ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Aquisição de solução de Software de segurança da informação do tipo UTM (Unified Threat Management) que tenha a capacidade de integrar em um único dispositivo: filtro de pacotes com controle de estado, camada de antivírus, filtro de conteúdo WEB, VPN, IDS/IPS, balanceamento de carga, QoS e Proxy reverso. Todos os produtos e serviços deverão ser orçados para um período mínimo de contrato de 12 meses.:

ITEM	DESCRIÇÃO
1	LICENCIAMENTO DE USO DE SOFTWARE DE SOLUÇÃO DE SEGURANÇA UTM PARA ATÉ 100 USUÁRIOS IP COM SISTEMA DE CATEGORIZAÇÃO DE URL PARA 100 USUÁRIOS
2	GARANTIA E ATUALIZAÇÃO DE SOFTWARE 1 ANO

2. JUSTIFICATIVA e OBJETIVO

Tendo em vista a necessidade de aquisição do produto AKER FIREWALL UTM, através de Dispensa de Licitação, amparada pelo Art. 24, II, da Lei 8.666/93, que dispõe sobre Licitações e Contratos Administrativos. A necessidade de segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente, infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação, entre outros, assim implementando os atributos básicos dos padrões internacionais (ISO/IEC 17799:2005), que são eles: Confidencialidade, Integridade e Disponibilidade, o que acarretou um significativo aumentando a produtividade de todos os setores, também evitando que os usuários acessem serviços ou sistemas indevidos, além de ter o controle sobre as ações realizadas na rede, sendo possível até mesmo descobrir quais usuários as efetuaram. A Segurança da Informação refere-se à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às pessoais. A aquisição do produto justifica e para permitir o desenvolvimento das atividades do Município, que objetiva trabalhar para o crescimento e bem estar dos munícipes de São Joaquim.

.

3. CLASSIFICAÇÃO DOS BENS COMUNS

3.1. Os serviços a serem adquiridos enquadram-se na classificação de bens comuns, nos termos da Lei n° 10.520, de 2002, do Decreto n° 3.555, de 2000, e do Decreto 5.450, de 2005.

4. ESPECIFICAÇÕES DO SERVIÇO

LICENCIAMENTO DE USO DE SOFTWARE DE SOLUÇÃO DE SEGURANÇA UTM PARA ATÉ 100 USUÁRIOS IP COM SISTEMA DE CATEGORIZAÇÃO DE URL PARA 100 USUÁRIOS

4.1 CARACTERÍSTICAS GERAIS

4. 1. 1. Ser licenciado seu uso para pelo menos 100 de IPs/usuários pelo período do contrato;

4. 1. 2. Não limitar o quantitativo de canais VPN site-to-site simultaneos;
4. 1. 3. Possuir manual de usuário completo, ajuda on-line, interface de administração e demais documentos correlatos em português;
4. 1. 4. Possuir sistema operacional customizado especificamente para funções de UTM. Não serão aceitos sistemas de firewall que sejam executados sobre sistemas operacional em versões ou configurações distribuídas comumente no mercado, como o Novell NetWare, Microsoft Windows, Linux ou FreeBSD;
4. 1. 5. Possuir uma interface para configuração e gerenciamento através de interface de linha de comando CLI (Command Line Interface);
4. 1. 6. Deve permitir a instalação em servidores físicos e em sistemas de virtualização como VMware, Xen, Oracle VM VirtualBox ou Microsoft Hyper-V.

4. 2. CARACTERÍSTICAS DO SOFTWARE PARA SOLUÇÃO DE SEGURANÇA UTM:

