PROJETO BÁSICO DA NOVA REDE MACEIÓ

PREFEITURA DA CIDADE DE MACEIÓ

Rui Soares Palmeira
Prefeito de Maceió

Marcelo Palmeira Cavalcante
Vice-Prefeito de Maceió

Reinaldo Braga da Silva Júnior
Secretário de Gestão

Israel Lucas Souza Guerreiro de Jesus
Secretário Adjunto de Gestão / Escola de Governo

Antônio Estanislau de Oliveira Neto
Secretário Adjunto de Gestão

Fernando Antônio Dantas Gomes Pinto
Diretor de Tecnologia da Informação / SEMGE

Felipe Gomes de Oliveira
Coordenador Geral de Controle e Acompanhamento de Serviços / SEMGE

Marlo Cezar de Aleluia
Gerência de Rede / SEMGE

João Geraldo de Oliveira Lima
Coordenador Geral de Desenvolvimento de Projetos / SEMGE

José Romulo Ribeiro da Silva
Coordenador de TI/SMS

José Max Deivys Alves de Moura
Coordenador TI/SEMED

Marcelo Santos Silva
Analista Sistema/SEMAS

PROJETO BÁSICO DA NOVA REDE MACEIÓ

PREFEITURA DA CIDADE DE MACEIÓ

1. APRESENTAÇÃO DO PROJETO NOVA REDE MACEIÓ

1.1. O projeto Intitulado "Nova Rede MACEIÓ" trata da estruturação da rede de Dados e telecomunicações da Prefeitura Municipal de Maceió, com a integração e melhoria dos serviços de MPLS, DADOS, VOIP, TELEFONIA FIXA, TELEFONIA MÓVEL, REDE DE DADOS e seus serviços auxiliares. A necessidade de implantação de uma rede convergente e multiplataforma é um desafio para a construção de estruturas que forneçam uma melhor prestação de serviço para a comunidade, além de disponibilizar um ambiente de trabalho mais eficiente para os servidores.

1.2. A informatização cada vez maior e a necessidade de trocas de dados e informações mais eficientes é tratado como prioritário para que a prestação de serviço público eleve seu padrão de qualidade e o seus usuários possam perceber suas melhorias, com o aumento do fornecimento de serviços on-line, redução de custos diversos, melhoria no acesso à informação além do aprimoramento e agilidade no processo de tomada de decisão.

2. OBJETIVOS DO PROJETO

2.1. Este projeto pretende oferecer a Prefeitura da Cidade de Maceió a prestação de serviços de comunicação multisserviços com racionalização de investimentos e ampliação de serviço, beneficiando e melhorando o exercício da gestão pública.

Subsidiar a construção de uma solução de comunicação chamada de SISTEMA INTEGRADO DE TELECOMUNICAÇÃO DA PREFEITURA DA CIDADE DE MACEIÓ.

2.2. Subsidiar a construção de uma solução de comunicação multisserviços.

3. FINALIDADES DO PROJETO

3.1. Proporcionar a Prefeitura de Maceió uma solução integrada garantindo um salto qualitativo e quantitativo na expansão da oferta de serviços públicos à sociedade de Maceió, assegurando alta qualidade tecnológica, relacionamento uniformizado para todos os clientes e usuários, racionalização de recursos e ampliação de serviços, economia de escala com preços aderentes aos atualmente praticados pelo mercado.

3.2. Utilizar serviços de teleinformática e tecnologias adequadas para a promoção de inovações tecnológicas, expansão dos serviços oferecidos por meios digitais, facilitando a interligação de órgãos, que por sua vez, ampliará a oferta e melhoria da qualidade dos serviços prestados à sociedade.

3.3. Atender às unidades administrativas, localizadas nas zonas urbanas da capital, inclusive aquelas menos assistidas por infraestrutura básica.

3.4. Permitir uma gestão integrada facilitando e otimizando tomada de decisões por parte da Prefeitura de Maceió.

3.5. Garantir a comunicação e integração de voz e dados entre todos os órgãos da Prefeitura através da NOVA REDE MACEIÓ.

3.6. Garantir a comunicação entre todos os órgãos municipais através da NOVA REDE MACEIÓ, que permitirá a operação de Sistemas Transacionais, Sistemas Informacionais, Sistemas Corporativos Públicos, acessos às Bases de Dados Públicas Institucionais, entrada/saída de dados, acesso à informação e serviços, na web, videoconferência e teleconferência.

4. JUSTIFICATIVA DO PROJETO

4.1. O projeto NOVA REDE MACEIÓ justifica-se pela necessidade de instrumentalizar a Prefeitura da Cidade de Maceió com uma Rede de voz e dados Integrada, a serviço da modernização da gestão pública e para o fomento do desenvolvimento econômico e social em diversas áreas do conhecimento, com os seguintes aspectos:

4.1.1. Ampliar a prestação dos serviços integrados de telemática adequando-os às necessidades das unidades administrativas da cidade de Maceió, possibilitando assim, a expansão dos serviços de prefeitura voltados ao atendimento do cidadão.

4.1.2. Estabelecer um Modelo de Gestão de Telemática que ofereça um controle efetivo de previsão mensal de despesas, por parte da Prefeitura, e acompanhamento das despesas na área de comunicação de dados.

4.2. Agilizar a prestação dos serviços de telemática unificando e padronizando a aquisição de tecnologias para comunicação convergente de forma a atender as especificações técnicas e de prazos exigidas pelos projetos da prefeitura, facilitando a Gestão Pública, como:

4.2.1. Atualização tecnológica;

4.2.2. Manutenção de equipamentos de rede de dados e telefonia fixa e móvel;

4.2.3. Administração e gerência dos recursos e serviços tecnológicos com abrangência em Maceió;

4.2.4. Melhorar a qualidade dos serviços.

4.3. Oferecer tecnologias convergentes e integradas para que os sistemas de informações setoriais e corporativos operacionalizados em diferentes plataformas passem a compartilhar uma mesma estrutura para os serviços de comunicação convergentes.

4.4. Oferecer tecnologias convergentes multisserviços para serem usadas em acessos a Sistemas de Informações Públicas, acesso à Internet, e disponibilizar um canal de comunicação entre as unidades administrativas da prefeitura e entre a sociedade, com a garantia de soluções específicas de segurança implementadas.

4.5. Oferecer e contemplar de forma padronizada às unidades administrativas da Prefeitura Municipal da cidade de Maceió, distribuídas em todo seu território, de acordo com as características específicas de cada uma.

4.6. Uniformizar os custos de operacionalização da rede, através da coordenação integrada dos recursos e serviços envolvidos.

4.7. Eliminar custos em aquisição de equipamentos para recursos de conectividade e configurações necessárias na prestação dos serviços de tecnologia de comunicação convergentes, tirando dos usuários o problema de manutenção e atualização tecnológica, que tem sido um fator dificultador para a Gestão Pública.

4.8. Manter e ampliar todos os benefícios já implantados com a atual REDE DE DADOS da Prefeitura da Cidade de Maceió.

ANEXO 1
Termo de Referência
LINK DEDICADO DE CONECTIVIDADE COM A INTERNET

1. LINK DEDICADO DE CONECTIVIDADE COM A INTERNET

1.1. Definições

O link dedicado é um serviço especialmente desenvolvido para o setor corporativo, onde as empresas ou governos tem acesso a um link exclusivo para a transmissão de dados, sem a necessidade de compartilhamento deste link.

2. OBJETO DA CONTRATAÇÃO

2.1. Trata-se da abertura de processo licitatório de Registro de preço, para contratação, de empresa especializada em telecomunicação para fornecimento do serviço de link dedicado de conectividade com a Internet nas velocidades de 1 Gbps, 300 Mbps, 200 Mbps e 50 Mbps, já incluindo a infraestrutura de conectividade física e lógica, com a disponibilização de suporte completo para roteamento dos protocolos de IPV4 e IPV6 e velocidades simétricas para *upstream* e *downstream* e serviço de firewall, conforme tabela 1 e contratação de empresa para fornecimento e gerenciamento da segurança de rede com a alocação de solução integrada de software e hardware com funcionalidades de firewall, filtro de conteúdo web, prevenção de instrução e Serviços de Monitoramento de Disponibilidade e Performance, Gestão de Eventos de Segurança e Gerenciamento de Segurança de Rede.

Tabela 1: Detalhamento da contratação

ITEM	SERVIÇOS	VELOCIDADE	QUANT.	ESTIMATIVA DE CONTRATAÇÃO INICIAL	NÚMEROS IP-V4	NÚMEROS /64 IP-V6	PAGAMENTO
1	Link dedicado de conectividade com a Internet com velocidade de 1 Gbps, suporte completo para roteamento dos protocolo IPV4 e IPV6 e velocidades	1 Gbps *Full*	1	1	30	1	Mensal

	simétricas para *upstream* e *downstream*.						
2	Link dedicado de conectividade com a Internet com velocidade de 300 Mbps, suporte completo para roteamento dos protocolo IPV4 e IPV6 e velocidades simétricas para *upstream* e *downstream*.	300 Mbps	5	1	20		Mensal
3	Link dedicado de conectividade com a Internet com velocidade de 200 Mbps, suporte completo para roteamento dos protocolo IPV4 e IPV6 e velocidades simétricas para *upstream* e *downstream*.	200 Mbps	5	0	10		Mensal
4	Link dedicado de conectividade com a Internet com velocidade de 50 Mbps, suporte completo para roteamento dos protocolo IPV4 e IPV6 e velocidades simétricas para *upstream* e *downstream*.	50 Mbps	15	0	10		Mensal

ITEM	DESCRIÇÃO	QUANTITATIVO	ESTIMATIVA DE CONTRATAÇÃO INICIAL
5	Solução para atuar, de forma proativa, no monitoramento e gestão de eventos de segurança para detectar precocemente incidentes e mitigar possíveis vulnerabilidades e/ou ataques que a Prefeitura esteja sofrendo naquele momento, incluindo solução de equipamentos (hardwares) e seus programas (softwares), objetivando uma melhor integração entre os equipamentos e os serviços já existentes, para um link de 1 Gbps	3	2
6	Solução para atuar, de forma proativa, no monitoramento e gestão de eventos de segurança para detectar precocemente incidentes e mitigar possíveis vulnerabilidades	5	1

	e/ou ataques que a Contratante esteja sofrendo naquele momento, incluindo solução de equipamentos (hardwares) e seus programas (softwares), objetivando uma melhor integração entre os equipamentos e os serviços já existentes, para um link de 300 Mbps		
7	Solução para atuar, de forma proativa, no monitoramento e gestão de eventos de segurança para detectar precocemente incidentes e mitigar possíveis vulnerabilidades e/ou ataques que a Contratante esteja sofrendo naquele momento, incluindo solução de equipamentos (hardwares) e seus programas (softwares), objetivando uma melhor integração entre	5	0

	os equipamentos e os serviços já existentes, para um link de 200 Mbps		
8	Solução para atuar, de forma proativa, no monitoramento e gestão de eventos de segurança para detectar precocemente incidentes e mitigar possíveis vulnerabilidades e/ou ataques que a Contratante que esteja sofrendo naquele momento, incluindo solução de equipamentos (hardwares) e seus programas (softwares), objetivando uma melhor integração entre os equipamentos e os serviços já existentes, para um link de 50 Mbps	15	0

3. JUSTIFICATIVA

3.1. Diante do atual cenário tecnológico que se encontra a Prefeitura Municipal de Maceió com a imprescindibilidade de acesso aos serviços fornecidos pelas suas Secretarias através de diversos sistemas desenvolvidos para ambiente WEB (World Wide Web - Rede Mundial de Computadores) - emissão de guias de pagamento de tributos (IPTU, ISS, Taxa de Localização, etc), sistema de gestão acadêmica, gestão de matrícula on-line dos estudantes (aproximadamente 50.000 alunos), emissão de contracheques, emissão de demonstrativo financeiro referente ao Imposto de

Renda Retido na Fonte - IRRF, Sistemas administrativos (Protocolo Unificado, Folha de Pagamento, Almoxarifado, Patrimônio, etc), Sistemas de gestão da saúde, E-SUS, entre outros.

3.2. Para prestação dos serviços supracitados, atualmente a Prefeitura Municipal de Maceió possui em sua estrutura tecnológica 1 (um) link dedicado de 1 (um) Gbps, que atende a demanda da Secretaria Municipal de Gestão, Secretaria Municipal de Economia, Secretaria Municipal de Educação (e suas escolas), Secretaria municipal de Saúde (e seus postos), além de outras que estão sendo atendidas na rede privada MPLS. Desta forma, faz-se necessário em casos específicos a previsão de contratação de links dedicados de Internet, com velocidades de 1 Gbps full e no intervalo de 50, 200 e 300 Mbps, para estas secretarias mais demandantes do recurso, atendendo necessidades temporárias ou fixas.

