CONSULTA PÚBLICA Nº 2/2017

A Câmara Municipal de Belo Horizonte - CMBH, inscrita no CNPJ sob o nº 17.316.563/0001-96, com sede na Avenida dos Andradas, n° 3.100, Bairro Santa Efigênia, nesta Capital, por intermédio da Comissão Permanente de Licitação - CPL, designada pelas Portarias n.º 16.999, 17.060, 17.185 e 17.189 publicadas no DOM/BH dos dias 24/1/2017, 18/2/2017, 13/05/2017 e 18/05/2017, respectivamente, torna público que fará realizar Consulta Pública, conforme abaixo:

■ **OBJETIVO:** Colocar para apreciação geral, sob ampla participação, Termo de Referência que tem por objeto **a aquisição de solução de proteção de redes com características de "Next Generation Firewall – NGFW" para segurança de informação perimetral, conforme especificado**, para que os interessados em participar da Consulta Pública possam apresentar críticas e sugestões .

■ **PRAZO: durante 15 (quinze) dias úteis,** a contar da última publicação do aviso desta Consulta Pública.

Anexo deste Edital, constituindo um só e indivisível documento:

a) ANEXO TERMO DE REFERÊNCIA para apreciação.

1 - DA FORMA DE PARTICIPAÇÃO

1.1 - A Consulta Pública será aberta a todos os interessados.

1.2 - O Termo de Referência a ser apreciado está disponibilizado no endereço eletrônico "**http://www.cmbh.mg.gov.br/transparencia/licitacoes**."

1.3 - As sugestões e as críticas poderão ser apresentadas por via postal ou eletronicamente (***cpl@cmbh.mg.gov.br***), além de poderem ser protocoladas na Seção de Apoio a Licitações, no horário de 9:00 às 18:00 horas, de segunda a sexta-feira, na Avenida dos Andradas, n° 3.100, sala A-121, Bairro Santa Efigênia, nesta Capital.

1.4 - A manifestação deverá indicar, de forma expressa e clara, o item específico do Termo de Referência, conforme o caso, sobre o qual pretenda apresentar crítica ou sugestão.

2 - DA FORMULAÇÃO DAS CRÍTICAS E SUGESTÕES

2.1 - As críticas e sugestões deverão ser apresentadas no idioma português, de forma concisa e objetiva, com observância do disposto no subitem 1.4 e com identificação pessoal de quem se manifesta e, se for o caso, da empresa que representa.

2.2 - As manifestações feitas pelos interessados serão disponibilizadas pela CMBH no endereço eletrônico "**http://www.cmbh.mg.gov.br/transparencia/licitacoes**".

3 - DO EQUACIONAMENTO DE DÚVIDAS

3.1 - A CPL apenas atenderá a questionamentos e dúvidas pertinentes a este edital e à realização em si da Consulta Pública.

3.2 - Dúvidas sobre o Termo de Referência poderão ser respondidas pela área demandante, por escrito, no curso da Consulta Pública ou posteriormente.

3.2.1 - Em qualquer caso, as dúvidas e as respostas serão disponibilizadas no site da CMBH.

3.2.1.1 - No caso de resposta posterior à Consulta Pública, será aberto o prazo de 5 (cinco) dias úteis para eventual contestação técnica por parte do interessado, a ser encaminhada por escrito, via e-mail ou por via postal.

4 - DO RESULTADO DA CONSULTA PÚBLICA

4.1 - A Consulta Publica terá por resultado o levantamento de subsídios que colaborem com a área demandante e com a CPL para eventual licitação. Em virtude disso, as críticas e sugestões apresentadas serão encaminhadas à Coordenadoria de Informática - COOINF - e serão objeto de análise técnica e administrativa posterior.

4.1.1 – A análise e decisão final da COOINF constará de documento formal que avalie cada crítica ou sugestão, sob a perspectiva do atendimento às necessidades institucionais, devendo esse documento ser divulgado no site da Câmara.

4.2 - Promovida ou não eventual licitação do objeto sob consulta, e visando ampla transparência do processo respectivo, será disponibilizado, no *link* a ele referente, atalho para o *link* referente à Consulta Pública, viabilizando a qualquer interessado conhecimento amplo do que foi proposto, mesmo que eventualmente não acatado.

5 - DAS DISPOSIÇÕES FINAIS

5.1 - Cópia deste edital encontra-se disponível no endereço eletrônico **http://www.cmbh.mg.gov.br/transparencia/licitacoes**", podendo, ainda, ser obtida na Seção de Apoio a Licitações, no horário de 9:00 às 18:00 horas, de segunda a sexta-feira.

5.1.1 - Encontra-se disponível no endereço eletrônico **http://www.cmbh.mg.gov.br/transparencia/licitacoes**" referente a esta Consulta Pública, um *link* para o Pregão Eletrônico nº 36/2016, que restou fracassado, para permitir a avaliação evolutiva e comparativa com o atual Termo de Referência, podendo, ainda, ser obtida cópia na Seção de Apoio a Licitações, no horário de 9:00 às 18:00 horas, de segunda a sexta-feira.

5.2 - As comunicações referentes a este edital serão realizadas apenas por meio de publicação no Diário Oficial do Município de Belo Horizonte e no endereço eletrônico "**http://www.cmbh.mg.gov.br/transparencia/licitacoes**", à exceção das comunicações relativas a pedidos de esclarecimentos específicos sobre a realização da Consulta, as quais serão feitas apenas por divulgação no *site* supracitado, ficando acessíveis a todos os interessados.

Belo Horizonte, 23 de outubro de 2017.

MÁRCIA VENTURA MACHADO
Presidente da Comissão Permanente de Licitação

ANEXO

- TERMO DE REFERÊNCIA para apreciação –

Integram este Termo de Referência, como parte indissociável, os seguintes documentos:

1. O próprio Termo de Referência com as especificações do objeto;
2. Modelo da Proposta Comercial;
3. A solicitação de aquisição com os detalhamentos para a contratação e os requisitos de julgamento e habilitação para a licitação;
4. Ofícios CPL 13/2017 e COOINF 12/17, com esclarecimentos adicionais.

CÂMARA MUNICIPAL DE BELO HORIZONTE

– TERMO DE REFERÊNCIA – COOINF 001/17 –

1. OBJETO

Registro de preços para contratação de empresa para o fornecimento de **solução de proteção de redes com característica de "Next Generation Firewall – NGFW" para segurança de informação perimetral,** que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN, IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", filtro de URL, bem como controle de transmissão de dados e acesso à internet, compondo uma plataforma de segurança integrada e com a capacidade necessária para atender as demandas de segurança da CMBH, incluindo equipamentos redundantes, licenças, instalação, configuração, treinamento, garantia e suporte técnico pelo prazo de 36 (trinta e seis) meses, de acordo com as especificações do edital.

2. JUSTIFICATIVA

A utilização das tecnologias da informação e comunicação pelas pessoas e organizações vem crescendo significativamente, de forma a suportar processos de negócio e organizacionais, comunicações e decisões mais ágeis.

A crescente disseminação de ataques às redes de computadores, em especial às redes do Governo, requer tratamento adequado, visando proteger o ambiente computacional da CMBH. Este contexto reforça a necessidade de proteção da informação contra acessos sem autorização, alterações indevidas ou indisponibilidade.

As ameaças, que podem ser internas ou externas, vêm aumentando em quantidade e complexidade, demandando a utilização de soluções avançadas com múltiplas camadas de proteção, de forma a reduzir o risco, minimizando a probabilidade e os impactos de um eventual ataque cibernético.

O sistema utilizado para proteção da rede de dados da CMBH, que não mais atende de forma satisfatória o cenário atual, precisa ser substituído por um sistema mais completo, moderno e que se mantenha ativo em alta disponibilidade.

Para responder ao cenário digital atual, explanado mais adiante, propomos a aquisição de um novo sistema de firewall com recursos de Next Generation

Firewall. Dentre as melhorias que poderão ser obtidas com esta solução, podemos destacar:
• Controle granular das aplicações web permitidas e bloqueadas, priorização de tráfego por tipo de aplicação e comutação automática entre links de *Internet*.
• Isto possibilitará maior preparação para enfrentar os desafios de hoje ligados à segurança da informação.
• As soluções de Next Generation Firewall integram diferentes tipos de proteção, tais como antivírus de perímetro, IPS (Sistema de Prevenção de Intrusão), firewall de camada de aplicação, filtro de navegação na *Internet*, entre outros, em um único equipamento, reduzindo o custo de manutenção e administração. Estas vêm sendo amplamente utilizadas por órgãos que precisam estar conectados de forma segura.

A contratação referida neste documento se justifica, ainda, pelas seguintes razões:

2.1. A CMBH possui diversos links de *Internet*, que agregados totalizam 700 Mbps, oferecendo acesso à *Internet* de qualidade para os usuários e visitantes da CMBH.

2.2. Prover acesso à *Internet* de forma segura.

2.3. Atender à crescente demanda por acesso aos recursos da *Internet* na CMBH, para o melhor desenvolvimento dos trabalhos da instituição.

2.4. Adequar o desempenho de acesso à *Internet* dos usuários que atualmente não são atendidos pelos recursos atuais de acordo com a qualidade esperada.

2.5. Suportar a estratégia de crescimento da CMBH nos processos internos e nos processos externos para atendimento ao cidadão.

2.6. Suportar o aumento constante microcomputadores na rede da CMBH, com o consequente aumento do número de usuários acessando a *Internet*.