4. 2. 1. Efetuar controle de tráfego por estado no mínimo para os protocolos TCP, UDP e ICMP baseados nos endereços de origem, destino e porta;
4. 2. 2. Suportar o *Internet Protocol* Versões 4 (IPv4)
4. 2. 3. Suportar o *Internet Protocol* Versões 6 (IPv6), deverão estar em conformidade com as RFCs listadas abaixo:
4. 2. 3. 1. RFC2460 - Internet Protocol, Version 6 (IPv6) Specification;
4. 2. 3. 2. RFC4291 - IP Version 6 Addressing Architecture;
4. 2. 3. 3. RFC3484 - Default Address Selection for Internet Protocol version 6 (IPv6);
4. 2. 3. 4. RFC4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification;
4. 2. 3. 5. RFC4862 - IPv6 Stateless Address Autoconfiguration;
4. 2. 3. 6. RFC1981 - Path MTU Discovery for IP version 6;
4. 2. 3. 7. RFC4861 - Neighbor Discovery for IP version 6 (IPv6);
4. 2. 3. 8. RFC4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers.
4. 2. 4. Suportar o protocolo 802.1q, para uso e segmentação da rede com VLANs;
4. 2. 5. Suportar o protocolo 802,1ax e 802.3ad (LACP), Link Aggregation Control Protocol;
4. 2. 6. Dispõe de servidor DHCP interno e permite DHCP relay;
4. 2. 7. Suportar PIM (Protocol Independent Multicast);
4. 2. 8. Suportar o protocolo Distance-Vector Multicast Routing Protocol (DVMRP);
4. 2. 9. Pode ser integrado com servidores de Network Time Protocol (NTP);
4. 2. 10. Suporta funcionar em modo BRIDGE (transparente mode) esta funcionalidade permite que o Firewall funcione em modo transparente/oculto na rede, impossibilitando sua identificação, otimizando o tempo de configuração e diminuindo a intervenção humana neste processo;
4. 2. 11. Capacidade para trabalhar com conversão de endereços e portas (NAT/NAPT) conforme RFC 3022;
4. 2. 12. Suportar no mínimo os seguintes protocolos de roteamento dinâmico IPv4: RIP1, RIP2, OSPF e BGP;
4. 2. 13. O equipamento deverá suportar o registro do dispositivo dinamicamente, pelo seu endereço IP de WAN, em pelo menos 5 (cinco) provedores de serviços de DDNS;

4. 2. 14. Possuir e fornecer manual escrito e em mídia eletrônica para todos os equipamentos e softwares componentes da solução;
4. 2. 15. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo, RTSP, H.323 e PPTP mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro;
4. 2. 16. Possuir interface em Inglês ou português brasileiro;
4. 2. 17. AUTENTICAÇÃO:
    4. 2. 17. 1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP, HTTPS e Gopher, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea;
    4. 2. 17. 2. Permitir a utilização de LDAP, LDAP/SSL, LDAP/TLS, RADIUS, hardware tokens (SecureID ou equivalente), certificados X.509 (gravados em disco e/ou em tokens criptográficos/smartcards) e sistema S/KEY para a autenticação de usuários;
    4. 2. 17. 3. Permitir o cadastro dos usuários e grupos em base de dados própria por meio da interface de gerencia remota do dispositivo;
    4. 2. 17. 4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs (Certificates Revogation Lists) emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo dispositivo via protocolos HTTP e LDAP;
    4. 2. 17. 5. Permitir o controle de acesso por usuário, para plataformas Windows NT, 2000, 2003, 2008, XP, Vista, Windows 7 e Windows 8 de forma transparente (sem a necessidade do usuário digitar novamente a senha), para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;
    4. 2. 17. 6. Permitir o controle de acesso por usuário, para todas as plataformas com browser através de autenticação via formulário para todos os serviços suportados, de forma que um determinado usuário tenha seu perfil de acesso automaticamente configurado;
    4. 2. 17. 7. Possuir perfis de acesso hierárquicos;
    4. 2. 17. 8. Permitir a atribuição de perfil de acesso à usuário ou grupo de usuários de acordo com o endereço ou range IP do equipamento que o usuário esteja utilizando;

4. 2. 18. POLÍTICA DE TRÁFEGO:
    4. 2. 18. 1. Permitir o agrupamento das regras de filtragem por política;
    4. 2. 18. 2. Prover mecanismo que permita a especificação de datas de validade inicial e final, para regras de filtragem, individualmente (por regra);
    4. 2. 18. 3. Prover mecanismo que permita a especificação da validade para regras de filtragem, individualmente (por regra), por dia da semana e horário;
    4. 2. 18. 4. Permitir a visualização pela interface gráfica, em tempo real, de todas as conexões TCP e sessões UDP ativas através do dispositivo e a finalização de qualquer uma destas sessões ou conexões;

4. 2. 18. 5. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em dado momento;

4. 2. 18. 6. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;

4. 2. 18. 7. Possuir mecanismo que permita capturar o tráfego de rede em tempo real (sniffer) via interface gráfica, com visualização em tempo real pela interface gráfica e com capacidade para exportação dos dados capturados para arquivo no mínimo em formato PCAP;

4. 2. 18. 8. A utilização da funcionalidade de captura de pacotes (sniffer) não deverá causar nenhuma queda de desempenho (*throughput)* do equipamento;