3.3. Nessa senda, torna-se necessária a eminente contratação de uma empresa especializada em telecomunicação para fornecimento do serviço de link de conectividade com a Internet nas velocidades de 1 Gbps, 300 Mbps, 200 Mbps e 50 Mbps para que a Prefeitura Municipal de Maceió disponibilize um serviço de acesso à Internet de maneira que venha produzir efeitos necessários com toda excelência na prestação de seus serviços de acesso dedicado e direto à Internet.

3.4. Considerando ainda que a Prefeitura de Maceió possui instalado, em sua plataforma corporativa, vários servidores computacionais críticos ao seu negócio; Considerando o crescente número de ameaças e ataques identificados, expondo ou debilitando a rede da Prefeitura de Maceió; Considerando o nível de especialização necessária e a grande quantidade de atualizações técnicas para a manutenção deste tipo de serviço; Considerando a necessidade de manter este serviço ativo ininterruptamente, inclusive com monitoramento constante e pessoa qualificado para atuação; Considerando a necessidade de suporte para múltiplos serviços de apoio técnicos e incidentes ilimitados; Fundamentado nas considerações descritas anteriormente, faz-se necessário contratação de solução para atuar, de forma proativa, no monitoramento e gestão de eventos de segurança para detectar precocemente incidentes e mitigar possíveis vulnerabilidades e/ou ataques que a Prefeitura esteja sofrendo naquele momento, incluindo solução de equipamentos (hardwares) e seus programas (softwares), objetivando uma melhor integração entre os equipamentos e os serviços já existentes.

3.5. Entende-se que a aquisição dos serviços de fornecimento de link de internet e a de serviço de segurança de rede são fundamentais para uma melhoria da qualidade dos serviços prestados a sociedade.

4. DEFINIÇÕES

4.1. **24x7** - Modelo de requisito da prestação de serviços, sendo exigido acesso ao serviço vinte e quatro horas por dia, sete dias por semana, inclusive em feriados.

4.2. **Appliance c**onjunto de Software e Hardware (equipamento) especializado e dedicado a uma finalidade (ou conjunto de) específica.

4.3. **BI** - (Business Intelligence) Refere-se ao processo de coleta, organização, análise, compartilhamento e monitoramento de informações que oferecem suporte a gestão de negócios.

4.4. **Captive Portal** Software responsável por controlar e gerenciar o acesso à Internet em redes públicas, de forma "automatizada".

4.5. **NGFW** - (Next-Generation Firewall) Appliance dedicado a segurança integrada de diversos itens da rede corporativa (Firewall intuitivo).

4.6. **DDoS** - (Distributed Denial of Service) Tipo de ataque virtual, sobrecarregando os servidores ou a rede com requisições inválidas (do ponto de vista do negócio), a partir de várias origens, gerando lentidão e até a parada total dos serviços.

4.7. **DoS** - (Denial of Service) Tipo de ataque virtual, sobrecarrega os servidores ou a rede com requisições inválidas (do ponto de vista do negócio), gerando lentidão e até a parada total dos serviços. Gbps Unidade de transferência de dados – Giga bits por segundo

4.8. **HA** - (High Availability) Característica de um sistema – eliminação de ponto único de falha; cruzamento confiável; detecção imediata e automática de falhas; alta disponibilidade com tolerância a falhas.

4.9. **IP** - (Internet Protocol) Protocolo de rede, representado pelo identificador, único na subrede, que individualiza cada equipamento a ela ligado.

4.10. **IPv6** - Versão mais atual do Protocolo de Internet (IP), ainda não amplamente adotado/utilizado, mas é uma atualização necessária dadas as limitações de sua versão mais difundida, o IPv4.

4.11. **LDAP** - (Lightweight Directory Access Protocol) Protocolo de aplicação para acessar e manter serviços de informação de diretório distribuído da rede.

4.12. **NAT** (Network Address Translation) Técnica que consiste em reescrever, os endereços IP de origem de um pacote que passam pelo firewall de maneira que um computador de uma rede interna tenha acesso ao exterior.

4.13. **P2P** - (Peer-to-Peer) Rede de troca de arquivos, interligando diretamente computadores ponto a ponto. URL (Uniform Resource Locator) Endereço da página na Internet.

4.14. **VoIP** - (Voice over IP) Tecnologia que permite efetuar ligações telefônicas através da internet (sem uso de sinal de telefone).

5. DA DOTAÇÃO ORÇAMENTÁRIA

5.1. As despesas decorrentes da aquisição do objeto deste termo de referência correrão por conta dos recursos consignados no Orçamento Geral do Município de Maceió.

6. REQUISITOS OBRIGATÓRIOS DA CONTRATADA

6.1. Os serviços apresentados pela empresa LICITADA, para os ITENS 1, 2,3 e 4, deverá abranger os seguintes requisitos:

6.1.1. Modalidade dedicado e deverá estar conectado à WEB (World Wide Web - Rede Mundial de Computadores) com total conectividade IP (Internet Protocol), provendo com total infraestrutura para instalação em equipamentos, meios de acesso e serviços da rede de dados e/ou outros projetos de redes mantidos ou gerenciados pela LICITANTE, incluindo disponibilização de todos os recursos de conectividade, tais como: modems, conversores, roteadores, cabos e outros concernentes ao funcionamento do serviço contratado;

6.1.2. O fornecimento dos serviços deverá ser realizado na estrutura física da Diretoria de Tecnologia da Informação - DTI da SEMGE e nas unidades demandantes do serviço apresentado no ANEXO A, de modo que possibilite administração através do gerenciamento concomitantemente com a LICITADA, de todo o roteamento de tráfego da rede, obrigando que todos os pacotes da rede com destino à Internet passem pelo ponto de acesso principal provendo de equipamentos com capacidade adequada para garantir o desempenho necessário no roteamento de todo o tráfego da Internet que estará conectado em suas interfaces;

6.1.3. A LICITADA deverá disponibilizar e implementar junto a LICITANTE recursos tecnológicos como protocolos e softwares que possibilitem o gerenciamento e, análise e auditoria em tempo real do desempenho do serviço prestado, bem como manter um histórico de acesso dos últimos 30 (trinta) dias;

6.1.4. Incorporar a rede de dados da LICITANTE a WEB (World Wide Web - Rede Mundial de Computadores), com acessos a velocidades de 1 Gbps, 300Mbps ou 200Mbps, dependendo do local da instalação;

6.1.5. Implementar aumentos de velocidades, quando necessários, de forma transparente. Sendo que, as atualizações tecnológicas requisitas para esse aumento devem

ser suportadas pelos recursos e equipamentos envolvidos na solução inicial, com paralisações de no máximo 3 (três) horas - impreterivelmente após o horário comercial - através de comunicação escrita e prévia de no mínimo 7 (sete) dias úteis;

6.1.6. O aumento de velocidade deverá ser realizado após a realização de um Laudo Técnico decorrente de análise de medições prévias solicitadas através de mecanismos formais previstos;

6.1.7. Fornecer endereçamento IP (Internet Protocol) público, versão IPv4 e IPv6, nas quantidades especificadas no quadro de "objeto da contratação", válidos para roteamento na Internet;

6.1.8. Assim que a LICITADA implantar o roteamento IPv6 em seu núcleo e suportar disponibilização de roteamento via BGP do mesmo, deverá disponibilizá-lo para a LICITANTE sem custos adicionais;

6.1.9. A LICITADA deve possuir acesso ao backbone nacional, e pelo menos 2 (dois) AS (Autonomous Systems) no Brasil;

6.1.10. A LICITADA deve possuir acesso ao backbone internacional, comprovados por meio de declaração de fornecedor, a pelo menos 2 (dois) AS (*Autonomous Systems*) no exterior;

6.1.11. Os equipamentos e a camada de ligação de dados (enlaces) disponibilizados pela LICITADA deverão apresentar certificação em conformidade com as normas e diretrizes estabelecidas através dos órgãos competentes ou entidades autônomas - ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações), e entidades de padrões reconhecidas internacionalmente – ITU-T (*International Telecommunication Union*), ISO (*International Standardization Organization*), IEEE (*Institute of Electrical and Electronics Engineers*), EIA/TIA (*Electronics Industry Alliance and Telecomumnication Industry Association*).

6.1.12. A tecnologia utilizada para tráfego de dados deverá ser implementada utilizando-se fibra óptica, ao longo de todo o circuito, com infraestrutura redundante tipo anel óptico;

6.1.13. O anel óptico redundante deve ser implementado de maneira tal que garanta total continuidade do serviço na indisponibilidade de uma das fibras ópticas (Ex.: Queda de poste, vandalismo, etc.);

6.1.14. Em caso de falha na fibra principal, o anel óptico redundante deverá assumir de imediato, sem perdas;

6.2. Os serviços apresentados pela empresa LICITADA, para o ITEM 5, deverá abranger os seguintes requisitos:

6.2.1. O profissional responsável pela gestão do projeto deverá ser certificado PMP e CISSP. A LICITADA deverá apresentar na fase de habilitação uma carta de intenção de contratação dos profissionais referidos e suas devidas certificações.

6.2.2. Deve apresentar 2 (DOIS) atestados de capacidade técnica de execução de serviços similares;

6.2.3. Carta dos fabricantes de hardware e software utilizadas para a prestação do serviço informando que é parceiro oficial e qualificado para dar suporte ou declaração do próprio licitante informando ser um parceiro oficial e qualificado do fabricante para dar suporte.

7. NÍVEIS DE SERVIÇO - ITENS 1, 2,3 e 4

7.1. Considerando que o período de indisponibilidade no ambiente de Tecnologia da Informação tem como preceito fundamental o tempo pelo qual os serviços que presumidamente estejam à disposição dos usuários e que não puderam ser acessados ou até mesmo não promoveram

um adequado resultado, faz-se necessário implementar um link de conectividade com a Internet com a maior disponibilidade possível.

7.2. O item Serviço de comunicação de dados entre a Prefeitura de Maceió e a Internet deverá possuir latência de no máximo, 60 MS (sessenta milissegundos). A latência será considerada como o tempo em que um pacote IP leva para ir de um ponto a outro da rede e retornar à origem. A latência será aferida pela LICITADA da seguinte forma:

7.2.1. Coletar amostras de latência a cada 05 (cinco) minutos;

7.2.2. Ao final de cada mês deverá verificar o percentual de pacotes acima do limite de latência, dentro desse período de apuração;

7.3. Para o item Serviço de Comunicação de Dados entre o ambiente da LICITADA e a Internet, as medições devem ser feitas entre o roteador responsável pelo serviço no ambiente da Prefeitura de Maceió e o primeiro roteador na Internet;

7.4. Os intervalos de tempo que o enlace apresentar aferições de latência superiores ao valor especificado serão considerados como períodos de indisponibilidade.

7.5. O Link de conectividade com a Internet deverá possuir perda de pacotes de no máximo 1% (um por cento), índice que será aferido pela CONTRATADA da seguinte forma:

7.5.1. A cada 5 (cinco) minutos deve ser medida a perda de pacotes;

7.5.2. Ao final de cada mês deverá ser verificado o percentual de pacotes perdidos dentro desse período de apuração;

7.5.3. As medições devem ser feitas entre o equipamento responsável pelo serviço no ambiente da Prefeitura de Maceió e o primeiro roteador na Internet;

7.5.4. Os intervalos de tempo que os enlaces apresentarem aferições do percentual de perda de pacotes superiores ao valor especificado, serão considerados como períodos de indisponibilidade;

7.5.5. Para o cálculo deste parâmetro serão considerados erros de interface, pacotes corrompidos pelo enlace, bem como descartes injustificados por parte do roteador;

7.5.6. Para o cálculo deste parâmetro não serão considerados pacotes descartados em função do esgotamento da capacidade do link entre o roteador instalado na Prefeitura de Maceió e a Internet, situações definidas quando a utilização for superior a 80% (oitenta por cento) da utilização da taxa CONTRATADA;

7.5.7. A solução deverá possuir disponibilidade de, no mínimo, 99,44% (noventa e nove vírgula quarenta e quatro por cento);

7.5.8. A disponibilidade do serviço corresponde ao percentual de tempo, durante o período de 1 (um) mês, em que o mesmo esteve em condições normais de funcionamento. Serão considerados como períodos de indisponibilidade o tempo em que o serviço estiver total ou parcialmente indisponível.