2.7. Atender às necessidades provenientes do aumento cada vez maior de dispositivos móveis, através da rede wireless, o que exige uma disponibilização maior da *Internet*, considerando os aspectos de desempenho, controle, segurança e qualidade.

2.8. Suportar a crescente utilização de sistemas aplicativos da CMBH que exigem acesso à *Internet*, como: site da CMBH, Portal da Transparência, SIL-*Internet*, Webmail, Moodle, etc.

2.9. A CMBH tem com objetivo aperfeiçoar requisitos de desempenho e segurança de redes.

2.10. A atual solução adotada está próxima de seu limite de carga, além de não atender mais tecnicamente às necessidades de controle e segurança da CMBH.

2.11. A solução atualmente instalada não está coberta por contrato, podendo gerar, caso outra solução não seja adotada, graves problemas de segurança para o ambiente computacional da CMBH

3. Descrição do GRUPO ÚNICO DE ITENS:

ITEM	Descrição	UN.	QTD
1	Solução de Segurança de alta disponibilidade licenciado para 36 meses baseada em Appliance com recursos de Next Generation Firewall (NGFW).	UN.	2
2	Implementação da solução completa no formato hands-on com suporte remoto (8 x 5) em português.	UN.	1
3	Treinamento para operação e administração da solução ofertada para uma equipe de 4 (quatro) pessoas, com carga horária de no mínimo 20 (vinte) horas-aula, a ser ministrado após a implementação da solução de segurança.	UN.	1
4	Contrato de manutenção, atualização e suporte 24 x 7, pelo período de 36 meses e garantia de troca do equipamento no próximo dia útil, a contar da efetiva instalação do Appliance.	UN	36

4. ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÂO de SEGURANÇA NGFW

A solução ofertada deve ser baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux. Os equipamentos da solução devem possuir como características:

4.1. Requisitos Gerais:

4.1.1. Prover sistema de segurança de informação perimetral que inclui Firewall, administração de banda de serviço de *Internet* (QoS e Traffic Shaping), suporte para conexões VPN, IPSec e SSL, proteção contra ameaças de vírus e malware, bem como controle de transmissão de dados e acesso a *Internet*, com desempenho suficiente para suportar a ativação e configuração simultânea de todas as funcionalidades e

recursos a serem providos para atender às exigências constantes destas especificações técnicas.

4.1.2. Prover módulos de proteção contra ameaças de rede, bloqueio de vírus, spyware, controle de transferência de arquivos, controle da navegação de *Internet* (filtros de conteúdo) e bloqueio de arquivos por tipo.

4.1.3. Fornecer, no mínimo, 2 (dois) equipamentos idênticos para garantir alta disponibilidade (HA – High Availability) da solução proposta.

4.1.4. As funcionalidades de proteção de rede que compõem a plataforma de segurança podem funcionar em múltiplos appliances, desde que obedeçam a todos os requisitos desta especificação.

4.1.5. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

4.1.6. O hardware e software que executem as funcionalidades de proteção de rede, bem como o console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

4.1.7. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação, se necessário, e cabos de alimentação.

4.1.8. O software deverá ser fornecido em sua versão mais atualizada.

4.1.9. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

4.1.9.1. Suporte a 4094 VLAN Tags 802.1q;

4.1.9.2. Agregação de links 802.3ad e LACP;

4.1.9.3. Policy based routing ou policy based forwarding;

4.1.9.4. Roteamento multicast (PIM-SM);

4.1.9.5. DHCP Relay;

4.1.9.6. DHCP Server;

4.1.9.7. Jumbo Frames;

4.1.9.8. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3.

4.1.10. Suportar sub-interfaces ethernet lógicas.

4.1.11. Deve suportar os seguintes tipos de NAT:

4.1.11.1. Nat dinâmico (Many-to-1);

4.1.11.2. Nat dinâmico (Many-to-Many);

4.1.11.3. Nat estático (1-to-1);

4.1.11.4. NAT estático (Many-to-Many);

4.1.11.5. Nat estático bidirecional 1-to-1;

4.1.11.6. Tradução de porta (PAT);

4.1.11.7. NAT de Origem;

4.1.11.8. NAT de Destino;

4.1.11.9. Suportar NAT de Origem e NAT de Destino simultaneamente;

4.1.11.10. Enviar log para sistemas de monitoração externos, simultaneamente;

4.1.11.11. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

4.1.11.12. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

4.1.11.13. Proteção contra anti-spoofing;

4.1.11.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

4.1.11.15. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

4.1.11.16. Suportar a OSPF graceful restart;

4.1.11.17. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação;

4.1.11.18. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);

4.1.11.18.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

4.1.11.18.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

4.1.11.18.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

4.1.11.18.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

4.1.12. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

4.1.12.1. Em modo transparente;

4.1.12.2. Em layer 3.

4.1.13. A configuração em alta disponibilidade deve sincronizar:

4.1.13.1. Sessões;

4.1.13.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

4.1.13.3. Certificados de-criptografados;

4.1.13.4. Associações de Segurança das VPNs;

4.1.13.5. Tabelas FIB;

4.1.13.6. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

4.1.14. As funcionalidades de controle de aplicações, VPN, IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

4.2. Controles por Politicas de Firewall:

4.2.1. Deverá suportar controles por zona de segurança.

4.2.2. Controles de políticas por porta e protocolo.

4.2.3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

4.2.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

4.2.5. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

4.2.6. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

4.2.7. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound).

4.2.8. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2.

4.2.9. Controle de inspeção e de-criptografia de SSH por política.

4.2.10. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança.

4.2.11. A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise, (Forense de rede, DLP, Análise de Ameaças, entre outras).

4.2.11.1. É permitido uso de appliance externo específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise.

4.2.12. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg.

4.2.13. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo).

4.2.14. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.

4.2.15. Suporte a objetos e regras IPV6.

4.2.16. Suporte a objetos e regras multicast.

4.2.17. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4.3. Controle de Aplicações:

Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

4.3.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos.

4.3.2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

4.3.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc.

4.3.4. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de

assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389.

4.3.5. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária.

4.3.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.

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

4.3.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas.

4.3.9. Identificar o uso de táticas evasivas via comunicações criptografadas.

4.3.10. Atualizar a base de assinaturas de aplicações automaticamente.

4.3.11. Reconhecer aplicações em IPv6.

4.3.12. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP.

4.3.13. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao LDAP, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

4.3.14. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

4.3.15. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística.

4.3.16. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

4.3.17. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão.

CÂMARA MUNICIPAL DE BELO HORIZONTE

4.3.18. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:

4.3.18.1. HTTP, FTP, SMTP, SMB, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC e RTSP

4.3.19. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

4.3.20. Deve alertar o usuário quando uma aplicação for bloqueada;

4.3.21. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

4.3.22. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/politicas para os mesmos.

4.3.23. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos.

4.3.24. Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o Gtalk chat e bloquear a transferência de arquivos.

4.3.25. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;

4.3.26. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

4.3.26.1. Tecnologia utilizada na aplicações (Client-Server, Browse Based, Network Protocol, etc).

4.3.26.2. Nível de risco da aplicação.

4.3.26.3. Categoria de aplicações.

4.3.26.4. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

4.4. Prevenção de ameaças.

4.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall, ou entregues através de composição com outro equipamento ou fabricante.

4.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

4.4.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

4.4.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementados em alta disponibilidade ativo/ativo e ativo/passivo.

4.4.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.

4.4.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura.

4.4.7. Deve suportar granularidade nas politicas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

4.4.8. Deve permitir o bloqueio de vulnerabilidades.

4.4.9. Deve permitir o bloqueio de exploits conhecidos.

4.4.10. Deve incluir proteção contra ataques de negação de serviços.

4.4.11. Deverá possuir os seguintes mecanismos de inspeção de IPS:

4.4.11.1. Análise de padrões de estado de conexões.

4.4.11.2. Análise de decodificação de protocolo.

4.4.11.3. Análise para detecção de anomalias de protocolo.

4.4.11.4. Análise heurística.

4.4.11.5. IP Defragmentation.

4.4.11.6. Remontagem de pacotes de TCP.

4.4.11.7. Bloqueio de pacotes malformados.

4.4.12. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc.

4.4.13. Detectar e bloquear a origem de portscans.

4.4.14. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões.

4.4.15. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados.

4.4.16. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.

4.4.17. Possuir assinaturas para bloqueio de ataques de buffer overflow.

4.4.18. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.

4.4.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.

4.4.19.1. É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede.

4.4.20. Suportar bloqueio de arquivos por tipo.

4.4.21. Identificar e bloquear comunicação com botnets.

4.4.22. Deve suportar varias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos).

4.4.23. Deve suportar referência cruzada com CVE.

4.4.24. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

4.4.24.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

4.4.25. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware.

4.4.26. Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes.

4.4.27. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos.

4.4.28. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.

4.4.29. Os eventos devem identificar o país de onde partiu a ameaça.

4.4.30. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

4.4.31. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.

4.4.32. Rastreamento de vírus em pdf.

4.4.33. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.).

COORDENADORIA DE INFORMÁTICA

4.4.34. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

4.5. Análise de Malwares Modernos

4.5.1. Possui a capacidade de análise de ameaças não conhecidas.

4.5.2. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante.

4.5.3. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado.

