÉCNICO REMOTO 14X6

9.1 Serviço de suporte REMOTO para os equipamentos de segurança de borda contratados, no horário 14 x 6 (Segunda a Sábado das 08:00 às 22:00, exceto feriados), pelo tempo de contrato, com as seguintes características:

9.2 A contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;

9.3 A contratada deverá iniciar o atendimento de suporte em no máximo 8 horas úteis após a abertura do chamado;

9.4 O atendimento de suporte deverá ser na língua portuguesa em todos os níveis;

9.5 Todos os documentos e manuais técnicos que serão entregues à Contratante, deverão apresentar-se em versão Português – Brasil e em formato digital, no mínimo na versão em PDF.

10 DO PRAZO PARA PRESTAÇÃO DOS SERVIÇOS

10.1 O prazo para o fornecimento dos equipamentos e instalação da Solução será de até 7 dias corridos à partir da emissão da Ordem de Serviço. Findo esse prazo, e/ou a partir da data, o sistema deverá estar devidamente implantado e funcionando em perfeitas condições.

11 VIGÊNCIA DO CONTRATO

11.1 O prazo de vigência do Contrato será de 04 (quatro) meses, contados a partir da emissão da OS.

12 DO FORNECIMENTO

12.1 A prestação dos serviços deverá ser realizada nas dependências da Sede do SAAE Jacareí sito à Rua Miguel Leite do Amparo, 121 – Jacareí.

13 DAS CONDIÇÕES DE PAGAMENTO

15.1 O pagamento da instalação dos equipamentos ocorrerá após a implentancao da solução na autarquia.

15.2 Os demais pagamentos ocorrerão mensalmente, com a emissão de 1(uma) nota fiscal a cada 30 dias correspondentes à execução dos serviços prestados.

15.3 O prazo de pagamento da prestação de serviços será conforme condições de pagamento da Autarquia e de acordo com o cronograma de desembolso.

14 TABELA REFERÊNCIA PARA FORMAÇÃO DE PREÇO DO OBJETO

ITEM	DESCRIÇÃO	QTDE		VALOR UNITÁRIO		VALOR TOTAL
A	SERVIÇO DE INSTALAÇÃO	1			R$ X	R$ X
ITEM	**DESCRIÇÃO**	**QTDE**	**MESES**	**VALOR UNITÁRIO**	**VALOR MENSAL**	**VALOR ANUAL**
B	APPLIANCE (HÁ) PARA SOLUÇÃO DE SEGURANÇA UTM DE 5 GBPS DE CAPACIDADE DE FIREWALL COM SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO – LICENÇA DE USO E SUPORTE TECNICO	2	4	R$ X	R$ X	R$X
					VALOR TOTAL GLOBAL	R$X

Joyce da Silva Cordeiro
Supervisora
Unidade Tecnologia de Informação

Eric dos S. Burgomeister
Diretor de Departamento Administrativo

ANEXO II

PLANILHA DE CUSTO - PROPOSTA

Ao
SAAE – SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE JACAREÍ
PREGÃO Nº _____/_____
NOME DA EMPRESA
N° CNPJ

NOME DA EMPRESA, pessoa jurídica de direito privado, inscrita no CPNJ n° _____ e inscrição municipal/estadual n° _____, estabelecida a_____, bairro _____, Município de_____, estado de _____ CEP_____, telefone/ fax: XXXXXXXXXX, Dados Bancários (nº da conta corrente, agência e respectivo banco), e-mail: XXXXXXXXXXXX, propõe ao Serviço Autônomo de Água e - SAAE de Jacareí, para execução dos serviços descritos no termo de referência, a seguinte Proposta de Preços:

ITEM	DESCRIÇÃO	QTDE		VALOR UNITÁRIO		VALOR TOTAL
A	SERVIÇO DE INSTALAÇÃO	1			R$ XXXX	R$ XXXX
ITEM	**DESCRIÇÃO**	**QTDE**	**MESES**	**VALOR UNITÁRIO**	**VALOR MENSAL**	**VALOR ANUAL**
B	APPLIANCE PARA SOLUÇÃO DE SEGURANÇA UTM DE 5 GBPS DE CAPACIDADE DE FIREWALL COM SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO – LICENÇA DE USO E SUPORTE TECNICO	2	4	R$ XXXX	R$ XXXX	R$ XXXX
					VALOR TOTAL GLOBAL	R$ XXXX

Informar marca e modelo do equipamento a ser fornecido.

XXXXXXXXXXX, ____ de _____ de 2024.

_____

Assinatura devidamente identificada do representante legal da empresa proponente (apontado no contrato social ou procuração com poderes específicos).