7.6. Não serão consideradas indisponibilidades as seguintes situações:

7.6.1. Paradas programadas pela CONTRATADA e aprovadas pela Prefeitura de Maceió. Neste caso a autorização deve ser solicitada pela Prefeitura de Maceió com, pelo menos, 5 (cinco) dias úteis de antecedência;

7.6.2. Paradas em função da falta de alimentação dos equipamentos instalados na sala de equipamentos servidores da Prefeitura de Maceió;

7.6.3. Paradas internas ocasionadas pela Prefeitura de Maceió, sem responsabilidade da CONTRATADA;

7.7. A CONTRATADA deverá disponibilizar à Prefeitura de Maceió um portal na Internet, para acompanhamento dos níveis de serviços prestados;

7.8. Entende-se por portal, ferramenta de gerência acessível pela Internet, por intermédio de um navegador Web, com acesso restrito através de usuário/senha eletrônica e utilizando-se de protocolo HTTPS;

7.9. O portal de acompanhamento dos serviços deverá possuir acesso aos históricos dos registros das ocorrências e registros de solicitações e reclamações enviadas pela Prefeitura de Maceió;

7.10. A análise técnica na qualidade de transmissão quanto a Taxa de Erros e Perda de Pacotes deverá ser realizada pela gerência da rede da CONTRATADA, com a auditoria da Diretoria de Tecnologia da Informação - DTI/SEMGE, sempre quando houver a necessária solicitação da CONTRATANTE, sem custos adicionais;

7.11. A gerência da rede da CONTRATADA deverá apurar, através de emissão de relatórios mensais, os tempos de falha do circuito dedicado, considerando as ocorrências desde a zero hora do primeiro dia do mês até as vinte e quatro horas do último dia do mês anterior ao da apuração e o valor apurado será ressarcido à CONTRATANTE na fatura dos serviços com vencimento no mês seguinte ao da apuração.

7.12. Considera-se início para efeito de contagem do prazo, o registro da chamada junto a Central de Atendimento (Telefônico, WEB, E-mail), disponibilizada pela CONTRATADA, até a comunicação da resolução definitiva com a análise técnica e aprovação realizadas pela Diretoria de Tecnologia da Informação - DTI da SEMGE, imprescindíveis para a autorização de fechamento do chamado.

7.13. A CONTRATADA deverá fornecer pelo menos 4 (quatro) usuário/senha para acesso ao portal de acompanhamento dos serviços de Internet e Segurança;

7.14. O portal de acompanhamento dos serviços deverá possibilitar que sejam visualizados e impressos os relatórios das informações de desempenho do link de conectividade;

7.15. Deverá ser fornecido, mensalmente, relatório contendo os registros das ocorrências no referido período;

7.16. A CONTRATADA deverá divulgar, no portal de acompanhamento dos serviços, relatórios detalhando os valores das medições dos parâmetros de qualidade do link de conectividade, conforme detalhamento deste Termo de Referência. Devem ser feitas medições a cada 5 (cinco) minutos. Para cada medição o relatório deve apresentar pelo menos os seguintes valores:

7.16.1. Dia e hora da medição;
7.16.2. Total de pacotes trafegados;
7.16.3. Total de pacotes com erros;
7.16.4. Latência;

7.17. A disponibilidade global do serviço IP (Internet Protocol), deverá ser calculada, para um período de 1 (um) mês, através da equação descrita na tabela 2:

Tabela 2: Equação que mede a disponibilidade global do serviço IP (período mensal)

D(%)= [(To - Ti)/To]*100, onde
D = Disponibilidade; To = Período de Operação (1 mês) em minutos. Para o cálculo do índice de disponibilidade, o "tempo total mensal" será calculado a partir do total de dias da prestação do serviço vezes 1440 (mil quatrocentos e quarenta) minutos; Ti (*Downtime*) = Somatório dos tempos de indisponibilidade do serviço observado durante o período de operação (1 mês), em minutos (excetuando-se as paradas internas sob responsabilidade da Prefeitura de Maceió)

7.18. Os serviços contratados serão considerados indisponíveis a partir do momento em que eventuais problemas forem detectados até o seu retorno às condições plenas de funcionamento;

7.19. A apuração e/ou contabilização das grandezas acima definidas, para efeito de aferição de resultados, dar-se-á mensalmente;

7.20. O período de indisponibilidade (Ti) será glosado proporcionalmente na fatura mensal em relação ao tempo total mensal de operação (To), conforme o seguinte cálculo:

$$G = [(100-D)/100] * VMF$$

Onde:

- VMF: Valor mensal da fatura;
- G: Valor Total da Glosa.
- D: Índice de Disponibilidade Mensal;

8. MANUTENÇÃO DE SERVIÇO E PRAZO DE ATENDIMENTO - ITENS 1, 2,3 e 4

8.1. A manutenção preventiva ou atualização dos recursos técnicos utilizados na prestação do serviço, quando necessárias interrupções programadas, deverá ser realizada através de comunicação escrita e prévia de no mínimo 7 (dias) dias úteis, a qual deverá ser agendada com a equipe técnica da CONTRATANTE e que será efetuada no período compreendido entre 00:01 e 06:00 horas, horário de Brasília, de domingo e/ou segunda-feira.

8.2. A CONTRATADA disponibilizará um número telefônico para abertura de chamados no regime 24x7x365. Ademais, a CONTRATADA deverá providenciar uma alternativa ao chamado telefônico para o registro do chamado através de sistema Web ou e-mail.

8.3. O suporte técnico deverá ser prestado à Prefeitura de Maceió, no endereço da Secretaria Municipal de Economia – Maceió/AL (Local de instalação do link de 1 Gbps) ou nas demais localidades de instalação dos links de menor velocidade;

8.4. O suporte técnico ocorrerá sem qualquer ônus para a Prefeitura de Maceió;

8.5. A Prefeitura de Maceió fará a abertura e acompanhamento de chamados técnicos por telefone 0800 e e-mail ou área em sítio da Web;

8.6. Para operacionalização do disposto anteriormente, a CONTRATADA deverá informar os números de telefone, endereços de correio eletrônico ou área em sítio da Web, disponíveis para a abertura e acompanhamento dos chamados técnicos;

8.7. O prazo de atendimento para resolução de possíveis indisponibilidades no uso dos serviços, deverá abranger três níveis de solução definitiva, quais sejam:

a) Severidade Alta: Esse nível de severidade é aplicado quando há a indisponibilidade total no uso dos serviços;

Solução Definitiva: ALTA

Indisponibilidade Total do Serviço:

Prazo Solução Definitiva: 2 (duas) horas

a.1. Entende-se indisponibilidade total, a prestação de serviços inaproveitáveis, conforme os seguintes parâmetros:

a.2. Perda do circuito contratado;

a.3. Latência do circuito contratado ultrapassar 80 MS (oitenta milissegundos);

b) Severidade Média: Esse nível de severidade é aplicado quando há falha, simultânea ou não, no uso dos serviços, estando ainda disponíveis, porém apresentando problemas;

Solução Definitiva: MÉDIA

Serviços disponíveis, mas apresentando conectividade intermitente:

Prazo Solução Definitiva: 4 (quatro) horas

b.1 Entende-se indisponibilidade, a prestação de serviço fora dos Níveis de Serviço, conformes os seguintes parâmetros:

b.2 Perda do circuito contratado entre 0,5% (zero vírgula cinco por cento) e 10% (dez por cento) de minutos de um dia;

b.3 Latência do circuito contratado de 50 MS (cinquenta milissegundos) até 80 MS (oitenta milissegundos)

c) Severidade Baixa: Esse nível de severidade é aplicado para problemas que não afetem o desempenho e disponibilidade dos serviços, bem como para atualizações de software e solicitações de alteração nas configurações dos roteadores e IPS.

Solução Definitiva: BAIXA

Serviços disponíveis e atualização:

Prazo Solução Definitiva: 4 (quatro) dias úteis

d) Prestação de Esclarecimentos Técnicos: é aplicado quando a CONTRATADA solicitar formalmente esclarecimentos técnicos relativos às ocorrências, ao uso e ao aprimoramento dos serviços.

Prazo de Resposta

Esclarecimentos técnicos:
Prazo Solução Definitiva: 4 (quatro) dias úteis

8.8. Será considerado como prazo de solução definitiva, o tempo decorrido entre a abertura do chamado técnico - efetuado por equipe técnica da Prefeitura de Maceió e a efetiva recolocação dos serviços em seu pleno estado de funcionamento;

8.9. A contagem do prazo de solução definitiva de cada chamado iniciar-se-á a partir da abertura do chamado, em um dos canais de atendimento disponibilizados pela CONTRATADA, até o momento da comunicação da resolução definitiva do problema e o aceite pela equipe técnica da Prefeitura de Maceió;

8.10. A glosa será contada a partir do tempo decorrido e identificado no item "Prazo Solução Definitiva" de acordo com a severidade prevista no item 14.

8.11. Depois de concluído o chamado, a CONTRATADA comunicará o fato à equipe técnica da Prefeitura de Maceió e solicitará autorização para o fechamento do mesmo. Caso a Prefeitura de Maceió não confirme que o problema foi de fato resolvido, o chamado permanecerá aberto até que seja efetivamente solucionado. Neste caso, a Prefeitura de Maceió fornecerá as pendências relativas ao chamado aberto;

8.12. A relação de chamados deverá estar disponível nos relatórios encaminhados mensalmente ao fiscal do contrato, atendendo aos seguintes tópicos:

8.12.1. Chamados Abertos no Período: listagem de todas as ocorrências registradas e ainda não solucionadas, durante o mês, com a indicação das ações já tomadas pela CONTRATADA;

8.12.2. Chamados Concluídos no Período: listagem de todas as ocorrências registradas e solucionadas, durante o mês, com a indicação das ações tomadas pela CONTRATADA.

8.13. O descumprimento dos prazos de atendimento implicarão a aplicação de glosas conforme tabela 3:

Tabela 3: Tabela de aplicação de Glosas

Resultado esperados e níveis de qualidade exigidos	Unidade de cálculo	Fórmula de cálculo da glosa	Limite da glosa
1 – Alta	1 h	NHAT * 0,50% * VMF	10% da VMF
2 – Média	1 h	NHAT * 0,25% * VMF	10% da VMF
3 – Baixo	1 h	NHAT * 0,05% * VMF	10% da VMF
4 – Esclarecimentos sobre incidentes	1 d	NDAT * 0,6% * VMF	10% da VMF

Onde:

VMF: Valor mensal da fatura;

NHAT: número de horas decorridas após o término de atendimento.

NDAT: número de dias decorridos após o término de atendimento.

8.14. A CONTRATADA deverá fornecer em meio eletrônico, documentação/formulário padronizado para cada circuito ativado, desativado ou para cada alteração ocorrida, contendo no mínimo, os seguintes dados:

8.14.1. Código de Identificação do Acesso;
8.14.2. Número do Contrato;
8.14.3. Endereço do Ponto de Acesso;
8.14.4. Velocidade de Acesso;
8.14.5. Data de solicitação do circuito;
8.14.6. Data de ativação/desativação/alteração do circuito;
8.14.7. Tipo/padrão de interface utilizada no circuito;
8.14.8. Meio de transmissão utilizado;
8.14.9. Valor da mensalidade.

9. NÍVEIS DE SERVIÇO - ITEM 5

9.1. ALOCAÇÃO DE SOLUÇÃO DE SEGURANÇA

9.1.1. Alocação de, no mínimo, 02 (dois) equipamentos (baseado em appliance), idênticos, com função de Next-Generation Firewall (NGFW), Statefull, implementando a solução de alta disponibilidade com tolerância a falhas (HA), podendo ser admitida a configuração ativo-passivo e ativo-ativo; Os equipamentos devem atender as funções e funcionalidades, no mínimo:

9.1.1.1. Controle de Aplicações
9.1.1.2. Proteção IPS
9.1.1.3. Proteção Antivírus , Atispyware e Antispam
9.1.1.4. Análise de Malwares Modernos
9.1.1.5. Filtro de URL
9.1.1.6. Controle de Transferência de Arquivos
9.1.1.7. Controle de Tráfego
9.1.1.8. De-criptografia SSL
9.1.1.9. Módulo VPN
9.1.1.10. Roteamento e NAT

9.2. CARACTERÍSTICAS DA DEMANDA, E CONFIGURAÇÕES MÍNIMAS DOS EQUIPAMENTOS:

9.2.1. O serviço deve incluir as substituições de equipamentos, sem ônus, caso se perceba limitação ou degradação da rede com base nos limites físicos (banda, portas, cabos), conforme demanda especificado neste Termo;
9.2.2. A solução appliance não irá permitir soluções instaladas e executadas em um sistema operacional regular, como Microsoft Windows, FreeBSD, SUN solaris, GNU/Linux, etc.
9.2.3. Garantir que não haja restrição por número de usuários que utilizem a solução disponibilizada;
9.2.4. O serviço deve incluir as substituições de equipamentos defeituosos fornecidos na composição da solução;
9.2.5. Os equipamentos devem ser instalados da Sede da DTI/SEMGE, em rack padrão de 19’’;
9.2.6. Incluir todas as licenças de software e de hardware necessárias ao perfeito e completo funcionamento das soluções ofertadas;
9.2.7. Disponibilizar um número de serviço, em língua portuguesa, para abertura de chamados técnicos. Este serviço deverá obrigatoriamente estar disponível 24x7;
9.2.8. Adicionalmente, o serviço deve prever que, ao término do contrato, todos os equipamentos e softwares deverão permanecer à disposição da contratante, sem custos a

contratante, por período de até seis meses, a critério da Contratante, para fins de migração da solução para um novo contrato, devendo, durante este período, atender e respeitar todas as cláusulas e regras deste Termo de Referência, bem como de seus anexos, contratos e adendos;

9.3. CARACTERÍSTICAS DA DEMANDA

9.3.1. Banda instalada de link da internet de 1 Gbps (um gigabit por segundo);
9.3.2. Previsão de crescimento para, no mínimo, o dobro (dois gigabits por segundo) em até-sessenta meses;
9.3.3. Para que o serviço não gere degradação da rede, recomenda-se que a solução instalada suporte, pelo menos, a taxa de transferência (throughput) de no mínimo 4 Gbps (quatro gigabits por segundo) de DPI total, com todos os recursos necessários, e recomendados pelo fabricante, habilitados (valor medido em sessões HTTP 64k), incluindo:

Especificação Mínima	**Valor**
Throughput de Firewall (Gbps)	4
Conexões simultâneas (milhões)	1,3
Novas conexões por segundo (mil)	30
Throughput de IPSec (Gbps)	2,5
Proteção combinada contra ameaças* (Mbps)	250
Quantidade mínima de interfaces (1 Gbps)	4
Políticas de Firewall (mil)	5

* Com funcionalidades habilitadas simultaneamente devidamente atuantes: controle de aplicação, IDS/IPS e controle de malware (antivírus, etc.) medidas com parâmetros de throughput considerando tráfego misto. Não serão aceitas medidas baseadas em condições ideais.