4. 2. 18. 9. Permitir configuração de filtros para a captura do tráfego em tempo real, no mínimo por protocolo, endereço IP de origem e/ou destino e porta de origem e/ou destino, utilizando para tanto linguagem textual;

4. 2. 18. 10. Permitir a visualização do tráfego de rede em tempo real (sniffer) tanto nas interfaces de rede do dispositivo quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT/NAPT (tradução de endereços) é eliminado;

4. 2. 18. 11. Permitir a execução de até oito capturas de tráfego em tempo real simultaneamente, inclusive em pontos diferentes ou com filtros diferentes;

4. 2. 19. SEGURANÇA:

4. 2. 19. 1. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;

4. 2. 19. 2. Prover proteção contra os ataques de negação de serviço *SYN Flood, Land, Tear Drop e Ping O'Death*;

4. 2. 19. 3. Possuir mecanismo que limite o número máximo de conexões simultâneas de um mesmo cliente para um determinado serviço e/ou servidor;

4. 2. 19. 4. Detectar automaticamente e inserir regras de bloqueio temporárias para varreduras de portas efetuadas contra o dispositivo ou contra qualquer máquina protegida por esse, mesmo que realizados em períodos maiores que 1 (um) dia;

4. 2. 19. 5. Permitir integração com sistema detecção de intrusão (IDS) externo, permitindo que esses agentes insiram regras temporárias no dispositivo em caso de detecção de algum ataque, com duração pré-determinada, de forma automática;

4. 2. 19. 6. Possuir sistema de prevenção de intrusão (IPS) nativo, permitindo o bloqueio do ataque em caso de detecção do mesmo;

4. 2. 19. 7. Possuir filtro de aplicações de modo a permitir a identificação de padrões de dados dentro das conexões, possibilitando o tratamento automático (bloqueio, liberação ou redução/aumento de banda) de aplicações do tipo peer-to-peer, de download de arquivos, entre outros;

4. 2. 20. PROXIES ESPECIALIZADOS:

4. 2. 20. 1. Possuir proxy SOCKS, permitindo que clientes da versão 4 e 5 deste protocolo acessem a Internet através do dispositivo;

4. 2. 20. 2. Possuir mecanismo de filtragem de serviços RPC pelo nome do serviço ou, no caso de serviço sem nome pré-definido, pelo seu número;

4. 2. 20. 3. Possuir Proxy nativo para tráfego HTTP, HTTPS, SIP, H323, FTP, SMTP, POP3, RTSP, Real Áudio, DCE-RPC, PPTP e TELNET;

4. 2. 20. 4. Possibilitar o gerenciamento completo e a implantação de quotas para navegação web a um determinado usuário ou a um grupo de usuários, de acordo com o perfil de acesso, sendo baseada em volume de dados ou em tempo de utilização do serviço;

4. 2. 20. 5. O Proxy HTTP deverá possuir mecanismo que bloqueie Banners, ActiveX, Java, Javascript, e ainda tentativas de navegação informando na URL apenas o número IP;

4. 2. 20. 6. Permitir visualização dos sites acessados em tempo real;

4. 2. 20. 7. Permitir a inclusão de macros enviada para a página de redirecionamento (no caso de bloqueio de categorias) com a categoria na qual o site bloqueado se encontrava;

4. 2. 20. 8. Permitir a inserção de uma URL de redirecionamento para bloqueio por palavras-chave nas regras de perfil para HTTP, FTP, Gopher e tipos de arquivos bloqueados;

4. 2. 20. 9. Permitir a filtragem de URLs, para os protocolos HTTP, HTTPS, FTP e Gopher, por usuário, permitindo a definição de perfis de acesso diferenciados para cada usuário ou grupo;

4. 2. 20. 10. Suportar a filtragem do protocolo HTTPS pelo campo "CommonName" do certificado digital;

4. 2. 20. 11. Permitir a remoção de anúncios em páginas HTML, sem que as mesmas percam formatação ou apresentem mensagens de erro;

4. 2. 20. 12. Implementar Proxy transparente para o protocolo HTTP e HTTPS, de forma a dispensar a configuração dos browsers das máquinas clientes para a utilização das características dos dois itens acima;

4. 2. 20. 13. Possuir funcionalidade de bloquear ou liberar a navegação web dependendo do navegador (browser) que o usuário estiver utilizado;

4. 2. 20. 14. Implementar sistema que possibilite a reescrita de URLs;

4. 2. 20. 15. Implementar sistema que possibilite a concatenação (Stripping) de cabeçalho HTTP;