4.5.4. Selecionar através de política de Firewall quais tipos de arquivos sofrerão esta análise.

4.5.5. Suportar a análise de comportamentos maliciosos para ameaças não conhecidas.

4.5.6. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP e Windows 7 32 bits e Windows 7 64 bits.

4.5.7. Deve suportar a monitoração de arquivos trafegados na internet (HTTP, FTP, HTTP, SMTP) como também arquivos trafegados internamente nos servidores de arquivos usando SMB.

4.5.8. A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits.

4.5.9. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque.

4.5.10. O sistema de análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo

Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede).

4.5.11. O sistema automático de analise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware.

4.5.12. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência.

4.5.13. Deve permitir o download dos malwares identificados a partir da própria interface de gerência.

4.5.14. Deve permitir visualizar o resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados.

4.5.15. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência.

4.5.16. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado.

4.6. Filtro de URL

4.6.1. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

4.6.1.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.6.1.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.

4.6.1.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, E-directory e base de dados local.

4.6.1.4. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.

4.6.1.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

4.6.1.6. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função.

4.6.1.7. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs.

4.6.1.8. Possui pelo menos 60 categorias de URLs.

4.6.1.9. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório.

4.6.1.10. Suporta a criação categorias de URLs customizadas.

4.6.1.11. Suporta a exclusão de URLs do bloqueio, por categoria.

4.6.1.12. Permite a customização de página de bloqueio.

4.6.1.13. Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site).

4.6.1.14. Suporta a inclusão nos logs do produto de informações das atividades dos usuários.

4.6.1.15. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For.

4.7. Prevenção de Evasão de Informações Sensíveis (Filtro de Dados)

4.7.1. Permite a criação de filtros para arquivos e dados pré-definidos.

4.7.2. Os arquivos devem ser identificados por extensão e assinaturas.

4.7.3. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc).

4.7.4. Suportar identificação de arquivos compactados e a aplicação de politicas sobre o conteúdo desses tipos de arquivos.

4.7.5. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

4.7.6. Permitir listar o número de aplicações suportadas para controle de dados.

4.7.7. Permitir listar o número de tipos de arquivos suportados para controle de dados.

4.8. Qualidade de Serviço (QoS)

4.8.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

4.8.2. Suportar a criação de políticas de QoS por:

4.8.2.1. Endereço de origem.

4.8.2.2. Endereço de destino.

4.8.2.3. Por usuário e grupo do LDAP.

4.8.2.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus.

4.8.2.5. Por porta.

4.8.3. O QoS deve possibilitar a definição de classes por:

4.8.3.1. Banda Garantida.

4.8.3.2. Banda Máxima.

4.8.3.3. Fila de Prioridade.

4.8.4. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

4.8.5. Suportar marcação de pacotes Diffserv, inclusive por aplicação.

4.8.6. Disponibilizar estatísticas RealTime para classes de QoS.

4.8.7. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

4.9. Geo Localização (GeoLocation)

4.9.1. Suportar a criação de políticas por Geo Localização, permitindo o tráfego de determinado País/Países sejam bloqueados.

4.9.2. Permitir a visualização dos países de origem e destino nos logs dos acessos.

4.9.3. Permitir a utilização de informações geográficas pela interface gráfica e criar políticas utilizando as mesmas.

4.10. Identificação de Usuários.

4.10.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via Ldap, E-directory e base de dados local.

4.10.2. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

4.10.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

4.10.4. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários.

4.10.5. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários.

4.10.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

4.10.7. Suporte a autenticação Kerberos.

4.10.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

4.10.9. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

4.11. Funcionalidades de Rede

4.11.1. Suportar funcionamento em Tap Mode (Via porta espelhada, Tap ou Span port).

4.11.2. Suportar funcionamento em modo transparente (Bridge ou similar).

4.11.3. Suportar funcionamento em Layer 2.

4.11.4. Suportar funcionamento em Layer 3.

4.11.5. Suportar a implementação simultânea de todos os modos descritos acima (Tap, Transparente, Layer2 e Layer3) no mesmo equipamento.

4.11.6. Suportar Vlan Tagging (802.1Q) em todas os cenários de implementação acima (Transparente, Layer2 e Layer3) .

4.11.7. Suportar o controle de aplicações em IPV6 em todos os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3).

4.11.8. Suportar sub-interfaces Ethernet lógicas.

4.12. VPN

4.12.1. Suportar VPN Site-to-Site e Cliente-To-Site.

4.12.2. Suportar IPSec VPN.

4.12.3. Suportar SSL VPN.

4.12.4. A VPN IPSEc deve suportar:

4.12.4.1. 3DES.

4.12.4.2. Autenticação MD5 e SHA-1.

4.12.4.3. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14.

4.12.4.4. Algoritmo Internet Key Exchange (IKE).

4.12.4.5. AES 128, 192 e 256 (Advanced Encryption Standard).

4.12.4.6. Autenticação via certificado IKE PKI.

4.12.5. Deve possuir interoperabilidade com os seguintes fabricantes:

4.12.5.1. Cisco.

4.12.5.2. Checkpoint.

4.12.5.3. Juniper.

4.12.5.4. Palo Alto Networks.

4.12.5.5. Fortinet.

4.12.5.6. Sonic Wall.

4.12.6. A VPN SSL deve suportar:

4.12.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.

4.12.6.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.

4.12.6.3. Atribuição de endereço IP nos clientes remotos de VPN.

4.12.6.4. Atribuição de DNS nos clientes remotos de VPN.

4.12.6.5. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário.

4.12.6.6. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

4.12.6.7. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE.

4.12.6.8. Suportar autenticação via LDAP, Secure id, certificado e base de usuários local.

4.12.6.9. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon.

4.12.6.10. Suporta leitura e verificação de CRL (certificate revocation list).

4.12.6.11. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

4.12.6.12. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN.

4.12.6.13. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário.

4.12.6.14. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

4.12.6.14.1. Antes do usuário autenticar na estação.

4.12.6.14.2. Após autenticação do usuário na estação.

4.12.6.14.3. Sob demanda do usuário.

4.12.6.15. Deverá manter uma conexão segura com o portal durante a sessão.

4.12.6.16. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8 e Mac OSx.

4.13. Console de Gerencia e monitoração

4.13.1. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento.

4.13.2. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.

4.13.3. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux.

4.13.4. O gerenciamento deve permitir/possuir:

4.13.4.1. Criação e administração de políticas de firewall e controle de aplicação.

4.13.4.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware.

4.13.4.3. Criação e administração de políticas de Filtro de URL.

4.13.4.4. Monitoração de logs.

4.13.4.5. Ferramentas de investigação de logs.

4.13.4.6. Debugging.

4.13.4.7. Captura de pacotes.

4.13.5. Acesso concorrente de administradores.

4.13.6. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

4.13.7. Deve permitir usar palavras chaves e cores para facilitar identificação de regras.

4.13.8. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas.

4.13.9. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores.

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

4.13.11. Autenticação integrada ao LDAP e servidor Radius.

4.13.12. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados.

4.13.13. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS.

4.13.14. Criação de regras que fiquem ativas em horário definido.

4.13.15. Criação de regras com data de expiração.

4.13.16. Backup das configurações e rollback de configuração para a última configuração salva.

4.13.17. Suportar Rollback de Sistema Operacional para a ultima versão local.

4.13.18. Validação de regras antes da aplicação.

4.13.18.1. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.

4.13.19. Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).

4.13.19.1. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).

4.13.20. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

4.13.21. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors).

4.13.22. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

4.13.23. 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.

4.13.24. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.

4.13.25. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes.

4.13.26. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança.

4.13.27. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc.

4.13.28. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução.

4.13.29. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime.

4.13.30. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso.

4.13.31. Deve ser possível exportar os logs em CSV.

4.13.32. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

4.13.33. Rotação do log.

4.13.34. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

4.13.34.1. Situação do dispositivo e do cluster.

4.13.34.2. Principais aplicações.

4.13.34.3. Principais aplicações por risco.

4.13.34.4. Administradores autenticados na gerência da plataforma de segurança.

4.13.34.5. Número de sessões simultâneas.

4.13.34.6. Status das interfaces.

4.13.34.7. Uso de CPU.

4.13.35. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

4.13.35.1. Resumo gráfico de aplicações utilizadas.

4.13.35.2. Principais aplicações por utilização de largura de banda de entrada e saída.

4.13.35.3. Principais aplicações por taxa de transferência de bytes.

4.13.35.4. Principais hosts por número de ameaças identificadas.

4.13.35.5. Atividades de um usuário específico e grupo de usuários do LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego.

4.13.35.6. Deve permitir a criação de relatórios personalizados.

4.13.36. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa.

4.13.37. Gerar alertas automáticos via:

4.13.37.1. Email.

4.13.37.2. SNMP.

4.13.37.3. Syslog.

4.13.38. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

5. REQUISITOS COMPLEMENTARES DOS FIREWALLS

5.1. A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:

5.1.1. Throughput de 2 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir.

5.1.2. Throughput de 1 Gbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

5.1.3. Suporte a, no mínimo, 240.000 conexões simultâneas.

5.1.4. Suporte a, no mínimo, 45.000 novas conexões por segundo.

5.1.5. Fonte 120/240 AC.

5.1.6. Disco Solid State Drive (SSD) de, no mínimo, 100 GB.

5.1.7. 10 (dez) interfaces de rede 10/100/1000 base-TX.

5.1.8. 6 (seis) interfaces de rede 1 Gbps SFP.