9.3.4. Todos os serviços web ofertados devem ser suportados por todos os navegadores web e sistemas operacionais disponíveis no mercado;

9.4. INSTALAÇÃO, CONFIGURAÇÃO E INTEGRAÇÃO

9.4.1. Executar todos dos serviços de instalação, configuração, integração e testes de funcionalidade, dentro do prazo máximo de 15 (quinze) dias corridos, a contar da data de aceite da solução;
9.4.2. Elaborar conjuntamente com a contratante o planejamento da implantação no ambiente da contratante;
9.4.3. Efetuar a instalação, configuração, integração e testes de funcionalidade dos equipamentos:

9.4.3.1. Instalação física do firewall no ponto de conexão com a Internet e as redes conectadas;

9.4.3.2. Deverão ser efetuadas de acordo com o plano de implantação, a ser elaborada em conjunto com a contratante visando obter o melhor uso dos equipamentos;

9.4.3.3. Realizar, com os técnicos da contratante, testes de funcionalidade para constatar que os equipamentos foram instalados, configurados e integrados de acordo com os requisitos técnicos e parâmetros de configuração solicitados;

9.4.3.4. Elaborar uma documentação técnica, contendo todas as configurações efetuadas e as descrições das características e recursos utilizados;

9.4.4. Colocar à disposição da contratante, analistas técnicos especializados para a execução das soluções a serem implantadas em sua rede corporativa durante o tempo de funcionamento da solução, estes técnicos deverão ser devidamente certificados pelo fabricante da solução, e a certificação não pode estar vencida durante o período o período do contrato:

9.4.5. Configuração do firewall com as políticas de acesso e estrutura de segurança:

9.4.5.1. Integração com o diretório de usuários corporativos (AD)/LDAP;

9.4.5.2. Configuração do controle de aplicações;

9.4.5.3. Configuração das VLAN;

9.4.5.4. Configuração do Filtro de conteúdo WEB;

9.4.5.5. Configuração do anti-malware de gateway;

9.4.5.6. Solução Anti Spam;

9.4.5.7. Configuração do IPS;

9.4.5.8. Configuração dos parâmetros de QoS que serão fornecidos pela equipe técnica da contratante;

9.4.5.9. Configuração dos clientes de VPN;

9.4.5.10. Testes e monitoração;

9.5. CONFIGURAÇÕES MÍNIMAS DOS EQUIPAMENTOS

9.5.1. Não deve haver degradação de performance de inspeção de firewall e de controle de aplicação, abaixo dos valores físicos da rede (banda do link e throughput das portas), quando funções de IPS, Antivírus e Antispyware forem habilitadas simultaneamente;

9.5.2. O equipamento não deve ser fator limitante para o tráfego da rede;

9.5.3. Fazer uso de appliance específico para o propósito solicitado;

9.5.4. Fonte de alimentação com operação automática entre 110/220V;

9.5.5. Possuir no mínimo 04 (quatro) interfaces 10/100/1000Base-TX autosense, operando em full duplex, com inversão automática de polaridade configuráveis pelo administrador da solução.

9.5.6. Possuir 02 (duas) interfaces de 10 Gbps (SFP+);

9.5.7. Suportar funcionamento em:

9.5.7.1. Tap (via porta espelhada, Tap ou SPAN port);

9.5.7.2. Transparente (Bridge ou similar);

9.5.7.3. Layer2;

9.5.7.4. Layer3;

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

9.5.9. Suportar controle de aplicações IPv6 em todas os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3);

9.5.10. Prover otimização para análise de conteúdo de aplicações na camada 7 do modelo OSI;

9.5.11. Possuir proteção anti-spoofing;

9.5.12. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados de rede;

9.5.13. Suportar os seguintes tipos de NAT:

9.5.13.1. Porta/IP Nat dinâmico (Many-to-1 e Many-to-Many);
9.5.13.2. Nat dinâmico (Many-to-Many);
9.5.13.3. Nat estático (1-to-1, Many-to-Many, Ips);
9.5.13.4. Nat estático bidirecional 1-to-1;
9.5.13.5. Tradução de porta (PAT);
9.5.13.6. NAT de Origem;
9.5.13.7. NAT de Destino;
9.5.13.8. Suportar NAT de Origem e NAT de Destino, individualmente e simultaneamente;

9.5.14. A solução deve sincronizar:

9.5.14.1. Todas as sessões;
9.5.14.2. Certificados decriptogafados;
9.5.14.3. Todas associações de segurança das VPN;
9.5.14.4. Todas as assinaturas de Antivírus, Antispyware e Aplicações;
9.5.14.5. Todas as configurações;
9.5.14.6. Tabelas FIB;

9.5.15. Possuir algoritmos de análise de comportamento e perfil do tráfego, detectando ações estranhas ao comportamento normal prevenindo as ações de invasão da rede;

9.5.16. Compatibilidade e integração, em todos os seus módulos, com o Microsoft Active Directory (AD) e LDAP, para fins de identificação e controle de acessos individualizados por usuário ou por grupo de usuários;

9.5.17. Capacidade de operar, de forma simultânea, mediante o uso das suas interfaces físicas nos seguintes modos:

9.5.17.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
9.5.17.2. Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
9.5.17.3. Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
9.5.17.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
9.5.17.5. Redes Virtuais, vLans 802.1q, 802.3ad link aggregation;

9.5.18. Tradução de endereços da rede (NAT) por origem e destino, por endereços IP dinâmicos e pool de portas;

9.5.19. Suportar Jumbo Frames, BGP, OSPF e RIP2, DHCP Server e DHCP Relay;

9.5.20. Suportar protocolos de encriptação IKE, AES (com criptografia de 128 e

9.5.21. 256 bits), 3Des, SHA1 e MD5;

9.5.22. Suportar os protocolos de VoIP: H.323, SIP, SCCP e MGCP;

9.5.23. Em caso de protocolos e aplicações desconhecidos, poderão designar-se assinaturas próprias;

9.5.24. Detecção de aplicações dinâmicas dentro de sessões de proxy HTTP;

9.5.25. Controle de tráfego IPv4 e IPv6, ambos incluem, visibilidade e inspeção de ameaças em aplicações e controle de conteúdo. O IPv6 deve ser suportado em interfaces trabalhando em L2 e L3;

9.5.26. Suporte a objetos e regras IPv6 e Multicast;

9.5.27. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 (aplicação);

9.5.28. Suportar a atribuição de agendamento das políticas, com o objetivo de habilitar e desabilitar políticas em horários predefinidos automaticamente;

9.5.29. Suporte a identificação de usuários em ambiente virtualizado (Citrix, Microsoft Terminal Server, etc.), permitindo visibilidade e controle granular por usuário;

9.5.30. Suportar e realizar a sincronização dos equipamentos da solução via protocolo NTP;

9.5.31. Atualização de assinaturas:

9.5.31.1. Sob demanda (diária, semanal e de emergência);

9.5.31.2. Suportar atualização automática das assinaturas através de conexão segura;

9.5.31.3. Não devem depender de reboot do equipamento para efetivação;

9.5.31.4. Todos os equipamentos devem utilizar as mesmas assinaturas;

9.6. CONTROLE DE APLICAÇÕES

9.6.1. Deverá contar com ferramentas de visibilidade e controle que permitam administrar o tráfego de aplicações, permitindo o tráfego de aplicações autorizadas e bloqueio de aplicações não autorizadas;

9.6.2. Controle de políticas por porta, protocolo, aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações, individualizado ou agrupado por usuários, grupos de usuários, IP, Redes;

9.6.3. Reconhecer no mínimo 2100 aplicações diferentes;

9.6.4. Suportar controle de políticas baseada em geolocalização (países);

9.6.5. Capacidade de identificar as aplicações, independente das portas e protocolos, assim como técnicas de evasão utilizadas;

9.6.6. Incluir a capacidade de atualização para identificar novas aplicações;

9.6.7. Atualizar a base de assinaturas de aplicações automaticamente;

9.6.8. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas do fabricante;

9.6.9. Alertar o usuário quando uma aplicação foi bloqueada;

9.6.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;

9.6.11. Possibilitar a diferenciação de aplicações Proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;

9.6.12. Possibilitar a diferenciação de aplicações que realizem o uso de táticas evasivas (deep web, rede tor);

9.6.13. Possibilitar a diferenciação e bloqueio de tráfegos P2P (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;

9.6.14. Possibilitar a diferenciação e bloqueio de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, Whatsapp, etc.) possuindo granularidade de controle/políticas para os mesmos;

9.6.15. Possibilitar a diferenciação e controle de partes das aplicações, como, por exemplo, permitir o Gtalk, mas bloquear a transferência de arquivos por ele;

9.6.16. 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);

9.6.17. Capacidade de criação de políticas baseadas no controle por aplicação:

9.6.17.1. Por tecnologia: cliente-servidor, Browse Based, Network Protocol, etc.;

9.6.17.2. Por nível de risco da aplicação;

9.6.17.3. Por categoria e subcategoria de aplicações;

9.6.18. Baseadas em “traffic shaping” por aplicação, usuário, origem, destino, túnel VPN-IPSEC-SSL;

9.7. PROTEÇÃO IPS

9.7.1. Dispor de IPS integrado a solução de segurança;
9.7.2. Permitir o bloqueio de vulnerabilidades;
9.7.3. Permitir o bloqueio de exploits conhecidos;
9.7.4. Proteção contra ataques de negação de serviços (DoS);
9.7.5. Deverá possuir os seguintes mecanismos de inspeção de IPS:

9.7.5.1. Análise de padrões de estado de conexões;
9.7.5.2. Análise de decodificação de protocolo;
9.7.5.3. Análise para detecção de anomalias de protocolo;
9.7.5.4. Análise heurística;
9.7.5.5. IP Defragmentation;
9.7.5.6. Remontagem de pacotes de TCP;
9.7.5.7. Bloqueio de pacotes malformados;

9.7.6. Possuir assinaturas para bloqueio de ataques "buffer overflow";
9.7.7. Possuir assinaturas para auxílio no bloqueio de ataques distribuídos de negação de serviço (DDoS);
9.7.8. Possuir assinaturas e mecanismos de detecção de anomalias prontas;
9.7.9. Suportar o reconhecimento de ataques em tráfego IPv6;
9.7.10. Possibilitar a criação de assinaturas customizadas;
9.7.11. Possibilitar a criação de exceções/exclusões por hosts para determinadas assinaturas;
9.7.12. Suportar referência cruzada com CVE (Common Vulnerabilities and Exposures);
9.7.13. Possuir granularidade de ajustes com opções para sobrescrever assinaturas individualmente;
9.7.14. Suportar várias técnicas de prevenção, incluindo Drop e TCP-RST (Cliente, Servidor e ambos);
9.7.15. Suportar ações por assinaturas;
9.7.16. Suportar notificações e alertas via e-mail, whatsapp, SNMP traps e log de pacotes;
9.7.17. Suportar a captura de pacotes (PCAP) para fins de forense;
9.7.18. Análise dinâmica de ameaças do ambiente móvel e APK;
9.7.19. Não deve possuir recursos que delimitem a quantidade de bytes da sessão que será inspecionada;
9.7.20. Suportar atualização de assinaturas de ataque;
9.7.21. Possuir mecanismos que permita bloquear um ataque por expressão regular DNS;
9.7.22. Possuir autenticação em query DNS por requisição em TCP;
9.7.23. Prevenir que hosts validos sejam adicionados a blacklists por engano;
9.7.24. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing), ou garantir que esta exigência seja plenamente atendida por meio diverso;