4. 2. 20. 16. Implementar sistema que possibilite a adição de cabeçalho HTTP;

4. 2. 20. 17. Possuir mecanismo de proxy SSL reverso, permitindo que VPNs cliente-servidor sejam estabelecidas com o dispositivo, de forma transparente, e então redirecionadas para qualquer servidor interno da rede, sem o uso de cliente de criptografia específico e com autenticação opcional de usuários via certificados digitais padrão X.509;

4. 2. 20. 18. Permitir o uso certificados digitais com chaves de tamanho até 4096 bits no proxy SSL reverso;

4. 2. 20. 19. Possuir mecanismo que limite opcionalmente o uso do proxy SSL reverso para serviços e servidores específicos de acordo com perfis de acesso atribuídos a usuários e grupos de usuários;

4. 2. 20. 20. Permitir o controle de acesso por usuário e grupos para controle de IMs como Skype, Google Talk, Yahoo Messenger e Facebook Messenger.

4. 2. 20. 21. Possui a capacidade de identificar o tráfego Web e classifica-lo de acordo com as aplicações e sub aplicações trafegando na rede, tais como redes sociais: Facebook, Google+, Twitter, etc; de comunicação: Skype, Gmail, GTalk, etc;

4. 2. 20. 22. Permite identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Ultrasurf, Skype e ataques mediante a porta 443;

4. 2. 20. 23. Suporta a detecção de aplicações dinâmicas dentro de sessões de proxy HTTP;

4. 2. 20. 24. Deve permitir o armazenamento em Cache de conteúdo trafegados pelo protocolo HTTP e HTTPS;

4. 2. 20. 25. Possuir sistema de cache interno, armazenando requisições WEB em disco local;

4. 2. 20. 26. Possibilitar a integração com servidores de cache WEB externos;

4. 2. 20. 27. Possibilitar a integração com cache WEB externos hierarquicos utilizando ICP (Internet Cache Protocol);

4. 2. 20. 28. Possuir a funcionalidade de eliminar o conteúdo do Cache (limpar o Cache);

4. 2. 21. VPN:

4. 2. 21. 1. Prover serviço VPN (Virtual Private Network) para pacotes IP e VPN SSL, com chaves de criptografia com tamanho igual ou superior a 128 bits, de forma a possibilitar a criação de canais seguros ou VPNs através da Internet;

4. 2. 21. 2. Suportar padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;

4. 2. 21. 3. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

4. 2. 21. 4. Mostrar, em tempo real, um gráfico de uso das VPNs IPSEC estabelecidas, permitindo auferir o tráfego em cada uma delas e as SPIs negociadas e ativas;

4. 2. 21. 5. Deverá fornecer no mínimo 50 licenças para conexões simultâneas de clientes VPNs (client-to-server) conforme especificações a abaixo:

4. 2. 21. 6. Possibilitar mecanismo de criação de VPNs entre máquinas Windows NT, 2000, 2003, XP, Vista, Windows 7, Windows 8, Linux e Mac OS e o dispositivo, com chaves de criptografia simétricas com tamanho igual ou superior a 128 bits;

4. 2. 21. 7. Funcionar como um provedor de VPN para clientes, de modo a atribuir aos clientes endereços IPs das redes internas, colocando-os, virtualmente, dentro das mesmas (0 hops);

4. 2. 21. 8. Prover cliente VPN para as plataformas Windows 2000, 2003, XP, Vista, Windows 7, Windows 8 e Linux, que permita uso de chaves criptográficas simétricas com 128 ou mais bits;

4. 2. 21. 9. O cliente de tunelamento de rede IP deverá ser, para clientes Windows e Linux, executar com privilégios básicos de

usuário comum. Esta funcionalidade não é exigida apenas durante a primeira instalação do cliente;

4. 2. 21. 10. Deverá ser possível configurar o endereço/range IP a ser atribuído a placa de rede virtual do cliente de VPN, bem como sua máscara de rede, endereços dos servidores DNS, endereço dos servidores WINS, rota default e rotas para sub-redes;

4. 2. 21. 11. No VPN cliente/firewall deverá ser possível a configuração do envio ou não de pacotes broadcast da rede onde o servidor se encontra para o cliente;

4. 2. 21. 12. O cliente de VPN deverá possibilitar que seu funcionamento seja sincronizado ou não com o dial-up do Windows, possibilitando que ele estabeleça a VPN automática e imediatamente depois de se ter estabelecido uma conexão discada;