5.1.9. 2 (duas) Gbps interfaces dedicadas para alta disponibilidade.

5.1.10. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento.

5.1.11. 1 (uma) interface do tipo console ou similar.

5.1.12. Suporte a, no mínimo, 10 (dez) roteadores virtuais.

5.1.13. Suporte a, no mínimo, 30 (trinta) zonas de segurança.

5.1.14. Estar licenciada para ou suportar sem o uso de licença, 1.000 (mil) clientes de VPN SSL simultâneos.

5.1.15. Estar licenciada para ou suportar sem o uso de licença, 1.000 túneis de VPN IPSEC simultâneos.

5.2. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento.

5.3. Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas.

5.4. As consoles de gerência e de monitoração podem residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função.

5.5. Na data da proposta nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

6. ATIVIDADES E REQUISITOS DA EXECUÇÃO DOS SERVIÇOS

6.1. DA DESCRIÇÃO DOS SERVIÇOS

6.1.1. Instalação básica dos equipamentos que consiste no serviço de atualização de firmware dos appliances para a última versão estável, definição e configuração do endereçamento IP, configuração do modo de funcionamento, configuração de usuário e senha de administração, conexão dos equipamentos na rede do cliente, teste de acesso para administração.

6.1.2. Configuração e implementação que consiste no serviço de consultoria, onde um especialista em Segurança da Informação da contratada, discutirá com a equipe técnica da CMBH todas as funcionalidades dos appliances adquiridos, e como elas serão mais bem implementadas dentro de sua infraestrutura, com apresentação de eventuais sugestões de melhorias em sua rede de perímetro, e utilização de links Internet. Além disto, o serviço engloba a configuração de todas as Regras.

6.1.3. A implementação deverá ser no modelo hands-on com acompanhamento da equipe técnica.

6.2. DA EXECUÇÃO DOS SERVIÇOS

6.2.1. PREMISSAS PARA O INICIO DA EXECUÇÃO:

6.2.1.1. A Equipe Técnica da CMBH deve contar com um Administrador de Rede e um Desenvolvedor das Aplicações – este último para dúvidas eventuais.

6.2.1.2. Possuir Diagrama de Rede, dos Servidores, e dos Sites (aplicações) a serem protegidas pelo Firewall; Local de trabalho com acesso à Internet, e ao equipamento para 2 (duas) pessoas da contratada; Mesa ou bancada para instalação preliminar do equipamento (com acesso à Internet); 1 (um) IP externo válido para testes de validação.

6.2.1.3. A CMBH deverá ter em mãos, a priori do inicio dos serviços contratados, e fornecer de imediato aos especialistas da contratada todas as regras e configurações de rede, roteamento, Firewall, IPS, VPNs, endereçamento IP, nomes DNS, Servidores de Domínio, Servidores DNS, Proxies e demais informações pertinentes ao projeto da infraestrutura existente atualmente na CMBH.

6.2.1.4. A CMBH deverá disponibilizar um analista de rede, para acompanhar a implementação dos Appliances, este técnico deverá ter acesso aos firewalls, roteadores, e servidor de domínio, atualmente em funcionamento, e conhecimento da rede wireless atualmente em produção.

6.2.1.5. A CMBH deve executar um backup e um checkpoint (ou snapshot) de todos os servidores, e elementos de rede que serão afetados por esta implementação, antes do inicio dos serviços, e caberá à CMBH a recuperação dos dados e configurações que eventualmente sejam necessárias.

6.2.1.6. Cabe a CMBH disponibilizar pontos e cabos de rede, pontos elétricos estabilizados, espaço em Rack, e ar condicionado adequados para a instalação dos equipamentos descritos na proposta.

6.2.2. ETAPAS DA EXECUÇÃO:

6.2.2.1. - 1ª Etapa - Levantamento

Etapa de levantamento de informações da situação atual e da situação desejada e discussão com a equipe técnica da CMBH das necessidades e melhorias a implementar.

6.2.2.2. - 2ª Etapa - Fornecimento dos equipamentos (Appliances) de Firewall

Os equipamentos deverão ser entregues em até 60 (sessenta) dias corridos após assinatura do contrato.

6.2.2.3. - 3ª Etapa – Instalação Básica:

Serviço de atualização de firmware dos Appliances para a última versão estável, definição e configuração do endereçamento IP, configuração do modo de funcionamento, configuração de usuário e senha de administração, conexão dos equipamentos na rede da CMBH, teste de acesso para administração.

6.2.2.4. - 4ª Etapa – Da Configuração e Implementação:

Serviço de consultoria, onde um especialista em Segurança da Informação da CONTRATADA, discutirá com a equipe técnica da CMBH todas as funcionalidades dos appliances adquiridos, e como elas serão melhor implementadas dentro de sua infraestrutura, com apresentação de eventuais sugestões de melhorias em sua rede de perímetro, e utilização de links Internet. Além disto, o serviço engloba a configuração de todas as Regras de Firewalls, VPNs, IPS, URL Filter, Integração da Autenticação de usuários com LDAP, Antivírus, levantadas e definidas pela CMBH, e acompanhamento pós-implementação.

6.2.2.5. TREINAMENTO

6.2.2.5.1. A CONTRATADA deverá fornecer treinamento específico sobre a instalação, configuração e operação da solução para até 04 (quatro) pessoas, na sede do CMBH, situada na Avenida dos Andradas, 3100, Bairro Santa Efigênia, em Belo Horizonte, Minas Gerais.

6.2.2.5.2. O treinamento deve abranger todas as funcionalidades da solução.

6.2.2.5.3. O treinamento deverá ter carga horária mínima de 20 horas, distribuídas em no máximo 4 horas diárias, e deverá ser realizado durante o período da tarde, dentro do horário comercial.

6.2.2.5.4. O treinamento deverá ser ofertado em Português e o material didático deverá ser em Português ou Inglês.

6.2.2.5.5. O treinamento deverá ser ministrado sem custo adicional ao preço formulado na proposta, devendo incluir instrutor, material didático e quaisquer outros necessários.

6.2.2.5.6. A CONTRATADA deve arcar com todas as despesas eventualmente realizadas com transporte, hospedagem, passagens aéreas/ terrestres, diárias, despesas com locomoção, alimentação, fotocópia e qualquer material ou contratação que se façam necessários para a execução das atividades.

6.2.3. Do Acompanhamento:

6.2.3.1. A CONTRATADA fica obrigada a acompanhar o correto funcionamento dos appliances na rede da CMBH e execução de eventuais ajustes que se mostrem necessários, durante o período de implementação.

6.2.4. SERVIÇOS DE GARANTIA, ASSISTÊNCIA TÉCNICA E SUPORTE TÉCNICO

6.2.4.1. Os serviços de garantia, assistência técnica e suporte técnico deverão ser prestados, em todos os produtos fornecidos, pelo período de 36 (trinta e seis) meses, a contar da data do recebimento definitivo dos produtos, compreendendo, entre outros:

6.2.4.1.1. Manutenção corretiva de hardware dos produtos fornecidos, incluindo a reparação de eventuais falhas, mediante a substituição de peças e componentes por outros de mesma especificação, novos, de primeiro uso e originais, de acordo com os manuais e normas técnicas específicas para os mesmos;

6.2.4.1.2. Atualizações corretivas e evolutivas de software e firmware, incluindo pequenas atualizações de release, reparos de pequenos defeitos (bug fixing, patches);

6.2.4.1.3. Ajustes e configurações conforme manuais e normas técnicas do fabricante;

6.2.4.1.4. Demais procedimentos destinados a recolocar os equipamentos em perfeito estado de funcionamento;

6.2.4.1.5. Assistência técnica especializada para investigar, diagnosticar e resolver incidentes e problemas relativos aos produtos fornecidos;

6.2.4.1.6. Fornecimento de informações e esclarecimentos de dúvidas sobre instalação, administração, configuração, otimização ou utilização dos produtos adquiridos.

6.2.4.1.7. A CONTRATADA deverá prestar serviços de assistência técnica e suporte técnico disponíveis por no mínimo 8 (oito) horas por dia, 5 (cinco) dias por semana, nos dias úteis e horário comercial, por técnicos devidamente habilitados e credenciados ou certificados pelo fabricante, com nível de certificação compatível com as atividades a serem executadas, e sem qualquer ônus adicional.

6.2.4.1.8. Deverá ser disponibilizado, durante a garantia, canal de atendimento 24x7x365 para abertura de chamados técnicos, mediante número 0800 ou número local (na cidade onde se encontram instalados os equipamentos). Adicionalmente, poderá ser disponibilizado serviço de abertura de chamado via site ou e-mail.

6.2.4.1.9. Para cada chamado técnico, deverá ser informado um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas.

6.2.4.1.10. Os chamados técnicos serão classificados por criticidade, de acordo com o impacto no ambiente computacional da CMBH, conforme abaixo:

6.2.4.1.11. Prioridade Alta: Sistema indisponível ou com severa degradação de desempenho;

6.2.4.1.12. Prioridade Média: Sistema disponível, com mau funcionamento, que importe baixa degradação de desempenho ou comprometimento em um de seus elementos que importe em risco para a disponibilidade do sistema.

6.2.4.1.13. Prioridade Baixa: Sistema disponível, sem impacto em seu desempenho ou disponibilidade; consultas gerais sobre instalação, administração, configuração, otimização, troubleshooting ou utilização.