9.8. PROTEÇÃO ANTIVÍRUS E ANTISPYWARE

9.8.1. Incluir módulo de Antivírus e Antispyware integrado na solução de segurança;
9.8.2. Permitir o bloqueio de Malwares e Spywares;
9.8.3. Capacidade de inspeção Antivírus, pelo menos, para os seguintes tipos de tráfegos: HTTP, SMTP, IMAP,POP3 e FTP;
9.8.4. Incluir proteção contra vírus em conteúdo HTML e javascript,software espião (spyware) e worms;
9.8.5. Proteção contra downloads involuntários, usando HTTP, de arquivos executáveis maliciosos;
9.8.6. Rastreamento de vírus em arquivos PDF
9.8.7. Permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, rar, etc.);
9.8.8. Suportar bloqueio de arquivos por tipo;
9.8.9. Suportar notificações e alertas via e-mail, whatsap, SNMP traps e log de pacotes;
9.8.10. Suportar a captura de pacotes (PCAP) para fins de forense;

9.9. PROTEÇÃO ANTISPAM

9.9.1. Deve ter a capacidade de permitir ou não endereços de e-mail com caracteres especiais, para no mínimo percentagem (%), hífen (-) e caracteres 8-bit
9.9.2. Deve ter a capacidade de rejeitar conexões que tentem serem abertas pelos comandos “HELO” e “EHLO”, sem que existam gravados seus endereços de “MX” e “A” nos servidores de DNS;
9.9.3. Deve ter a capacidade de fazer filtragem do remetente a partir de uma correlação da reputação global, informada pelo fabricante do produto, em conjunto com a reputação local, restringindo conexões indesejadas;
9.9.4. Deve ter a capacidade de implementar pesquisas de reputação, a partir da console do produto, informando seu histórico de reputação, assim como, sua reputação atual;
9.9.5. Deve ter a capacidade de arquivar qualquer mensagem que viole as políticas corporativas, enviando-as para a estrutura de arquivamento do órgão;
9.9.6. Deve ser capaz de processar o tráfego de mensagens de entrada e de saída, com políticas diferenciadas para cada sentido de tráfego;
9.9.7. Deve permitir a execução de múltiplas ações para uma mesma mensagem que for categorizada como SPAM ou violação dos filtros de conteúdo, entre elas:

9.9.7.1. Apagar mensagem;
9.9.7.2. Enviar para Quarentena;
9.9.7.3. Encaminhar mensagens;
9.9.7.4. Encaminhar em BCC;
9.9.7.5. Gravar mensagem em disco;
9.9.7.6. Gravar em pasta de conformidade;
9.9.7.7. Modificar o assunto;
9.9.7.8. Adicionar informações ao cabeçalho;
9.9.7.9. Deferir a mensagem;
9.9.7.10. Rejeitar a mensagem;

9.9.8. Deve ser capaz de quando a mensagem for gravada em pasta de conformidade,
9.9.9. permitir definir ações distintas para as mensagens aprovadas e reprovadas;
9.9.10. Deve possuir capacidade de notificar remetente, destinatário, administrador e outros e-mails, simultaneamente;

9.9.11. Deve ter precisão de identificação de spam de pelo menos 95% (spam-catching rate);
9.9.12. Deve ter precisão de filtragem de pelo menos 99,9999% (accuracy rate);
9.9.13. Deve permitir atualização automática dos filtros a cada 10 minutos, sem interrupção dos serviços;
9.9.14. Deve ter suporte a listas negras e listas brancas com opção por domínio, endereço de e-mail e endereço IP;
9.9.15. Deve ter a capacidade de bloquear mensagens consideradas como SPAM baseado na utilização de listas DNSBL (DNS BlackHole) ou RBL (Real Time Black List);
9.9.16. Deve ter capacidade de utilização de pelo menos as seguintes tecnologias de detecção de spam:

9.9.16.1. Assinaturas para corpo da mensagem e anexos;
9.9.16.2. Análise heurística, através de análise de cabeçalhos, conteúdo e estrutura da mensagem;

9.9.17. Filtros de reputação local (criado automaticamente através da análise das mensagens recebidas) e global (criado pela rede de monitoramente do fornecedor da solução):

9.9.17.1. Identificação de idiomas;
9.9.17.2. Filtros de URLs;
9.9.17.3. Filtros anti-phishing;
9.9.17.4. Deve possuir capacidade para criação de filtros baseados no cabeçalho, remetente, tipos e conteúdo de anexos, dicionários de palavras, assunto e corpo da mensagem, incluindo o uso de expressões regulares;
9.9.17.5. Deve possuir recurso para a detecção de ataques, que penalize dinamicamente a origem baseado no nível de reputação, com dez níveis de sensibilidade;
9.9.17.6. Deve possuir a cada nível da detecção dos ataques, citados no item anterior, o controle do percentual de mensagens que serão recusadas;
9.9.17.7. Deve possuir a cada nível da detecção dos ataques, citados, o tempo limite para nova tentativa de conexão, número de conexões por IP e número de mensagens por conexão;
9.9.17.8. Deve possuir tecnologia para prevenção de ataques de “Bounce Messages”;
9.9.17.9. Deve possuir a capacidade de implementar Sender Policy Framework (SPF) e SenderID;
9.9.17.10. Deve possuir a capacidade para criação de regras baseada no tipo de arquivo anexado;
9.9.17.11. Deve possuir a capacidade para criação de regras baseada na detecção por “Wildcard”;
9.9.17.12. Deve possuir a capacidade para criação de regras baseada na detecção por expressões regulares;
9.9.17.13. Deve possuir a capacidade de implementar comunicação segura via TLS (Transport Layer Security);
9.9.17.14. Deve possuir capacidade de configurar criptografia TLS por domínio e por política;
9.9.17.15. Deve ter capacidade de detecção a pelo menos 10 idiomas (incluindo Português), permitindo o bloqueio de mensagens escritas nos idiomas não desejados;
9.9.17.16. Deve possuir capacidade de criar uma lista de IP´s confiáveis baseado no Comportamento do IP originário da mensagem, visando minimizar o impacto de performance em grandes ambientes;
9.9.17.17. Deve possuir a capacidade de atualização automática periódica da lista de IP’s confiáveis, citada no item anterior;

9.9.17.18. Deve permitir bloquear anexos pela extensão, pelo tipo real do arquivo, nome, tamanho, e número de anexos;

9.9.17.19. Deve permitir a verificação em arquivos compactados nos formatos mais utilizados em até 20 níveis de compactação;

9.10. ANÁLISE DE MALWARES MODERNOS

9.10.1. Solução ofertada deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria solução de segurança;

9.10.2. 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;

9.10.3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a escopo de proteção, tais como endereço de destino, podendo aplicar regras de exceção por assinaturas, endereço IP e/ou site;

9.10.4. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Microsoft Windows XP e versões mais novas;

9.10.5. Deve suportar a monitoração de arquivos trafegados na internet (HTTPS, HTTP, SMTP, FTP, IMAP, POP3) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

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

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

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

9.10.9. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

9.10.10. A solução deve ser fornecida em appliance local, deve possuindo, no mínimo, 28 ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;

9.10.11. Caso seja necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

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

9.11. FILTRO DE URL

9.11.1. Incluir módulo de filtro de URL integrado a solução de segurança;

9.11.2. Possibilitar a configuração de políticas de filtro de URL baseado em políticas do firewall, individualizado ou agrupado por usuários, grupos de usuários, IP, redes ou zonas de segurança;

9.11.3. Incluir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

9.11.4. Possibilitar base de URL local no appliance, evitando atrasos (delay) de comunicação/validação da URL;

9.11.5. Possuir, pelo menos, 50 categorias de URL;
9.11.6. Possibilitar a criação Categorias de URL customizadas;
9.11.7. Possibilitar a exclusão de URL do bloqueio por categoria;
9.11.8. Possibilitar a customização de página de bloqueio;

9.12. CONTROLE DE TRANSFERÊNCIA DE ARQUIVOS

9.12.1. Possibilitar a criação de filtros para arquivos e dados predefinidos;
9.12.2. Os arquivos devem ser identificados por extensão e assinaturas;
9.12.3. Capacidade de identificar e prevenir a transferência de arquivos por tipo (ex.: doc, ppt, exe, pdf, bat, dll, ocx), mesmo dentro de aplicações (ex.: P2P, IM, SMB, POP3, IMAP);
9.12.4. Possibilitar a identificação de arquivos compactados em até 20 níveis de compactação e as aplicações de políticas sobre o conteúdo desses tipos de arquivos;
9.12.5. Capacidade de identificar e prevenir a transferência de informações sensíveis (ex.: número de cartão de crédito) possibilitando a criação de novos tipos de dados via expressão regular;

9.13. CONTROLE DE TRÁFEGO

9.13.1. Permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.
9.13.2. Controle de políticas QoS por porta, aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações, endereço de origem e de destino, individualizado ou agrupado por usuários, grupos de usuários e IP;
9.13.3. Traffic shaping QoS baseado em políticas (prioridade, garantia e máximo);
9.13.4. Com a finalidade de controlar aplicações e trafego cujo consumo possa ser excessivo, (como youtube, upstream, 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, deva 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.
9.13.5. O QoS deve possibilitar a definição de classes por:

9.13.5.1. Banda Garantida;
9.13.5.2. Banda Máxima;
9.13.5.3. Fila de Prioridade;

9.13.6. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
9.13.7. Suportar marcação de pacotes Diffserv;
9.13.8. Disponibilizar estatísticas em tempo real para classes de QoS;
9.13.9. Permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.
9.13.10. Possibilitar a visualização dos países de origem e destino nos logs dos acessos;

9.14. CRIPTOGRAFIA SSL/TLS

9.14.1. Identificar, de-criptografar e analisar o trafego SSL em conexões de saída (Outbound) e em conexões de entrada (Inbound);

9.14.2. Controle de políticas e exceções para de-criptografia SSL por categoria de URL, endereço de origem e de destino, individualizado ou agrupado por usuários, grupos de usuários, IP ou por zonas de segurança;
9.14.3. Diferenciar conexões pessoais (bancos, shopping, etc.) e tráfegos não pessoais usando categorias de URL na regra de de-criptografia;
9.14.4. Simplicidade na criação das políticas usando uma tabela de regras similar as regras de firewall;
9.14.5. Possibilitar a identificação de usuários sem a necessidade de instalação de agente individualmente em cada equipamento da rede;

9.15. GERAÇÃO DE LOGS

9.15.1. Os logs do produto devem incluir informações das atividades dos usuários;
9.15.2. Popular todos os logs de tráfego, IPS, URL, Data, Aplicações entre outros com as informações dos usuários;
9.15.3. Os logs de identificação de usuários devem ser feitos em tempo real (e não correlacionado após a ocorrência do tráfego em questão);
9.15.4. Deve suportar protocolo syslog, enviando as informações para um servidor syslog remoto a solução;
9.15.5. Enviar os logs para uma solução de centralização de logs da CONTRATANTE, e manter por 365 dias com acesso online, até o fim do contrato, em solução de backup.