4. 2. 21. 13. Na VPN cliente/firewall deve ser possível especificar e fixar quais são as portas usadas na comunicação entre o cliente e o servidor;

4. 2. 21. 14. Suportar VPN Failover (re-estabelecimento da VPN sobre um segundo enlace caso haja falha no enlace principal);

4. 2. 21. 15. A solução de VPN deverá trabalhar no mínimo com os seguintes protocolos: IPSEC, PPTP, L2TP, SSL;

4. 2. 21. 16. Possuir funcionalidade Dead Peer Detection (DPD), ou similar;

4. 2. 21. 17. Prover funcionalidade de VPN SSL, com o estabelecimento do túnel VPN e autenticação via browser;

4. 2. 21. 18. A conexão VPN SSL deverá ser totalmente transparente para o usuário final, de forma que seja realizado o download e instalação do Applets, assim que necessários;

4. 2. 21. 19. Deve ter a capacidade para fazer o download do Software Client da VPN SSL direto do dispositivo;

4. 2. 21. 20. Disponibilidade de Software SSL-Client para no mínimo: Windows XP, Windows Vista, Windows 7, Windows 8, Linux e Mac OS;

4. 2. 21. 21. Deverá permitir a integração de algoritmos de terceiros em seus sistemas criptográficos sem intervenção de terceiros, Hardware ou Software, sujeito exclusivamente as normas Brasileiras.

4. 2. 21. 22. Possuir capacidade de integração de algoritmos de estado, em hardware, em seu sistema criptográfico, sujeito exclusivamente as normas Brasileiras.

4. 2. 22. MONITORAMENTO E ADMINISTRAÇÃO:

4. 2. 22. 1. Possuir suporte ao protocolo SNMP (v1, 2 e 3), através de MIB2;

4. 2. 22. 2. Permitir em tempo real a visualização de estatísticas do uso de CPU, memória do dispositivo, bem como o tráfego de rede em todas as interfaces do dispositivo através da interface gráfica remota, de forma gráfica ou em tabelas;

4. 2. 22. 3. Caso o dispositivo utilize agentes externos para divisão de processamento (antivírus, filtro de conteúdo, IDS ou Anti-spam) o dispositivo deverá permitir a verificação em tempo real da comunicação com estes agentes;

4. 2. 22. 4. Possuir sistema de alerta que informe o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de traps SNMP;

4. 2. 22. 5. Permitir a criação de perfis de administração baseado em papéis (role-based), de forma a possibilitar a definição de diversos administradores para o dispositivo, cada um responsável por determinada tarefa da administração;

4. 2. 22. 6. Permitir a conexão simultânea de vários administradores, sendo apenas um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas;

4. 2. 22. 7. Permitir que o segundo administrador ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração;

4. 2. 22. 8. Fornecer gerência remota, com interface gráfica nativa, através de canal criptografado com chave de criptografia igual ou superior a 128 bits, para plataformas Windows Me, Windows NT/2000/XP/2003/2008/Vista/Windows 7/Windows 8 e Linux;

4. 2. 22. 9. Capacidade para criação de entidades/objetos, que podem ser um IP, um range IP ou um dispositivo, etc. para facilitar a administração;

4. 2. 22. 10. Possibilitar drag-and-drop (arrastar e soltar) para criação e alteração de regras, por meio da interface gráfica;

4. 2. 22. 11. A interface gráfica deverá possuir mecanismo que permita a gerência remota de múltiplos dispositivos sem a necessidade de se executar várias interfaces;

4. 2. 22. 12. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do dispositivo, incluindo a configuração de VPNs, NAT, perfis de acesso e regras de filtragem;

4. 2. 22. 13. Possuir mecanismo que permita a realização de cópias de segurança (backups) e restauração remota, através da interface gráfica, sem necessidade do reinício do sistema;

4. 2. 22. 14. Deverá ser capaz de executar um backup por linha de comando e oferecer a opção de salvar o arquivo de backup localmente ou exportar usando o protocolo FTP;

4. 2. 22. 15. Possuir mecanismo que possibilite a aplicação de correções e atualizações para o dispositivo de forma remota por meio da interface gráfica;

4. 2. 22. 16. Possuir mecanismo anti-suicídio para a administração remota, evitando que o administrador perca o acesso ao dispositivo por uma configuração incorreta;

4. 2. 22. 17. Permitir de integração com produto de gerenciamento centralizado de múltiplos dispositivos;

4. 2. 22. 18. Possuir interface orientada a linha de comando (Command Line Interface) para a administração do dispositivo a partir do console;