6.2.4.1.14. O nível de severidade será informado pela CMBH no momento da abertura do chamado.

6.2.4.1.15. O prazo de atendimento inicial dos chamados técnicos deverá ser de até 4 (quatro) horas, contadas a partir da hora do acionamento do suporte técnico pela CMBH.

6.2.4.1.16. O encerramento do chamado será dado por empregado da CMBH na conclusão dos serviços, após a disponibilização da solução para uso em perfeitas condições de funcionamento no local onde está instalada.

6.2.4.1.17. Caberá aos técnicos do fabricante ou da empresa por ele autorizada identificar os componentes, peças e materiais responsáveis pelo mau funcionamento dos produtos fornecidos.

6.2.4.1.18. Em caso de falhas irrecuperáveis de hardware ou impossibilidade de solução pela assistência técnica, deverá ser providenciado a troca por equipamento idêntico, com cobertura para o próximo dia útil 8 x 5 NBD (NBD – Next Business Day).

6.2.4.1.19. Por questão de segurança, os equipamentos e softwares nunca deverão ser removidos das dependências da CMBH sem a remoção de dados ou regras sigilosas.

6.2.4.1.20. No caso de troca de equipamento com defeito, não haverá qualquer ônus adicional para a CMBH.

6.2.4.1.21. Relativamente à manutenção corretiva de hardware e software:

Os componentes danificados deverão ser substituídos, entregues, instalados e configurados, de modo a deixar o equipamento em perfeitas condições de uso e com todas as funcionalidades operacionais, nas dependências da CMBH, nos prazos de solução estabelecidos acima, sem a cobrança de quaisquer custos adicionais (frete, seguro, etc.);

6.2.4.1.22. Durante todo o período de garantia deverá ser atualizado ou disponibilizado para download, sem ônus adicionais para a CMBH, os softwares necessários ao funcionamento dos produtos fornecidos, fornecendo as novas versões ou releases lançados. Os softwares tratados neste item incluem vacinas de antivírus/antimalware, assinaturas do filtro de conteúdo web, software de gerenciamento, firmwares de BIOS e drivers.

6.2.4.1.23. Qualquer manutenção e/ou intervenção por solicitação do fabricante da solução, mesmo não implicando em inoperância da solução ou alteração de suas características, deverá ser agendada e acordada previamente com a CMBH.

6.2.4.1.24. Nos casos em que os produtos operem em alta disponibilidade deverá ser realizado o reparo ou troca do equipamento que apresente falha ou defeito ainda que o serviço não seja interrompido, sendo contados normalmente os prazos de atendimento.

6.2.5. PRAZOS E TERMO DE ACEITE DEFINITIVO

O recebimento dos produtos e serviços será realizado de acordo com a execução das seguintes etapas:

6.2.5.1. Entrega dos produtos (equipamentos, softwares, sistemas de informação e demais materiais).

6.2.5.2. Execução dos serviços de instalação, configuração e treinamento de toda a solução.

6.2.5.3. Prestação dos serviços de operação assistida.

6.2.5.4. Prestação dos serviços de garantia, assistência técnica e suporte técnico.

6.2.5.5. Os prazos para execução da cada uma das etapas é o seguinte:

6.2.5.6. Os **produtos** deverão ser entregues em um prazo de até 60 (sessenta) dias corridos contados da data de assinatura do contrato.

6.2.5.7. Os **serviços de instalação, configuração e treinamento** deverão ser prestados em um prazo de até 60 (sessenta) dias corridos contados da data de entrega dos produtos.

6.2.5.8. Os serviços de **operação assistida** deverão ser prestados em um prazo de até 05 (cinco) dias úteis contados da data de conclusão dos serviços de instalação e configuração da solução.

6.2.5.9. Os serviços de **garantia, assistência técnica e suporte técnico** deverão ser prestados em um prazo de 36 (trinta e seis) meses contados da data de registro dos produtos, softwares e serviços junto ao fabricante.

6.2.5.10. Caso sejam constatadas irregularidades nos produtos e serviços entregues pela CONTRATADA, a CMBH poderá rejeitá-los no todo

COORDENADORIA DE INFORMÁTICA CMBH

ou em parte, determinando que sejam providenciadas as correções necessárias à adequação do objeto contratado.

6.2.5.11. O Termo de Aceite somente será emitido após o recebimento de cada item do objeto conforme a tabela do modelo de proposta comercial, incluindo a entrega dos produtos, a execução dos serviços de instalação, configuração, operação assistida, treinamento, habilitação da garantia, assistência técnica e suporte técnico, além do atendimento de todos os requisitos e exigências do Termo de Referência e do Edital.

6.2.6. SERVIÇOS DE OPERAÇÃO ASSISTIDA

6.2.6.1. Após a data de conclusão dos serviços de instalação e configuração da solução, a CONTRATADA deverá acompanhar a equipe técnica da CMBH na execução das principais tarefas administrativas do dia-a-dia, atuando em eventuais correções, durante 05 (cinco) dias úteis.

6.2.6.2. O técnico da CONTRATADA que prestará os serviços de Operação Assistida deverá ser certificado pelo fabricante da solução e ficar presente 8h (oito horas) por dia na CMBH, em horário a ser definido pelo CMBH, comprovado através de relatório de atendimento elaborado pelo técnico e aprovado pela CMBH.

6.2.6.3. As despesas de viagem, hospedagem, alimentação e demais para execução do serviço de operação assistida por qualquer pessoal ou técnico da CONTRATADA correrão por conta da própria CONTRATADA.

6.2.6.4. A CONTRATADA deverá manter à disposição da CMBH, durante o período de Operação Assistida, pessoal técnico especializado e qualificado para o acompanhamento e verificação do desempenho operacional e eliminação imediata de eventuais falhas na solução.

6.2.6.5. A CONTRATADA deverá emitir relatório técnico identificando e diagnosticando as falhas que ocorrerem.

6.2.6.6. A CONTRATADA deverá propor e tomar as ações necessárias para a prevenção da repetição das falhas que ocorrerem.

7. DAS OBRIGAÇÕES

7.1. DA CMBH:

7.1.1. Observar para que, durante toda a vigência do contrato, seja mantida a compatibilidade com as obrigações assumidas pela CONTRATADA, referente às condições de qualificação exigidas na licitação;

7.1.2. Deverá permitir o acesso dos técnicos da CONTRATADA em suas instalações, devidamente identificados por crachás;

7.1.3. Estabelecer prioridades de serviço dentro de critérios previamente acordados com a CONTRATADA;

7.1.4. Notificar, por intermédio de ofício ou e-mail, à CONTRATADA sobre ocorrência de eventuais imperfeições no curso de execução dos serviços, fixando prazo para a sua correção;

7.1.5. Aplicar à Contratada as penalidades regulamentares e contratuais;

7.1.6. Deverá acompanhar a execução do objeto do contrato por intermédio da Equipe da SECITI;

7.1.7. Rejeitar, no todo ou em parte, os serviços em desacordo com as obrigações assumidas pela CONTRATADA;

7.1.8. A CMBH se reserva no direito de, a qualquer tempo, solicitar informações sobre a qualificação do pessoal utilizado pela CONTRATADA, bem como notificar a Contratada sobre possíveis irregularidades que prejudiquem a execução dos serviços;

7.1.9. É Responsabilidade da CMBH, nomear Equipe Técnica da SECITI para acompanhar a execução dos serviços;

7.1.10. Dar ciência a CONTRATADA, imediatamente e por escrito, de qualquer anormalidade que verificar na execução dos serviços;

7.2. DA CONTRATADA:

7.2.1. Prestar os serviços em conformidade com as especificações contidas no presente termo de referência;

7.2.2. Executar os serviços em observância aos padrões estabelecidos pela Equipe da SECITI da CMBH;

7.2.3. Observar para que durante toda a vigência do contrato, seja mantida a compatibilidade com as obrigações assumidas, referente a habilitação e qualificação exigidas na licitação;

7.2.4. Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, especialmente aquelas relacionadas ao INSS e FGTS;

7.2.5. Responsabilizar-se pelo fiel cumprimento dos serviços contratados;

7.2.6. Arcar com qualquer prejuízo causado à CMBH ou a terceiros por seus empregados ou prepostos, no cumprimento e execução dos serviços, ora contratados, resultantes em indenização;

7.2.7. Responsabilizar-se, às suas custas, pelo transporte de seu pessoal e dos equipamentos de proteção e segurança de trabalho;

7.2.8. Responsabilizar-se por qualquer acidente de que possam ser vítimas os empregados, no desempenho dos serviços objeto desta licitação;

7.2.9. Alocar equipe técnica para execução dos serviços objeto do Contrato em quantidade suficiente e com nível de conhecimento técnico compatível, de modo a cumprir os prazos estabelecidos e garantir a qualidade dos serviços;

7.2.10. Cumprir todas as orientações da CMBH, através da Equipe da SECITI, prestando todos os esclarecimentos solicitados e reclamações formuladas;

7.2.11. Os empregados da CONTRATADA deverão portar "crachá" de identificação, com o nome do referido funcionário;

7.2.12. Dar ciência à CMBH, imediatamente e por escrito, de qualquer anormalidade que verificar na execução dos serviços;

7.2.13. Responder por quaisquer compromissos com terceiros, ainda que vinculado à execução do presente contrato;

7.2.14. Nomear técnico responsável pela supervisão e execução do contrato, com as seguintes atribuições:

7.2.14.1. Atuar em todas as fases dos trabalhos, avaliando o seu desenvolvimento e promovendo ações que assegurem que sejam atingidos, com qualidade, os resultados contratados;