9.16. MÓDULO VPN:

9.16.1. Suportar VPN Site-to-Site e Cliente-To-Site;
9.16.2. Suportar IPSec VPN;
9.16.3. Suportar SSL VPN;
9.16.4. Suportar atribuição de IP nos clientes remotos de VPN;
9.16.5. Suportar atribuição de DNS nos clientes remotos de VPN;

9.17. IPSEC VPN DEVE SUPORTAR:

9.17.1. 3DES, AES;
9.17.2. Autenticação MD5 e SHA-1;
9.17.3. Diffie-Hellman Group 1, Group 2 e Group 5;
9.17.4. Algoritimo Internet Key Exchange (IKE); e. AES 128, 256 (Advanced Encryption Standard);
9.17.5. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
9.17.6. Dispor de software cliente de VPN-SSL para os sistemas operacionais Windows (XP e mais novos), Linux e MacOS;
9.17.7. Permitir criar políticas para tráfego VPN-SSL;
9.17.8. SSL VPN com suporte a proxy ARP;
9.17.9. Suportar, pelo menos, 200 (duzentos) usuários simultâneos via SSL VPN; 1
9.17.10. Suporte para autenticação de VPN SSL, Ldap, Secure ID e base de dados própria;
9.17.11. Possuir interoperabilidade com, no mínimo, os seguintes fabricantes: Cisco, CheckPoint, Juniper, Palo Alto, Fortinet, SonicWall;

9.18. ROTEAMENTO E NAT

9.18.1. Suportar as seguintes funcionalidades de roteamento:

9.18.1.1. Estático e Dinâmico;
9.18.1.2. RIP v2;
9.18.1.3. OSPF;
9.18.1.4. BGP v4;

9.18.2. Suporte a roteamento IPv6;
9.18.3. Controle de políticas de redirecionamento por porta, aplicação, endereço de origem e de destino, individualizado ou agrupado por usuários, grupos de usuários e IP;

9.19. GERENCIAMENTO

9.19.1. Possuir interface "Out-Of-Band" dedicada para gerenciamento;

9.19.1.1. SSH;
9.19.1.2. HTTPS;

9.19.2. Monitoração de falha de link;
9.19.3. Suportar o gerenciamento por:

9.19.3.1. CLI via SSH;
9.19.3.2. WebUI via HTTPS;
9.19.3.3. Console;

9.19.4. O gerenciamento local do equipamento deve permitir:

9.19.4.1. Criação e administração de políticas;
9.19.4.2. Administração de políticas de IPS, Antivírus e Antispyware;
9.19.4.3. Política de Filtro de Dados e Filtro de URL;
9.19.4.4. Monitoração de logs;
9.19.4.5. Ferramentas de investigação de logs;
9.19.4.6. Debugging;
9.19.4.7. Captura de pacotes;

9.19.5. Possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;
9.19.6. Possibilidade de acessar o equipamento e aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;
9.19.7. Possibilitar gerenciamento do equipamento via protocolos SNMP, SNMP-V2 e SNMP-V3

9.20. ADMINISTRAÇÃO DO EQUIPAMENTO

9.20.1. Possibilitar a criação de diferentes profiles de administração separando, pelo menos: Leitura, Alterações, Relatórios e Monitoração;
9.20.2. Deverá ser possível de forma granular, assinar permissões para os administradores criarem outros usuários, alterarem configurações, ler configurações, etc.
9.20.3. Possibilidade de administrar o firewall localmente ou remotamente, sem causar problemas de sincronismo de configurações;
9.20.4. Habilidade de upgrade via SCP e Web-UI;

9.20.5. Suportar rollback de configuração para a última configuração salva;
9.20.6. Suportar rollback de Sistema Operacional para a última versão local;
9.20.7. Validação de regras antes da aplicação;
9.20.8. Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores, quando houver mais de um administrador executando alterações simultaneamente;
9.20.9. Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
9.20.10. Possibilitar a integração com outras soluções de SIEM de mercado ("third-party SIEM vendors");

9.21. RELATÓRIOS

Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos gateways de segurança em tempo real;
9.21.1. Possuir relatórios de utilização dos recursos por aplicações,URL, Ameaças, etc.;
9.21.2. Prover uma visualização sumarizada de todas as aplicações, ameaças e URL que passaram pela solução em tempo real;
9.21.3. Possibilidade de identificar o usuário que fez determinado acesso;
9.21.4. Possibilidade de exportar os logs CSV;
9.21.5. Possibilidade de capturar as URL acessadas para todas as sessões HTTP;
9.21.6. Gerar alertas automáticos via:

9.21.6.1. E-mail;
9.21.6.2. SNMP;
9.21.6.3. WhatsApp.

10. NÍVEIS DE SERVIÇO - ITEM 6

10.1. ALOCAÇÃO DE SOLUÇÃO DE SEGURANÇA

10.1.1. Alocação de, no mínimo, 02 (dois) equipamentos (baseado em appliance), idênticos, com função de Next-Generation Firewall (NGFW), Statefull, implementando a solução de alta disponibilidade com tolerância a falhas (HA), podendo ser admitida a configuração ativo-passivo e ativo-ativo; os equipamentos devem atender as funções e funcionalidades, no mínimo:

10.1.1.1. Controle de Aplicações
10.1.1.2. Proteção IPS
10.1.1.3. Proteção Antivírus, Antispyware
10.1.1.4. Análise de Malwares Modernos
10.1.1.5. Filtro de URL
10.1.1.6. Controle de Transferência de Arquivos
10.1.1.7. Controle de Tráfego
10.1.1.8. Módulo VPN
10.1.1.9. Roteamento e NAT

10.2. CARACTERÍSTICAS DA DEMANDA, E CONFIGURAÇÕES MÍNIMAS DOS EQUIPAMENTOS:

10.2.1. O serviço deve incluir as substituições de equipamentos, sem ônus, caso se perceba limitação ou degradação da rede com base nos limites físicos (banda, portas, cabos), conforme demanda especificado neste Termo;

10.2.2. O serviço deve incluir as substituições de equipamentos defeituosos fornecidos na composição da solução;

10.2.3. A solução appliance não irá permitir soluções instaladas e executadas em um sistema operacional regular, como Microsoft Windows, FreeBSD, SUN solaris, GNU/Linux, etc.

10.2.4. Garantir que não haja restrição por número de usuários que utilizem a solução disponibilizada;

10.2.5. Os equipamentos devem ser instalados no endereço indicado pela Contratante, em rack padrão de 19'';

10.2.6. Incluir todas as licenças de software e de hardware necessárias ao perfeito e completo funcionamento das soluções ofertadas;

10.2.7. Disponibilizar um número de serviço, em língua portuguesa, para abertura de chamados técnicos. Este serviço deverá obrigatoriamente estar disponível 24x7;

10.2.8. Adicionalmente, o serviço deve prever que, ao término do contrato, todos os equipamentos e softwares deverão permanecer à disposição da contratante, sem custos a contratante, por período de até seis meses, a critério da Contratante, para fins de migração da solução para um novo contrato, devendo, durante este período, atender e respeitar todas as cláusulas e regras deste Termo de Referência, bem como de seus anexos, contratos e adendos;

10.3. CARACTERÍSTICAS DA DEMANDA

10.3.1. Banda instalada de link da internet de 300 Mbps (trezentos megabits por segundo);

10.3.2. Previsão de crescimento para, no mínimo, o dobro (seiscentos megabits por segundo) em até sessenta meses;

10.3.3. Para que o serviço não gere degradação da rede, recomenda-se que a solução instalada suporte, pelo menos, a taxa de transferência (throughput) de no mínimo 300 Mbps (trezentos megabits por segundo) de DPI total, com todos os recursos necessários, e recomendados pelo fabricante, habilitados (valor medido em sessões HTTP 64k), incluindo:

Especificação Mínima	**Valor**
Throughput de Firewall (Gbps)	0,95
Conexões simultâneas (milhões)	0,9
Novas conexões por segundo (mil)	15
Throughput de IPSec (Gbps)	0,7
Proteção combinada contra ameaças* (Mbps)	150
Quantidade mínima de interfaces (1 Gbps)	2
Políticas de Firewall (mil)	5

* Com funcionalidades habilitadas simultaneamente devidamente atuantes: controle de aplicação, IDS/IPS e controle de malware (antivírus, etc.) medidas

com parâmetros de throughput considerando tráfego misto. Não serão aceitas medidas baseadas em condições ideais.

10.3.4. Todos os serviços web ofertados devem ser suportados por todos os navegadores web e sistemas operacionais disponíveis no mercado;

10.4. INSTALAÇÃO, CONFIGURAÇÃO E INTEGRAÇÃO

10.4.1. Executar todos dos serviços de instalação, configuração, integração e testes de funcionalidade, dentro do prazo máximo de 15 (quinze) dias corridos, a contar da data de aceite da solução;

10.4.2. Elaborar conjuntamente com a contratante o planejamento da implantação no ambiente da contratante;

10.4.3. Efetuar a instalação, configuração, integração e testes de funcionalidade dos equipamentos:

10.4.3.1. Instalação física do firewall no ponto de conexão com a Internet e as redes conectadas;

10.4.3.2. Deverão ser efetuadas de acordo com o plano de implantação, a ser elaborada em conjunto com a contratante visando obter o melhor uso dos equipamentos;

10.4.3.3. Realizar, com os técnicos da contratante, testes de funcionalidade para constatar que os equipamentos foram instalados, configurados e integrados de acordo com os requisitos técnicos e parâmetros de configuração solicitados;

10.4.3.4. Elaborar uma documentação técnica, contendo todas as configurações efetuadas e as descrições das características e recursos utilizados;

10.4.4. Colocar à disposição da contratante, analistas técnicos especializados para a execução das soluções a serem implantadas em sua rede corporativa durante o tempo de funcionamento da solução, estes técnicos deverão ser devidamente certificados pelo fabricante da solução, e a certificação não pode estar vencida durante o período o período do contrato:

10.4.5. Configuração do firewall com as políticas de acesso e estrutura de segurança:

10.4.5.1. Integração com o diretório de usuários corporativos (AD) /LDAP;

10.4.5.2. Configuração do controle de aplicações;

10.4.5.3. Configuração das VLAN;

10.4.5.4. Configuração do Filtro de conteúdo WEB;

10.4.5.5. Configuração do anti-malware de gateway;

10.4.5.6. Configuração do IPS;

10.4.5.7. Configuração dos parâmetros de QoS que serão fornecidos pela equipe técnica da contratante;

10.4.5.8. Configuração dos clientes de VPN;

10.4.5.9. Testes e monitoração;

10.5. CONFIGURAÇÕES MÍNIMAS DOS EQUIPAMENTOS

10.5.1. Não deve haver degradação de performance de inspeção de firewall e de controle de aplicação, abaixo dos valores físicos da rede (banda do link e throughput das portas), quando funções de IPS, Antivírus e Antispyware forem habilitadas simultaneamente;

10.5.2. O equipamento não deve ser fator limitante para o tráfego da rede;

10.5.3. Fazer uso de appliance específico para o propósito solicitado;

10.5.4. Fonte de alimentação com operação automática entre 110/220V;

10.5.5. Possuir no mínimo 2 (duas) interfaces 10/100/1000Base-TX autosense, operando em full duplex, com inversão automática de polaridade configuráveis pelo administrador da solução.

10.5.6. Prover otimização para análise de conteúdo de aplicações na camada 7 do modelo OSI;

10.5.7. Possuir proteção anti-spoofing;

10.5.8. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados de rede;

10.5.9. Possuir 02 (duas) interfaces de 1 Gbps (SFP+);

10.5.10. Suportar funcionamento em:

10.5.10.1. Tap (via porta espelhada, Tap ou SPAN port);

10.5.10.2. Transparente (Bridge ou similar);

10.5.10.3. Layer2;

10.5.10.4. Layer3;

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

10.5.12. Suportar controle de aplicações IPv6 em todas os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3);

10.5.13. Suportar os seguintes tipos de NAT:

10.5.13.1. Porta/IP Nat dinâmico (Many-to-1 e Many-to-Many);

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

10.5.13.3. Nat estático (1-to-1, Many-to-Many, Ips);

10.5.13.4. Nat estático bidirecional 1-to-1;

10.5.13.5. Tradução de porta (PAT);

10.5.13.6. NAT de Origem;

10.5.13.7. NAT de Destino;

10.5.13.8. Suportar NAT de Origem e NAT de Destino, individualmente e simultaneamente;

10.5.14. A solução deve sincronizar:

10.5.14.1. Todas as sessões;

10.5.14.2. Certificados decriptogafados;

10.5.14.3. Todas associações de segurança das VPN;

10.5.14.4. Todas as assinaturas de Antivírus, Antispyware e Aplicações;

10.5.14.5. Todas as configurações;

10.5.14.6. Tabelas FIB;

10.5.15. Possuir algoritmos de análise de comportamento e perfil do tráfego, detectando ações estranhas ao comportamento normal prevenindo as ações de invasão da rede;

10.5.16. Compatibilidade e integração, em todos os seus módulos, com o Microsoft Active Directory (AD) e LDAP, para fins de identificação e controle de acessos individualizados por usuário ou por grupo de usuários;

10.5.17. Capacidade de operar, de forma simultânea, mediante o uso das suas interfaces físicas nos seguintes modos:

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

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

10.5.17.3. Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

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

10.5.17.5. Redes Virtuais, vLans 802.1q, 802.3ad link aggregation;

10.5.18. Tradução de endereços da rede (NAT) por origem e destino, por endereços IP dinâmicos e pool de portas;
10.5.19. Suportar Jumbo Frames, BGP, OSPF e RIP2, DHCP Server e DHCP Relay;
10.5.20. Suportar protocolos de encriptação IKE, AES (com criptografia de 128 e
10.5.21. 256 bits), 3Des, SHA1 e MD5;
10.5.22. Suportar os protocolos de VoIP: H.323, SIP, SCCP e MGCP;
10.5.23. Em caso de protocolos e aplicações desconhecidos, poderão designar-se assinaturas próprias;
10.5.24. Detecção de aplicações dinâmicas dentro de sessões de proxy HTTP;
10.5.25. Controle de tráfego IPv4 e IPv6, ambos incluem, visibilidade e inspeção de ameaças em aplicações e controle de conteúdo. O IPv6 deve ser suportado em interfaces trabalhando em L2 e L3;
10.5.26. Suporte a objetos e regras IPv6 e Multicast;
10.5.27. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 (aplicação);
10.5.28. Suportar a atribuição de agendamento das políticas, com o objetivo de habilitar e desabilitar políticas em horários predefinidos automaticamente;
10.5.29. Suporte a identificação de usuários em ambiente virtualizado (Citrix, Microsoft Terminal Server, etc.), permitindo visibilidade e controle granular por usuário;
10.5.30. Suportar e realizar a sincronização dos equipamentos da solução via protocolo NTP;
10.5.31. Atualização de assinaturas:

10.5.31.1. Sob demanda (diária, semanal e de emergência);
10.5.31.2. Suportar atualização automática das assinaturas através de conexão segura;
10.5.31.3. Não devem depender de reboot do equipamento para efetivação;
10.5.31.4. Todos os equipamentos devem utilizar as mesmas assinaturas;

10.6. CONTROLE DE APLICAÇÕES

10.6.1. Deverá contar com ferramentas de visibilidade e controle que permitam administrar o tráfego de aplicações, permitindo o tráfego de aplicações autorizadas e bloqueio de aplicações não autorizadas;
10.6.2. Reconhecer no mínimo 2100 aplicações diferentes;
10.6.3. Controle de políticas por porta, protocolo, aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações, individualizado ou agrupado por usuários, grupos de usuários, IP, Redes;
10.6.4. Suportar controle de políticas baseada em geolocalização (países);
10.6.5. Capacidade de identificar as aplicações, independente das portas e protocolos, assim como técnicas de evasão utilizadas;
10.6.6. Incluir a capacidade de atualização para identificar novas aplicações;
10.6.7. Atualizar a base de assinaturas de aplicações automaticamente;
10.6.8. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas do fabricante;
10.6.9. Alertar o usuário quando uma aplicação foi bloqueada;
10.6.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
10.6.11. Possibilitar a diferenciação de aplicações Proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;

10.6.12. Possibilitar a diferenciação e bloqueio de tráfegos P2P (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;
10.6.13. Possibilitar a diferenciação e bloqueio de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, Whatsapp, etc.) possuindo granularidade de controle/políticas para os mesmos;
10.6.14. Possibilitar a diferenciação e controle de partes das aplicações, como, por exemplo, permitir o Gtalk, mas bloquear a transferência de arquivos por ele;
10.6.15. 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);
10.6.16. Capacidade de criação de políticas baseadas no controle por aplicação:

10.6.16.1. Por tecnologia: cliente-servidor, Browse Based, Network Protocol, etc.;
10.6.16.2. Por nível de risco da aplicação;
10.6.16.3. Por categoria e subcategoria de aplicações;

10.6.17. Baseadas em “traffic shaping” por aplicação, usuário, origem, destino, túnel VPN-IPSEC-SSL;

10.7. PROTEÇÃO IPS

10.7.1. Dispor de IPS integrado a solução de segurança;
10.7.2. Permitir o bloqueio de vulnerabilidades;
10.7.3. Permitir o bloqueio de exploits conhecidos;
10.7.4. Proteção contra ataques de negação de serviços (DoS);
10.7.5. Deverá possuir os seguintes mecanismos de inspeção de IPS:

10.7.5.1. Análise de padrões de estado de conexões;
10.7.5.2. Análise de decodificação de protocolo;
10.7.5.3. Análise para detecção de anomalias de protocolo;
10.7.5.4. Análise heurística;
10.7.5.5. IP Defragmentation;
10.7.5.6. Remontagem de pacotes de TCP;
10.7.5.7. Bloqueio de pacotes malformados;

10.7.6. Possuir assinaturas para bloqueio de ataques "buffer overflow";
10.7.7. Possuir assinaturas para auxílio no bloqueio de ataques distribuídos de negação de serviço (DDoS);
10.7.8. Possuir assinaturas e mecanismos de detecção de anomalias prontas;
10.7.9. Suportar o reconhecimento de ataques em tráfego IPv6;
10.7.10. Possibilitar a criação de assinaturas customizadas;
10.7.11. Possibilitar a criação de exceções/exclusões por hosts para determinadas assinaturas;
10.7.12. Suportar referência cruzada com CVE (Common Vulnerabilities and Exposures);
10.7.13. Possuir granularidade de ajustes com opções para sobrescrever assinaturas individualmente;
10.7.14. Suportar várias técnicas de prevenção, incluindo Drop e TCP-RST (Cliente, Servidor e ambos);
10.7.15. Suportar ações por assinaturas;
10.7.16. Suportar notificações e alertas via e-mail, whatsapp, SNMP traps e log de pacotes;
10.7.17. Suportar a captura de pacotes (PCAP) para fins de forense;

10.7.18. Análise dinâmica de ameaças do ambiente móvel e APK;
10.7.19. Não deve possuir recursos que delimitem a quantidade de bytes da sessão que será inspecionada;
10.7.20. Suportar atualização de assinaturas de ataque;
10.7.21. Possuir mecanismos que permita bloquear um ataque por expressão regular DNS;
10.7.22. Possuir autenticação em query DNS por requisição em TCP;
10.7.23. Prevenir que hosts validos sejam adicionados a blacklists por engano;
10.7.24. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing), ou garantir que esta exigência seja plenamente atendida por meio diverso;

10.8. PROTEÇÃO ANTIVÍRUS E ANTISPYWARE

10.8.1. Incluir módulo de Antivírus e Antispyware integrado na solução de segurança;
10.8.2. Permitir o bloqueio de Malwares e Spywares;
10.8.3. Capacidade de inspeção Antivírus, pelo menos, para os seguintes tipos de tráfegos: HTTP, SMTP, IMAP,POP3 e FTP;
10.8.4. Incluir proteção contra vírus em conteúdo HTML e javascript,software espião (spyware) e worms;
10.8.5. Proteção contra downloads involuntários, usando HTTP, de arquivos executáveis maliciosos;
10.8.6. Rastreamento de vírus em arquivos PDF
10.8.7. Permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, rar, etc.);
10.8.8. Suportar bloqueio de arquivos por tipo;
10.8.9. Suportar notificações e alertas via e-mail, whatsap, SNMP traps e log de pacotes;
10.8.10. Suportar a captura de pacotes (PCAP) para fins de forense;

10.9. ANÁLISE DE MALWARES MODERNOS

10.9.1. Solução ofertada deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria solução de segurança;
10.9.2. 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;
10.9.3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a escopo de proteção, tais como endereço de destino, podendo aplicar regras de exceção por assinaturas, endereço IP e/ou site;
10.9.4. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Microsoft Windows XP e versões mais novas;
10.9.5. Deve suportar a monitoração de arquivos trafegados na internet (HTTPS, HTTP, SMTP, FTP, IMAP, POP3) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

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

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

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

10.9.9. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

10.9.10. A solução deve ser fornecida em appliance local, deve possuindo, no mínimo, 10 ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;

10.9.11. Caso seja necessário licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

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

10.10. FILTRO DE URL

10.10.1. Incluir módulo de filtro de URL integrado a solução de segurança;

10.10.2. Possibilitar a configuração de políticas de filtro de URL baseado em políticas do firewall, individualizado ou agrupado por usuários, grupos de usuários, IP, redes ou zonas de segurança;

10.10.3. Incluir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

10.10.4. Possibilitar base de URL local no appliance, evitando atrasos (delay) de comunicação/validação da URL;

10.10.5. Possuir, pelo menos, 50 categorias de URL;

10.10.6. Possibilitar a criação Categorias de URL customizadas;

10.10.7. Possibilitar a exclusão de URL do bloqueio por categoria;

10.10.8. Possibilitar a customização de página de bloqueio;

10.11. CONTROLE DE TRÁFEGO

10.11.1. Permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.

10.11.2. Controle de políticas QoS por porta, aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações, endereço de origem e de destino, individualizado ou agrupado por usuários, grupos de usuários e IP;

10.11.3. Traffic shaping QoS baseado em políticas (prioridade, garantia e máximo);

10.11.4. Com a finalidade de controlar aplicações e trafego cujo consumo possa ser excessivo, (como youtube, upstream, 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, deva 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.

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

10.11.5.1. Banda Garantida;

10.11.5.2. Banda Máxima;
10.11.5.3. Fila de Prioridade;

10.11.6. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
10.11.7. Suportar marcação de pacotes Diffserv;
10.11.8. Disponibilizar estatísticas em tempo real para classes de QoS;
10.11.9. Permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.
10.11.10. Possibilitar a visualização dos países de origem e destino nos logs dos acessos;

10.12. GERAÇÃO DE LOGS

10.12.1. Os logs do produto devem incluir informações das atividades dos usuários;
10.12.2. Popular todos os logs de tráfego, IPS, URL, Data, Aplicações entre outros com as informações dos usuários;
10.12.3. Os logs de identificação de usuários devem ser feitos em tempo real (e não correlacionado após a ocorrência do tráfego em questão);
10.12.4. Deve suportar protocolo syslog, enviando as informações para um servidor syslog remoto a solução

10.13. MÓDULO VPN:

10.13.1. Suportar VPN Site-to-Site e Cliente-To-Site;
10.13.2. Suportar IPSec VPN;
10.13.3. Suportar SSL VPN;
10.13.4. Suportar atribuição de IP nos clientes remotos de VPN;
10.13.5. Suportar atribuição de DNS nos clientes remotos de VPN;

10.14. IPSEC VPN DEVE SUPORTAR:

10.14.1. 3DES, AES;
10.14.2. Autenticação MD5 e SHA-1;
10.14.3. Diffie-Hellman Group 1, Group 2 e Group 5;
10.14.4. Algoritimo Internet Key Exchange (IKE); e. AES 128, 256 (Advanced Encryption Standard);
10.14.5. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
10.14.6. Dispor de software cliente de VPN-SSL para os sistemas operacionais Windows (XP e mais novos), Linux e MacOS;
10.14.7. Permitir criar políticas para tráfego VPN-SSL;
10.14.8. SSL VPN com suporte a proxy ARP;
10.14.9. Suportar, pelo menos, 200 (duzentos) usuários simultâneos via SSL VPN; 1
10.14.10. Suporte para autenticação de VPN SSL, Ldap, Secure ID e base de dados própria;
10.14.11. Possuir interoperabilidade com, no mínimo, os seguintes fabricantes: Cisco, CheckPoint, Juniper, Palo Alto, Fortinet, SonicWall;

10.15. ROTEAMENTO E NAT

10.15.1. Suportar as seguintes funcionalidades de roteamento:

10.15.1.1. Estático e Dinâmico;
10.15.1.2. RIP v2;
10.15.1.3. OSPF;
10.15.1.4. BGP v4;

10.15.2. Suporte a roteamento IPv6;
10.15.3. Controle de políticas de redirecionamento por porta, aplicação, endereço de origem e de destino, individualizado ou agrupado por usuários, grupos de usuários e IP;

10.16. GERENCIAMENTO

10.16.1. Possuir interface "Out-Of-Band" dedicada para gerenciamento;

10.16.1.1. SSH;
10.16.1.2. HTTPS;

10.16.2. Monitoração de falha de link;
10.16.3. Suportar o gerenciamento por:

10.16.3.1. CLI via SSH;
10.16.3.2. WebUI via HTTPS;
10.16.3.3. Console;

10.16.4. O gerenciamento local do equipamento deve permitir:

10.16.4.1. Criação e administração de políticas;
10.16.4.2. Administração de políticas de IPS, Antivírus e Antispyware;
10.16.4.3. Política de Filtro de Dados e Filtro de URL;
10.16.4.4. Monitoração de logs;
10.16.4.5. Ferramentas de investigação de logs;
10.16.4.6. Debugging;
10.16.4.7. Captura de pacotes;

10.16.5. Possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;
10.16.6. Possibilidade de acessar o equipamento e aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;
10.16.7. Possibilitar gerenciamento do equipamento via protocolos SNMP, SNMP-V2 e SNMP-V3

10.17. ADMINISTRAÇÃO DO EQUIPAMENTO

10.17.1. Possibilitar a criação de diferentes profiles de administração separando, pelo menos: Leitura, Alterações, Relatórios e Monitoração;
10.17.2. Deverá ser possível de forma granular, assinar permissões para os administradores criarem outros usuários, alterarem configurações, ler configurações, etc.
10.17.3. Possibilidade de administrar o firewall localmente ou remotamente, sem causar problemas de sincronismo de configurações;
10.17.4. Habilidade de upgrade via SCP e Web-UI;
10.17.5. Suportar rollback de configuração para a última configuração salva;
10.17.6. Suportar rollback de Sistema Operacional para a última versão local;
10.17.7. Validação de regras antes da aplicação;

10.17.8. Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores, quando houver mais de um administrador executando alterações simultaneamente;

10.17.9. Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;

10.17.10. Possibilitar a integração com outras soluções de SIEM de mercado ("third-party SIEM vendors");

10.18. RELATÓRIOS

10.18.1. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos gateways de segurança;