4. 2. 22. 19. Suportar o rollback (voltar para a versão anterior) de *patches* aplicados;

4. 2. 23. LOG:

4. 2. 23. 1. Prover mecanismo de consulta às informações registradas (logs) por meio da interface gráfica de administração;

4. 2. 23. 2. Possibilitar o armazenamento de seus registros (log e/ou eventos) em máquina remota em plataformas Windows Server (NT/2000/2003/2008) ou Unix, através de protocolo criptografado ou SYSLOG;

4. 2. 24. RELATÓRIOS:

4. 2. 24. 1. Possibilitar a geração de pelo menos os seguintes tipos de relatório, publicados em formato HTML, TXT e PDF:
4. 2. 24. 2. Máquinas mais acessadas;
4. 2. 24. 3. Serviços mais utilizados;
4. 2. 24. 4. Usuários que mais utilizaram serviços;
4. 2. 24. 5. URLs mais visualizadas;
4. 2. 24. 6. Categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web);
4. 2. 24. 7. Categoria do site bloqueado (em caso de existência de um filtro de conteúdo Web);
4. 2. 24. 8. Downloads realizados;
4. 2. 24. 9. Downloads bloqueados;
4. 2. 24. 10. Endereço IP acessado pelo proxy Web;
4. 2. 24. 11. Endereço IP bloqueado pelo proxy Web;
4. 2. 24. 12. Quota – bytes consumidos;
4. 2. 24. 13. Quota – tempo consumidos;
4. 2. 24. 14. Sites acessados;
4. 2. 24. 15. Sites Bloqueados;
4. 2. 24. 16. Maiores emissores/receptores de e-mail;
4. 2. 24. 17. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML, TXT e PDF:
4. 2. 24. 18. Máquinas acessadas X serviços bloqueados;
4. 2. 24. 19. Usuários X URLs acessadas;
4. 2. 24. 20. Usuários X categorias Web bloqueadas (quando utilizado com filtragem de conteúdo Web);
4. 2. 24. 21. Possibilitar a geração dos relatórios dos itens acima sob demanda e através de agendamento diário, semanal, mensal, período específico ou por demanda pelo menos nos formatos HTML, TXT e PDF;
4. 2. 24. 22. Permitir publicação automatizada dos relatórios utilizando FTP em pelo menos três equipamentos distintos;
4. 2. 24. 23. Permitir exportação dos registros (logs) no mínimo em formato TXT e CSV;

4. 2. 25. QOS:
4. 2. 25. 1. Implementar mecanismo de divisão justa de largura de banda (QoS), permitindo a priorização de tráfego por regra de filtragem, por usuário ou ainda priorizando acesso a sites por categoria ou palavra-chave;
4. 2. 25. 2. Implementar mecanismo de limitação de banda através da criação de canais virtuais, permitindo que os mesmos serem alocados por regra de filtragem e por usuário;
4. 2. 25. 3. Permitir modificação (remarcação) de valores DSCP para o DiffServ;
4. 2. 25. 4. Implementar no mínimo 07 classes de serviço distintas, com configuração do mapeamento e marcação para códigos DSCP através da interface gráfica;
4. 2. 25. 5. Suporta priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

4. 2. 26. BALANCEAMENTO:
4. 2. 26. 1. Suportar o uso simultâneo de múltiplos links em um mesmo firewall, de provedores distintos ou não, sendo o

firewall o responsável por dividir o tráfego entre os distintos links;

4. 2. 26. 2. Permitir o balanceamento de links com IPs dinâmicos para ADSL, ou outra tecnologia de banda larga que não utilize IP Fixo;

4. 2. 26. 3. Implementar mecanismo de balanceamento de carga, permitindo com que vários servidores internos, sejam acessados externamente pelo mesmo endereço IP. O balanceamento de canal deverá monitorar os servidores internos e, em caso de queda de um destes, dividir o tráfego entre os demais, automaticamente;

4. 2. 26. 4. Implementar mecanismo de persistência de sessão para o balanceamento de carga, através de diversas conexões, para quaisquer protocolos suportados pelos servidores sendo balanceados;

4. 2. 26. 5. O balanceamento de carga deverá ainda possibilitar que os servidores sejam monitorados através do protocolo ICMP ou requisições HTTP. Ele deverá também possuir pelo menos dois algoritmos distintos de balanceamento;

4. 2. 27. CLUSTER:

4. 2. 27. 1. A solução deve suportar funcionamento com 2 (dois) ou mais equipamentos idênticos, de forma que funcione com tolerância a falhas (ativo/passivo) ou alta performance (ativos/ativos), onde poderá trabalhar no mínimo de duas formas, de acordo com a necessidade da instalação. Sendo elas:

4. 2. 27. 2. Os dois dispositivos são ligados em paralelo, com réplicas do estado de conexões entre eles. O dispositivo secundário não estará tratando o tráfego, ele entrará em funcionamento para tratamento de tráfego somente quando o dispositivo principal cair, sem que se tenha perda de conexão, de canal VPN, usuários autenticados e IPs bloqueados pelo IPS/IDS;

4. 2. 27. 3. Dois ou mais dispositivos devem estar em funcionamento simultaneamente, balanceando o tráfego de rede entre eles de forma automática e replicando configuração, estado das conexões entre eles e também de forma automática, sem que se tenha perda de conexão, de canal VPN, usuários autenticados e IPs bloqueados pelo IPS/IDS em caso de falha de algum equipamento. Nesta modalidade, podem ser colocados até 64 firewalls em paralelo;

4. 2. 27. 4. Deverá ser capaz de manter o sincronismo entre as seguintes configurações como Regras de Firewall, Regras de NAT, Entidades, Contas administrativas, Configuração de VPN, Configurações de rede, Roteamento estático, Roteamento dinâmicas, Perfis e bases de antivírus, filtros web, anti-spam e IDS/IPS.

4. 2. 28. Filtro de acesso WEB com atualização de URL´s para UTM para até 100 usuários:

4. 2. 28. 1. A base de conhecimento WEB, que irá executar dentro do próprio appliance sem a necessidade de utilização de outro servidor, deve ser fornecido, durante todo o contrato, com todas as atualizações de bases de URLs, categorias, software embarcado, e deverá conter as seguintes características:

4. 2. 28. 2. Deverá fornecer filtro de acesso web conforme especificações a abaixo:

4. 2. 28. 3. Possuir capacidade para efetuar classificação de URLs, de maneira a bloquear acesso a páginas WEB, para usuários ou grupo deles, a partir de categorias genéricas;

4. 2. 28. 4. Possuir pelo menos 75 categorias de classificação de URLs a serem consultadas no analisador de URLs do item anterior;

4. 2. 28. 5. Deverão ser fornecidas todas as atualizações de software assim como a atualização da base de conhecimento (URLs categorizadas), sem custo adicional, por todo o período do contrato;

4. 2. 28. 6. Possibilitar agendamento mensal e semanal do download automático das atualizações das URLs;

4. 2. 28. 7. Possuir mecanismo que permita fazer download apenas das novas atualizações diárias e não da base completa, de modo a economizar banda do link com a Internet;

4. 2. 28. 8. Possui pelo menos 16.000.000 (Dezesseis Milhões) de URLs classificadas;

4.3 GARANTIA E ATUALIZAÇÃO DE SOFTWARE

4.3.1 Atualização do software embarcado durante o período de 12 meses;

4.3.2 Atualização do sistema operacional embarcado durante o período de 12 meses;

4.3.3 No preço deverá estar incluído todo o software necessário para atender as características exigidas, bem como as atualizações para todas as versões do produto que forem lançadas durante o período do contrato;

5. VALOR ESTIMADO

5.1. O valor máximo a ser gasto com a presente contratação é de R$ 3.284,86.

5.2. O custo estimado foi apurado a partir de mapa de preços constante do processo administrativo, elaborado com base em orçamentos recebidos de empresas especializadas.

6. PRAZOS E FORMA DE EXECUÇÃO

6.1. Os serviços deverão ser efetuados através de Autorização de Fornecimento, onde a empresa contratada efetuará a entrega, nas quantidades solicitadas, no prazo máximo 10 (dez) dias úteis, após solicitação e Autorização de Fornecimento expedido pelo solicitante.

6.2. É responsabilidade da empresa fornecedora a realização dos serviços nas quantidades, no horário e data estipulada, bom como nas condições estabelecidas nesse termo.

6.3. Serão recebidos apenas os itens e serviços nas quantidades estabelecidas nas Autorizações de Fornecimento. A empresa contratada deverá seguir as orientações dos fiscais de contrato.

6.4. Em caso de não cumprimento das especificações exigidas na prestação do serviço, a empresa contratada deverá efetuar a regularização no prazo máximo de 48 (quarenta e oito) horas, arcando com todas as despesas decorrentes.