7.2.14.2. Prestar apoio técnico aos componentes da equipe;

7.2.14.3. Prestar os esclarecimentos que forem solicitados pela CMBH, obrigando-se a atender prontamente;

7.2.15. Permitir a CMBH, o direito de fiscalizar a fiel observância das disposições do contrato;

7.2.16. Absorver para si todos os encargos trabalhistas, previdenciários e fiscais oriundos dos empregados que executarão os serviços objeto do termo de referência, eximindo a CMBH de quaisquer vínculos trabalhistas e/ou sociais;

7.2.17. Guardar sigilo absoluto sobre os detalhes e dados do objeto da prestação de serviços, respondendo legalmente pela inobservância deste item, inclusive após o término do contrato. Não permitir que estes dados sejam copiados em qualquer dispositivo de armazenamentos bem como enviados por e-mail ou qualquer ação que caracterize a quebra deste sigilo;

7.2.18. A CONTRATADA deverá apresentar relatório das atividades desenvolvidas mensalmente, devidamente subscrito pela CMBH;

7.2.19. A CONTRATADA compromete-se a corrigir ou refazer, a critério da CMBH, sem ônus, quaisquer serviços que não apresentem os níveis de qualidade especificados;

8. DA INFRAESTRUTURA

8.1. A CONTRATADA deverá fornecer, às suas custas, toda estrutura necessária para execução dos serviços. Todos os softwares necessários ao funcionamento e operação para a execução dos serviços do objeto licitado devidamente legalizados e compatíveis com ambiente tecnológico da CMBH, a serem instalados utilizando a infraestrutura física da CMBH.

8.2. A CMBH disponibilizará a infraestrutura básica que constitui em espaço físico nas suas dependências, instalações sanitárias e elétricas, energia elétrica, climatização, linha telefônica e acesso à rede interna e internet / extranet;

8.3. A CONTRATADA deverá fornecer todas as licenças de uso dos softwares utilizados nos equipamentos fornecidos para o ambiente da CMBH, com as respectivas certificações, além de manter serviço de suporte técnico remoto (8x5) necessário para a execução de seus serviços. Fornecer pessoal qualificado para a configuração e adequação da solução de segurança com todas as funcionalidades de NGFW;

8.4. A CONTRATADA deverá responsabilizar-se por todas as atividades necessárias para implementação do objeto contratado.

9. DA SEGURANÇA

9.1. Todas as informações necessárias à execução dos serviços são consideradas sigilosas, não podendo, a CONTRATADA, divulgá-las a terceiros e nem divulgá-las para outra finalidade;

9.2. A CONTRATADA deverá orientar seus profissionais para que respeitem as normas de segurança e disciplina da CMBH nos locais onde forem desenvolver suas atividades;

9.3. A CONTRATADA será responsabilizada por documentos rasurados e rasgados, ou mesmo por perdas, reproduções ou adulterações que porventura venham a ocorrer nos documentos e arquivos magnéticos durante o período em que estes estiverem sob sua guarda, cabendo, neste sentido, além de multa pecuniária, as penalidades previstas em lei;

9.4. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados, informações, documentos e especificações técnicas da CMBH que a ela venham a ser confiados ou que venha a ter acesso em razão deste contrato;

9.5. A CONTRATADA deverá zelar pela veracidade de todas as informações que irão compor a documentação dos serviços realizados, não podendo, sob qualquer pretexto, divulgá-los, reproduzi-los ou deles dar conhecimento a quaisquer terceiros estranhos a este contrato;

10. PRAZOS DE EXECUÇÃO

DEVERÃO SER RIGOROSAMENTE OBEDECIDOS OS PRAZOS ABAIXO:	
Cronograma Geral	
PRAZO	EXECUÇÃO
Em até 10 (dez) dias corridos após assinatura do contrato. Responsável: CONTRATADA	Apresentar o plano de instalação, que deverá conter, no mínimo: • Cronograma descrevendo as atividades, sendo certo que será firmado, entre a Contratada e a CMBH, termo contendo o início e término dos serviços; • Lista de recursos de software e hardware que serão utilizados nos equipamentos para auxílio da implantação, restando aqueles que serão fornecidos pela contratada, já incluídos no preço da licitação; • Requisitos de infraestrutura a serem providenciados previamente pela CMBH; • Plano de trabalho para a instalação da nova solução, sem interrupção do funcionamento da solução atualmente instalada; • Procedimentos a serem seguidos para a realização dos testes de funcionamento da solução; • Plano de migração da solução atual para a nova, dentro do prazo previsto para a instalação; • Informações adicionais, caso venham a ser requeridas pela CMBH
Em até 2 (dois) dias corridos após a apresentação das Etapas de Execução pela CONTRATADA Responsável: CMBH	O Plano de instalação apresentado pela CONTRATADA deve ser aprovado formalmente pela Equipe Técnica da SECITI.
Até 60 (sessenta) dias corridos da assinatura do contrato Responsável: CONTRATADA	Deve entregar todos os equipamentos Appliances para instalação no ambiente da CMBH.

Até 30 (trinta) dias corridos da entrega dos equipamentos na CMBH. Responsável: CONTRATADA	A CONTRATADA deve instalar e configurar todos os equipamentos Appliances no ambiente da CMBH, assim como realizar o treinamento Hands-on para os seus administradores, de 8h as 18h de segunda a sexta feira.

Resoluções de problemas	
PRAZO	EXECUÇÃO
Até 48 horas úteis	Todas as inconsistências identificadas pela equipe técnica da SECITI serão devidamente registradas e apresentadas à Contratada, para correção, em relação à implementação e configuração dos equipamentos, durante o período de garantia.
Até 02 (dois) dias úteis	Os equipamentos que apresentarem problemas serão devolvidos à CONTRATADA, retirados por conta da contratada, para ser substituído por outro com as mesmas especificações técnicas. Essa troca não poderá ser feita sem a comunicação à área de patrimônio da CMBH.
Até 1 (hum) dia útil para solução do problema, contados da formalização do chamado pela CMBH	Durante a execução do serviço e período de garantia vigente, a CONTRATADA deverá ser acionada formalmente através de chamadas de e-mail, ofícios e/ou sistema disponibilizado para tal, devendo ser iniciado o atendimento.

11. FORMA DE PAGAMENTO

Os pagamentos de darão da seguinte forma:

11.1. Da Entrega: a empresa contratada terá até 60 (sessenta) dias corridos, contados da assinatura do contrato para entregarem os equipamentos. O pagamento referente aos equipamentos será feito, em parcela única, em até 30 (trinta) dias, após a entrega dos mesmos, devidamente atestado pelo fiscal do contrato;

11.2. Da Instalação: a empresa, após a entrega dos equipamentos, terá até 60 (sessenta) dias para instalar e configurar os equipamentos no ambiente da

CMBH. O pagamento dos serviços será feito, em parcela única, em até 30 (trinta) dias, após a conclusão do serviço, devidamente atestado pelo fiscal do contrato;

11.3. Do Treinamento: O pagamento dos serviços será feito, em parcela única, em até 30 (trinta) dias, após a conclusão do treinamento, devidamente atestado pelo fiscal do contrato.

11.4. Da prestação de serviços de manutenção e garantia: O serviço de manutenção deverá ser prestado por 36 (trinta e seis) meses, a contar do termo de aceite do serviço de implementação / instalação. O pagamento do item 4 da proposta será feito mensalmente, a patir da conclusão e aceite da instalação, devidamente atestado pelo fiscal do contrato.

12. FISCALIZAÇÃO

12.1. Nos termos do § 1º do artigo 67 da Lei 8.666/1993, caberá ao representante da SECITI, que será também o fiscal do contrato, proceder às anotações das ocorrências relacionadas com a execução do objeto, determinando o que for necessário à regularização das falhas ou impropriedades observadas.

12.2. A fiscalização é exercida no interesse da CMBH, não excluindo ou reduzindo a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade e, na sua ocorrência, não implica corresponsabilidade da CMBH ou de seus agentes e prepostos.

12.3. A CMBH se reserva o direito de não receber o serviço prestado em desacordo com as especificações e condições constantes deste Anexo, podendo rescindir a contratação e aplicar as penalidades previstas em Contrato e na legislação pertinente.

12.4. Quaisquer exigências da fiscalização, inerentes ao objeto contratado, deverão ser prontamente atendidas pela CONTRATADA, sem quaisquer ônus adicionais para a CMBH.

13. VIGÊNCIA DO CONTRATO:

O contrato vigorará, a partir da data de sua assinatura, por 40 (quarenta) meses, podendo ser renovado dentro dos limites legais.

CÂMARA MUNICIPAL DE BELO HORIZONTE

ANEXO - MODELO DE PROPOSTA COMERCIAL -

OBJETO: Contratação de empresa para o fornecimento de **solução de proteção de redes com característica de "Next Generation Firewall – NGFW" para segurança de informação perimetral** incluindo equipamentos redundantes, licenças, treinamento, suporte técnico e garantia pelo prazo de 36 (trinta e seis) meses, em acordo com as especificações do edital.

DENOMINAÇÃO SOCIAL DA SOLICITANTE:_____
CNPJ:_____

Apresenta esta licitante, **por intermédio de seu representante legal**, proposta comercial para os itens abaixo, cuja especificação completa encontra-se detalhada no termo de referência:

ITEM	QTD	DESCRIÇÃO RESUMIDA	UNIDADE	PREÇO UNITÁRIO (R$)	PREÇO TOTAL DO ITEM (R$)
I	2	Solução de Segurança de alta disponibilidade licenciado para 36 meses e garantia pelo mesmo período(hardware e software) **Especificar fabricante e modelo do equipamento**	UN		
2	1	Implementação / instalação da solução completa no formato hands-on com suporte remoto (8 x 5) em português.	UN		
3	1	Treinamento para operação e administração da solução ofertada para uma equipe de 4 (quatro) pessoas, com carga horária de no mínimo 20 (vinte) horas-aula	UN		

SECORC 86v.

CÂMARA MUNICIPAL DE BELO HORIZONTE

4	36	Manutenção, atualização e suporte 24 x 7, garantia de troca do equipamento no próximo dia útil. Por 36 meses a contar do aceite da instalação.	UN		
VALOR TOTAL DA PROPOSTA:					

OBSERVAÇÕES

1) O serviço ofertado obedece a todas as condições, especificações e características estabelecidas no **TERMO DE REFERÊNCIA "COOINF 003/16"**, responsabilizando-se a licitante, com a apresentação de sua proposta, pela veracidade desta informação.

2) Nos preços ofertados já foram considerados todos os encargos e tributos incidentes sobre o objeto supracitado.

PRAZO DE VALIDADE DA PROPOSTA COMERCIAL: _____ dias (mínimo de 60 dias, a contar da data final prevista para a entrega dos envelopes).

Belo Horizonte, _____ de _____ de 2017.

_____

Nome, carimbo e assinatura de **representante legal** da licitante

CÂMARA MUNICIPAL DE BELO HORIZONTE

SOLICITAÇÃO ADMINISTRATIVA AQUISIÇÃO/CONTRATAÇÃO

SECORC 40

Nº TR *(Deverá ser preenchido nos casos em que o setor controla a produção de TRs e/ou quando o setor fizer a cotação de preços)*	Nº Protocolo Geral de Solicitação Administrativa *(Preenchimento pela SECORC)*
COOINF 001/2017	

1. TIPO

■ Contratação tradicional

☐ Registro de Preços

Vigência da Ata em meses:
(máximo 12 meses)

Em caso de vigência inferior a 12 meses: A Ata poderá ter sua vigência renovada nos termos e limites legais?

☐ SIM ☐ NÃO

2. QUANTITATIVO DE ITENS

LOTE Nº	ITEM Nº	BEM/SERVIÇO	UNIDADE	QUANTIDADE
	01	Solução de Segurança de alta disponibilidade licenciado para 36 meses baseada em Appliance com recursos de Next Generation Firewall (NGFW).	UN	2
	02	Implementação da solução completa no formato hands-on com suporte remoto (8 x 5) em português.	UN	1
	03	Treinamento para operação e administração da solução ofertada para uma equipe de 4 (quatro) pessoas, com carga horária de no mínimo 20 (vinte) horas-aula, a ser ministrado após a implementação da solução de segurança.	UN	1
	04	Contrato de manutenção, atualização e suporte 24 x 7, pelo período de 36 meses e garantia de troca do equipamento no próximo dia útil, a contar da efetiva instalação do Appliance.	UN	1

COORDENADORIA DE INFORMÁTICA

CÂMARA MUNICIPAL DE BELO HORIZONTE

SOLICITAÇÃO ADMINISTRATIVA AQUISIÇÃO/CONTRATAÇÃO

SECORC 41

3. ESPECIFICAÇÃO COMPLETA DO OBJETO (contemplar também as condições gerais de execução e de aceitação do objeto)

CONFORME TR

4. LOCAL E HORÁRIO PARA ENTREGA DO BEM OU DA PRESTAÇÃO DO SERVIÇO

CONFORME TR

5. FORMA DE ENTREGA DO BEM OU DA PRESTAÇÃO DO SERVIÇO

■ Única

Para os itens:

☐ Constante

Para os itens:

☐ Parcelada:

Para os itens:

Definir forma de parcelamento:

6. PRAZO PARA A ENTREGA DO BEM OU INÍCIO DA PRESTAÇÃO DO SERVIÇO

☐ Até dias a partir da emissão da Ordem de Compra.

■ Outro: **CONFORME TR**

7. PRAZO E CONDIÇÕES DE GARANTIA PARA O BEM OU SERVIÇO (Refere-se à garantia quanto aos vícios (defeitos) dos produtos ou dos serviços)

É caso de exigência de garantia diversa da prevista no Código de Defesa do Consumidor?

☐ Não ■ Sim

Justificativa em caso positivo:

Conforme TR

Prazo e condições da garantia:

8. GARANTIA CONTRATUAL (Refere-se à garantia do adimplemento e do fiel cumprimento das obrigações assumidas pela contratada)

Exigência de garantia contratual?

■ Sim ☐ Não

COORDENADORIA DE INFORMÁTICA

Justificativa em caso positivo:

Devido ao prazo do contrato, valor do bem/serviço e importância do processo para o perfeito funcionamento e segurança da rede de dados da casa.

Em caso positivo:

Percentual da garantia: 2% (até 5% do valor contratado)

Justificativa para o percentual escolhido:

O montante mair do contrato esta relacionado à entrega de bens ou serviços, assim sendo a garantia cobre os custos caso seja necessária a contratação de serviço de reconfiguração caso a empresa não cumpra o contrato.

9. VIGÊNCIA DA CONTRATAÇÃO*

☐ Durante o Exercício (Ano):

■ Nº de meses: 36 meses

☐ Até o dia:

☐ Até o término da garantia

Em caso de serviço continuado e vigência superior a 12 meses, justificar a vantajosidade da contratação pelo período solicitado:

Pela característica do bem/serviço adquirido que envolve proteção de dados para da CMBH é estratégia adquirir pelo prazo especificado uma vez que é um serviço com atualização de assinaturas constante.

*Obs: No caso de Registro de Preços esta vigência se refere às futuras contratações decorrentes da Ata de Registro de Preços.

10. POSSIBILIDADE DE PRORROGAÇÃO

Conforme Lei 8666/1993:

Art. 57. A duração dos contratos regidos por esta Lei ficará adstrita à vigência dos respectivos créditos orçamentários, exceto quanto aos relativos:

I - aos projetos cujos produtos estejam contemplados nas metas estabelecidas no Plano Plurianual, os quais poderão ser prorrogados se houver interesse da Administração e desde que isso tenha sido previsto no ato convocatório;

II - à prestação de serviços a serem executados de forma contínua, que poderão ter a sua duração prorrogada por iguais e sucessivos períodos com vistas à obtenção de preços e condições mais vantajosas para a administração, limitada a sessenta meses;

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

11. CONDIÇÕES DE PAGAMENTO

As condições de pagamento são as previstas nos modelos de Minuta de Contrato / Contratação por nota de empenho disponíveis no Portal da CMBH.

Adaptações a serem consideradas nas condições e prazos de pagamento para atendimento ao objeto especificado:

☐ Sem alterações

■ Considerar as seguintes alterações:

CONFORME TR

Justificativa da alteração:

Obs: Caso as alterações constantes neste item conflitem com as condições estabelecidas no edital e seus anexos, prevalecerá este Termo de Referência.

12. PENALIDADES

As penalidades aplicáveis são as previstas na Portaria 16.707/2016, constantes nos modelos de Minuta de Contrato / Contratação por nota de empenho disponíveis no Portal da CMBH.

Adaptações a serem consideradas nas penalidades para atendimento ao objeto especificado:

■ Sem alterações

☐ Considerar as seguintes alterações:

Justificativa da alteração:

Obs: Caso as alterações constantes neste item conflitem com as condições estabelecidas no edital e seus anexos, prevalecerá este Termo de Referência.

13. FATURAMENTO

O faturamento será realizado:

■ Ao final da execução

☐ Por evento

☐ Mensalmente

14. OBRIGAÇÕES DA CMBH

a) Proporcionar todas as condições para que a CONTRATADA possa executar o objeto.

b) Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA.
c) Exercer o acompanhamento e a fiscalização da execução do objeto.
d) Notificar a CONTRATADA acerca da ocorrência de eventuais imperfeições na execução do objeto.
e) Efetuar à CONTRATADA o pagamento resultante da execução do objeto.

15. INFORMAÇÕES COMPLEMENTARES

- *Os campos a seguir são de uso interno da CMBH*

CÂMARA MUNICIPAL DE BELO HORIZONTE

SOLICITAÇÃO ADMINISTRATIVA AQUISIÇÃO/CONTRATAÇÃO

SECORC 45

PARA USO INTERNO NA CMBH

16. JUSTIFICATIVA DA CONTRATAÇÃO

CONFORME TR

17. AGRUPAMENTO DE ITENS

A contratação será por:

☐ Item ■ Lote

18. Justificativa no caso de aquisição por lote:

Devido a complexidade da aquisição é necessário que a empresa fornecedora dos equipamentos seja também responsável pela sua configuração, instalação e manutenção.

19. INDICAÇÃO DE MARCA

Foi necessário indicar marca de produto na especificação, que não seja apenas de referência?