6.5. Apresentadas irregularidades pelo fiscal a contratada será notificada e terá prazo de 10 dias para proceder à regularização. Findo esse prazo, em não se manifesto ou não regularizando, o Gestor de Contrato certificará o fato e submeterá ao Ordenador de

Fls. 09

Despesa (Prefeito Municipal) para que se manifeste quanto à rescisão contratual.

6.6. Apresentada a Nota Fiscal, caberá ao fiscal do contrato atestar a regular entrega dos itens e serviços, encaminhando o documento para as providências relativas aos pagamentos aprovados pela fiscalização.

6.7. A Contratada deverá reparar, ou quando isto for impossível, indenizar por danos materiais e/ou pessoais decorrentes de erro na execução dos serviços, objeto do presente termo de referência, que sobrevenha em prejuízo da Contratante ou de terceiros, sem quaisquer ônus para a Contratante.

6.8. A Contratada deverá responsabilizar-se pelos danos causados diretamente à Contratante ou a terceiros, decorrentes de sua culpa ou dolo na execução do Contrato.

6.9. A Contratada deverá responsabilizar-se por todo o ferramental, dispositivos e aparelhos adequados à perfeita execução do Contrato.

6.10. Após a conclusão dos serviços, o documento de aceitação do serviço deverá ser assinado por responsável do Departamento de Tecnologia da Informação da Prefeitura de São Joaquim, certificando o cumprimento da instalação e o bom funcionamento.

□

7. OBRIGAÇÕES DA CONTRATADA

7.1. A Contratada obriga-se a:

7.1.1. Efetuar a entrega dos bens em perfeitas condições, no prazo e local indicados pela Administração, em estrita observância das especificações do Edital e da proposta, acompanhado da respectiva nota fiscal constando detalhadamente as indicações da marca, fabricante, modelo, tipo, procedência e prazo de garantia;

7.1.2. Responsabilizar-se pelos vícios e danos decorrentes do produto, de acordo com os artigos 12, 13, 18 e 26, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

7.1.2.1. O dever previsto no subitem anterior implica na obrigação de, a critério da Administração, substituir, reparar, corrigir, remover, ou reconstruir, às suas expensas, no prazo máximo de **10(dez) corridos**, o produto com avarias ou defeitos;

7.1.3. Atender prontamente a quaisquer exigências da Administração, inerentes ao objeto da presente licitação;

7.1.4. Comunicar à Administração, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

7.1.5. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

7.1.6. Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, exceto nas condições autorizadas no Termo de Referência ou na minuta de contrato;

7.1.7. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos,

exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

7.1.8. Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do contrato.

8. OBRIGAÇÕES DA CONTRATANTE

8.1. A Contratante obriga-se a:

8.1.1. Receber provisoriamente o material, disponibilizando local, data e horário;

8.1.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivos;

8.1.3. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de servidor especialmente designado;

8.1.4. Efetuar o pagamento no prazo previsto.

9. MEDIDAS ACAUTELADORAS

9.1. Consoante o artigo 45 da Lei nº 9.784, de 1999, a Administração Pública poderá, sem a prévia manifestação do interessado, motivadamente, adotar providências acauteladoras, inclusive retendo o pagamento, em caso de risco iminente, como forma de prevenir a ocorrência de dano de difícil ou impossível reparação.

10. CONTROLE DA EXECUÇÃO

10.1. A fiscalização da contratação será exercida por um representante da Administração, ao qual competirá dirimir as dúvidas que surgirem no curso da execução do contrato, e de tudo dará ciência à Administração.

10.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da fornecedora, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior, e, na ocorrência desta, não implica em co-responsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

10.3. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das faltas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

Fls. 10V

11. CONSIDERAÇÕES

Fiscal do Contrato: Ernesto Eduardo de Melo Lemos

Gestora de Contratos: Andréa Neves de Souza

Dotação nº 05 fonte de recurso 5000 projeto atividade 2.003

São Joaquim, 14 de Julho de 2021.

Daniele Hugen Rodrigues
Cargo/carimbo
Secretário de Administração

Aprovo, em 14de Julho de 2021.

GIOVANI NUNES
PREFEITO MUNICIPAL
APROVO O PRESENTE TERMO DE REFERÊNCIA E AUTORIZO A REALIZAÇÃO DA LICITAÇÃO.
(inciso II, Art. 9º, Decreto nº 5.450/05)

ciente em 14 de Julho de 2021.
ERNESTO EDUARDO DE MELO LEMOS
Técnico de Informática
Matr. 10.341

Ernesto Eduardo de Melo Lemos
Técnico em informática