☐ Sim ■ Não

Em caso positivo, justificar nos termos específicos da lei:

20. DOCUMENTOS ADICIONAIS DE HABILITAÇÃO

☐ Nenhum

■ Atestado de Capacidade Técnica

☐ Declaração de Disponibilidade de Pessoal

☐ Declaração de Disponibilidade de Equipamentos

☐ Registros de profissional/empresa

☐ Certidão de falência/recuperação judicial

☐ Análise de índices financeiros

☐ Outro:

21. Justificativa(s) e condições para o(s) documento(s) exigido(s):

Devido à especificidade e complexidade do produto / serviço torna-se necessário a comprovação que a empresa tem experiência previa na execução do trabalho. Além de resguardar a CMBH quanto a qualidade do produto entregue.

22. NECESSIDADE DE AMOSTRA

☐ SIM ■ NÃO

23. Justificativa:

COORDENADORIA DE INFORMÁTICA

24. Critérios objetivos para análise da amostra:

25. TERMO DE CONTRATO

25.1. O objeto pretendido envolve em sua execução a entrega parcelada dos bens a serem adquiridos?

☐ Sim ☐ Não ■

25.2. Na descrição do objeto a ser contratado, exige-se alguma obrigação futura que não seja exclusivamente a entrega dos bens a serem adquiridos (exemplo: garantia estendida, manutenção, treinamento, assistência técnica)?

■ Sim ☐ Não

25.3. Está incluída, na descrição do objeto a ser contratado, a prestação de assistência técnica?

■ Sim ☐ Não

26. Caso a resposta às três indagações anteriores seja sempre NÃO, o termo de contrato é dispensado.

Mesmo sendo dispensável o termo de contrato, há interesse em sua celebração?

■ Sim ☐ Não

27. Justificativa em caso positivo:

Observações:
Nos casos em que o Termo de Contrato for exigência legal a celebração será realizada independente da opção do demandante.

28. SERVIDOR RESPONSÁVEL PARA ESCLARECIMENTOS

NOME: Lilliam Brandão

SETOR: SECITI

RAMAL: 1135

NOME: Paulo Furiati

SETOR: COOINF

RAMAL: 1135

29. GESTOR DA CONTRATAÇÃO

O gestor será o titular do setor indicado abaixo:

Setor: SECITI

30. FISCAL DA CONTRATAÇÃO

Será designado fiscal para esta contratação? ☐ Sim ■ Não

Nome do profissional fiscal da contratação:

31. RESPONSÁVEL PELA ELABORAÇÃO DESTE TERMO DE REFERÊNCIA

Nome: Paulo Furiati

Cargo: Coordenador de Informática

Assinatura: _____

Paulo César Soares Furiati
Coordenador de Informática
CM 40.434

32. APROVAÇÃO PELO DIRETOR DA ÁREA OU EQUIVALENTE

Nome: Paulo Furiati

Cargo: Coordenador de Informática

Assinatura: _____

Paulo César Soares Furiati
Coordenador de Informática
CM 40.434

33. Belo Horizonte 04 de 07 de 2017.

Em caso de fornecedor exclusivo, nos termos do art. 25, I, da Lei 8.666/93, apresentar documentação comprobatória de exclusividade.

Após preenchido pela área demandante, o arquivo eletrônico deste documento deve ser encaminhado para o e-mail sistemasdirafi@cmbh.mg.gov.br.

CÂMARA MUNICIPAL DE BELO HORIZONTE

Ofício CPL 13/2017

Belo Horizonte, 28 de setembro de 2017.

Senhor Coordenador,

Encaminho a Vossa Senhoria o processo de aquisição protocolado sob o nº 2868/2017, que visa "Aquisição de solução de segurança de borda de rede baseada em tecnologia NGFW", e solicito o esclarecimento das questões apontadas no quadro abaixo, para que seja dada continuidade à análise do processo e elaboração do edital de licitação.

Assunto	Item	Item contraditório / observação
Prazo de execução das etapas 3 , 4 e treinamento	Item 10 – quadro: até 30 dias da entrega dos equipamentos	11.2 e 6.2.5.7 - Até 60 dias da entrega dos equipamentos
Início da Manutenção	- Proposta comercial (item 4): do aceite da instalação; - Item 11.4 da especificação: do aceite da implementação / instalação	- 6.2.4.1 : do aceite definitivo (ver 6.2.5.11 – inclui ter sido feita a habilitação da garantia) - 6.2.5.9 : do registro dos produtos junto ao fabricante
Vigência do Contrato	Item 13: 40 meses	Item 9 do TR padrão (pág. 42): 36 meses
Item 13 do TR padrão	Faturamento ao final da execução: final da execução é após 40 meses.	Não teria que acrescentar execução "de cada etapa" (ou marcar evento) e incluir o mensalmente?
Pagamento da manutenção	11.4: mensal e inicia com o aceite da instalação	Resolver contradições do início da manutenção, para determinar o início do pagamento.
Código do comprasnet	Manter os anteriores? 150100 – 1260 – 16837 - 1260	
Atestado de capacidade técnica	Item 20 do TR	Definir os termos exatos que devem constar no atestado, tomando o cuidado de não restringir a competitividade.

Coloco-me à disposição para quaisquer esclarecimentos que se fizerem necessários.

Atenciosamente,

Márcia Ventura Machado
Pregoeira

Senhor Paulo Furiati
Coordenador de Informática
Câmara Municipal de Belo Horizonte

CÂMARA MUNICIPAL DE BELO HORIZONTE

Of. COOINF Nº 0012/2017

Belo Horizonte, 16 de outubro 2017.

Prezada Pregoeira,

Seguem nossas considerações relativas ao seu ofício de 28/09 referente ao processo de aquisição de "Solução de Segurança de borda de rede baseada em tecnologia NGFW", processo 2868/2017.

Assunto	Esclarecimento ao questionamento
Prazo de execução das etapas 3, 4 e treinamento	O prazo de 30 dias constante do quadro do item 10 está equivocado, deve ser atualizado para os mesmos dos itens 11.2 e 6.2.5.7, ou seja, 60(sessenta dias).
Início da Manutenção	Não há divergência entre as informações. Os termos constantes da proposta comercial são apenas um resumos das atividades informadas nos itens 6.2.4.1, 6.2.5.11 e 6.2.5.9
Vigência do contrato	Diante das somas de prazos de entrega, instalação e garantia o contrato deve prevalecer por 40 meses. O Valor do edital padrão deve ser modificado para este prazo.
Item 13 do TR padrão	Correto, o faturamento deve acontecer de acordo com o descrito no edital, ou seja, a cada etapa cumprida.
Pagamento da manutenção	Deve iniciar-se após a instalação, conforme descrito acima. A prática de mercado é o pagamento em única parcela, mas por exigência da DIVIGEF aconteceu a modificação. Este é um ponto que poderá ser elucidado no memento da consulta pública.
Código Comprasnet	Podem ser mantidos pois não houve modificação do objeto.
Atestado de capacidade técnica	Devido a padronização do formulário, por equívoco no preenchimento, ficaram faltando as condições para habilitação técnica. Assim sendo as mesmas seguem em anexo.

Atenciosamente,

Paulo César Soares Furiati
Coordenador de Informática

Sra. Márcia Ventura
Pregoeira
Câmara Municipal de Belo Horizonte.

Documentos necessários para habilitação técnica

3 - Deverão ser exigidos, na fase de habilitação, em virtude da necessidade de se garantir qualidade aos serviços pretendidos, os seguintes documentos, afora os habitualmente pedidos nas licitações realizadas pela CMBH:

3.1 - de qualificação técnica:

(a) Atestado de capacidade técnica: Apresentar pelo menos 1 (um) atestado de capacidade técnica, que comprove o fornecimento, instalação, configuração e treinamento, cujo projeto seja do mesmo fabricante da solução ofertada e tenha sido realizado para um ambiente com no mínimo 1.000 (mil) usuários.

(b) Indicar, através de declaração, possuir em seu quadro de profissionais, pelo menos 1 (um) profissional com Certificado emitido pelo fabricante da solução ofertada capacitando-o para sua implementação. A comprovação se dará através da apresentação de cópia autenticada do contrato social da empresa em caso de sócio, cópia da carteira de trabalho do profissional ou cópia autenticada do contrato de trabalho firmado entre as partes em caso de empregado. Será solicitada também a cópia do certificado emitido pelo fabricante da solução.

(c) Considerando as características do objeto deste edital, onde trata de projeto de monta considerável far-se-á necessário a comprovação de que a licitante já utiliza as melhores práticas no gerenciamento de projetos, indicando, através de declaração, possuir em seu quadro de profissionais, pelo menos 1 (um) profissional com **Certificação PMP**. A comprovação se dará através da apresentação de cópia autenticada do contrato social da empresa em caso de sócio, cópia da carteira de trabalho do profissional ou cópia autenticada do contrato de trabalho firmado entre as partes em caso de empregado. Será solicitada também a cópia do certificado.

(d) Considerando as características que o objeto deste edital, onde trata de serviços na infraestrutura de TIC da CMBH far-se-á necessário a comprovação de que a licitante já utiliza as melhores práticas em gerenciamento de serviços e suporte de TI indicando, através de declaração, possuir em seu quadro de profissionais pelo menos 01 (um) profissional certificado em ITIL CERTIFIED FOUNDATION. A comprovação se dará através da apresentação de cópia autenticada do contrato social da empresa em caso de sócio, cópia da carteira de trabalho do profissional ou cópia autenticada do contrato de trabalho firmado entre as partes em caso de empregado. Será solicitada também a cópia do certificado.

Obs.: Todas as comprovações exigidas acima deverão ser feitas no momento da assinatura do contrato.