10.18.2. Possuir relatórios de utilização dos recursos por aplicações,URL, Ameaças, etc.;

10.18.3. Prover uma visualização sumarizada de todas as aplicações, ameaças e URL que passaram pela solução;

10.18.4. Possibilidade de identificar o usuário que fez determinado acesso;

10.18.5. Possibilidade de exportar os logs CSV;

10.18.6. Possibilidade de capturar as URL acessadas para todas as sessões HTTP;

10.18.7. Gerar alertas automáticos via:

10.18.7.1. E-mail;

10.18.7.2. SNMP;

10.18.7.3. WhatsApp.

11. NÍVEIS DE SERVIÇO - ITEM 7

11.1. ALOCAÇÃO DE SOLUÇÃO DE SEGURANÇA

11.1.1. Alocação de, no mínimo, 02 (dois) equipamentos (baseado em appliance), idênticos, com função de Next-Generation Firewall (NGFW), Statefull, implementando a solução de alta disponibilidade com tolerância a falhas (HA), podendo ser admitida a configuração ativo-passivo e ativo-ativo; Os equipamentos devem atender as funções e funcionalidades, no mínimo:

11.1.1.1. Controle de Aplicações

11.1.1.2. Proteção IPS

11.1.1.3. Proteção Antivírus, Antispyware

11.1.1.4. Análise de Malwares Modernos

11.1.1.5. Filtro de URL

11.1.1.6. Controle de Transferência de Arquivos

11.1.1.7. Controle de Tráfego

11.1.1.8. Módulo VPN

11.1.1.9. Roteamento e NAT

11.2. CARACTERÍSTICAS DA DEMANDA, E CONFIGURAÇÕES MÍNIMAS DOS EQUIPAMENTOS:

11.2.1. O serviço deve incluir as substituições de equipamentos, sem ônus, caso se perceba limitação ou degradação da rede com base nos limites físicos (banda, portas, cabos), conforme demanda especificado neste Termo;

11.2.2. O serviço deve incluir as substituições de equipamentos defeituosos fornecidos na composição da solução;

11.2.3. A solução appliance não irá permitir soluções instaladas e executadas em um sistema operacional regular, como Microsoft Windows, FreeBSD, SUN solaris, GNU/Linux, etc.

11.2.4. Garantir que não haja restrição por número de usuários que utilizem a solução disponibilizada;

11.2.5. Os equipamentos devem ser instalados no endereço indicado pela Contratante, em rack padrão de 19'';

11.2.6. Incluir todas as licenças de software e de hardware necessárias ao perfeito e completo funcionamento das soluções ofertadas;

11.2.7. Disponibilizar um número de serviço, em língua portuguesa, para abertura de chamados técnicos. Este serviço deverá obrigatoriamente estar disponível 24x7;

11.2.8. Adicionalmente, o serviço deve prever que, ao término do contrato, todos os equipamentos e softwares deverão permanecer à disposição da contratante, sem custos a contratante, por período de até seis meses, a critério da Contratante, para fins de migração da solução para um novo contrato, devendo, durante este período, atender e respeitar todas as cláusulas e regras deste Termo de Referência, bem como de seus anexos, contratos e adendos;

11.3. CARACTERÍSTICAS DA DEMANDA

11.3.1. Banda instalada de link da internet de 200 Mbps (duzentos megabits por segundo);

11.3.2. Previsão de crescimento para, no mínimo, o dobro (quatrocentos megabits por segundo) em até sessenta meses;

11.3.3. Para que o serviço não gere degradação da rede, recomenda-se que a solução instalada suporte, pelo menos, a taxa de transferência (throughput) de no mínimo 200 Mbps (duzentos megabits por segundo) de DPI total, com todos os recursos necessários, e recomendados pelo fabricante, habilitados (valor medido em sessões HTTP 64k), incluindo:

Especificação Mínima	**Valor**
Throughput de Firewall (Gbps)	0,95
Conexões simultâneas (milhões)	0,9
Novas conexões por segundo (mil)	15
Throughput de IPSec (Gbps)	0,7
Proteção combinada contra ameaças* (Mbps)	150
Quantidade mínima de interfaces (1 Gbps)	2
Políticas de Firewall (mil)	5

* Com funcionalidades habilitadas simultaneamente devidamente atuantes: controle de aplicação, IDS/IPS e controle de malware (antivírus, etc.) medidas com parâmetros de throughput considerando tráfego misto. Não serão aceitas medidas baseadas em condições ideais.

11.4. INSTALAÇÃO, CONFIGURAÇÃO E INTEGRAÇÃO

11.4.1. Executar todos dos serviços de instalação, configuração, integração e testes de funcionalidade, dentro do prazo máximo de 15 (quinze) dias corridos, a contar da data de aceite da solução;

11.4.2. Elaborar conjuntamente com a contratante o planejamento da implantação no ambiente da contratante;

11.4.3. Efetuar a instalação, configuração, integração e testes de funcionalidade dos equipamentos:

11.4.3.1. Instalação física do firewall no ponto de conexão com a Internet e as redes conectadas;

11.4.3.2. Deverão ser efetuadas de acordo com o plano de implantação, a ser elaborada em conjunto com a contratante visando obter o melhor uso dos equipamentos;

11.4.3.3. Realizar, com os técnicos da contratante, testes de funcionalidade para constatar que os equipamentos foram instalados, configurados e integrados de acordo com os requisitos técnicos e parâmetros de configuração solicitados;

11.4.3.4. Elaborar uma documentação técnica, contendo todas as configurações efetuadas e as descrições das características e recursos utilizados;

11.4.4. Colocar à disposição da contratante, analistas técnicos especializados para a execução das soluções a serem implantadas em sua rede corporativa durante o tempo de funcionamento da solução, estes técnicos deverão ser devidamente certificados pelo fabricante da solução, e a certificação não pode estar vencida durante o período o período do contrato:

11.4.5. Configuração do firewall com as políticas de acesso e estrutura de segurança:

11.4.5.1. Integração com o diretório de usuários corporativos (AD) /LDAP;

11.4.5.2. Configuração do controle de aplicações;

11.4.5.3. Configuração das VLAN;

11.4.5.4. Configuração do Filtro de conteúdo WEB;

11.4.5.5. Configuração do anti-malware de gateway;

11.4.5.6. Configuração do IPS;

11.4.5.7. Configuração dos parâmetros de QoS que serão fornecidos pela equipe técnica da contratante;

11.4.5.8. Configuração dos clientes de VPN;

11.4.5.9. Testes e monitoração;

11.5. CONFIGURAÇÕES MÍNIMAS DOS EQUIPAMENTOS

11.5.1. Não deve haver degradação de performance de inspeção de firewall e de controle de aplicação, abaixo dos valores físicos da rede (banda do link e throughput das portas), quando funções de IPS, Antivírus e Antispyware forem habilitadas simultaneamente;

11.5.2. O equipamento não deve ser fator limitante para o tráfego da rede;

11.5.3. Fazer uso de appliance específico para o propósito solicitado;

11.5.4. Fonte de alimentação com operação automática entre 110/220V;

11.5.5. Possuir no mínimo 08 (oito) interfaces 10/100/1000Base-TX autosense, operando em full duplex, com inversão automática de polaridade configuráveis pelo administrador da solução.

11.5.6. Prover otimização para análise de conteúdo de aplicações na camada 7 do modelo OSI;

11.5.7. Possuir proteção anti-spoofing;

11.5.8. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados de rede;
11.5.9. Possuir 02 (duas) interfaces de 1 Gbps (SFP+);
11.5.10. Suportar funcionamento em:

11.5.10.1. Tap (via porta espelhada, Tap ou SPAN port);
11.5.10.2. Transparente (Bridge ou similar);
11.5.10.3. Layer2;
11.5.10.4. Layer3;

11.5.11. Suportar Vlan Tagging (802.1Q) em todas os cenários de implementação acima (Transparente, Layer2 e Layer3);
11.5.12. Suportar controle de aplicações IPv6 em todas os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3);
11.5.13. Suportar os seguintes tipos de NAT:

11.5.13.1. Porta/IP Nat dinâmico (Many-to-1 e Many-to-Many);
11.5.13.2. Nat dinâmico (Many-to-Many);
11.5.13.3. Nat estático (1-to-1, Many-to-Many, Ips);
11.5.13.4. Nat estático bidirecional 1-to-1;
11.5.13.5. Tradução de porta (PAT);
11.5.13.6. NAT de Origem;
11.5.13.7. NAT de Destino;
11.5.13.8. Suportar NAT de Origem e NAT de Destino, individualmente e simultaneamente;

11.5.14. A solução deve sincronizar:

11.5.14.1. Todas as sessões;
11.5.14.2. Certificados decriptogafados;
11.5.14.3. Todas associações de segurança das VPN;
11.5.14.4. Todas as assinaturas de Antivírus, Antispyware e Aplicações;
11.5.14.5. Todas as configurações;
11.5.14.6. Tabelas FIB;

11.5.15. Possuir algoritmos de análise de comportamento e perfil do tráfego, detectando ações estranhas ao comportamento normal prevenindo as ações de invasão da rede;
11.5.16. Compatibilidade e integração, em todos os seus módulos, com o Microsoft Active Directory (AD) e LDAP, para fins de identificação e controle de acessos individualizados por usuário ou por grupo de usuários;
11.5.17. Capacidade de operar, de forma simultânea, mediante o uso das suas interfaces físicas nos seguintes modos:

11.5.17.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
11.5.17.2. Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
11.5.17.3. Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
11.5.17.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
11.5.17.5. Redes Virtuais, vLans 802.1q, 802.3ad link aggregation;

11.5.18. Tradução de endereços da rede (NAT) por origem e destino, por endereços IP dinâmicos e pool de portas;
11.5.19. Suportar Jumbo Frames, BGP, OSPF e RIP2, DHCP Server e DHCP Relay;
11.5.20. Suportar protocolos de encriptação IKE, AES (com criptografia de 128 e

11.5.21. 256 bits), 3Des, SHA1 e MD5;
11.5.22. Suportar os protocolos de VoIP: H.323, SIP, SCCP e MGCP;
11.5.23. Em caso de protocolos e aplicações desconhecidos, poderão designar-se assinaturas próprias;
11.5.24. Detecção de aplicações dinâmicas dentro de sessões de proxy HTTP;
11.5.25. Controle de tráfego IPv4 e IPv6, ambos incluem, visibilidade e inspeção de ameaças em aplicações e controle de conteúdo. O IPv6 deve ser suportado em interfaces trabalhando em L2 e L3;
11.5.26. Suporte a objetos e regras IPv6 e Multicast;
11.5.27. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 (aplicação);
11.5.28. Suportar a atribuição de agendamento das políticas, com o objetivo de habilitar e desabilitar políticas em horários predefinidos automaticamente;
11.5.29. Suporte a identificação de usuários em ambiente virtualizado (Citrix, Microsoft Terminal Server, etc.), permitindo visibilidade e controle granular por usuário;
11.5.30. Suportar e realizar a sincronização dos equipamentos da solução via protocolo NTP;
11.5.31. Atualização de assinaturas:

11.5.31.1. Sob demanda (diária, semanal e de emergência);
11.5.31.2. Suportar atualização automática das assinaturas através de conexão segura;
11.5.31.3. Não devem depender de reboot do equipamento para efetivação;
11.5.31.4. Todos os equipamentos devem utilizar as mesmas assinaturas;

11.6. CONTROLE DE APLICAÇÕES

11.6.1. Deverá contar com ferramentas de visibilidade e controle que permitam administrar o tráfego de aplicações, permitindo o tráfego de aplicações autorizadas e bloqueio de aplicações não autorizadas;
11.6.2. Reconhecer no mínimo 2100 aplicações diferentes;
11.6.3. Controle de políticas por porta, protocolo, aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações, individualizado ou agrupado por usuários, grupos de usuários, IP, Redes;
11.6.4. Suportar controle de políticas baseada em geolocalização (países);
11.6.5. Capacidade de identificar as aplicações, independente das portas e protocolos, assim como técnicas de evasão utilizadas;
11.6.6. Incluir a capacidade de atualização para identificar novas aplicações;
11.6.7. Atualizar a base de assinaturas de aplicações automaticamente;
11.6.8. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas do fabricante;
11.6.9. Alertar o usuário quando uma aplicação foi bloqueada;
11.6.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
11.6.11. Possibilitar a diferenciação de aplicações Proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;
11.6.12. Possibilitar a diferenciação e bloqueio de tráfegos P2P (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;
11.6.13. Possibilitar a diferenciação e bloqueio de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, Whatsapp, etc.) possuindo granularidade de controle/políticas para os mesmos;

11.6.14. Possibilitar a diferenciação e controle de partes das aplicações, como, por exemplo, permitir o Gtalk, mas bloquear a transferência de arquivos por ele;
11.6.15. 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);
11.6.16. Capacidade de criação de políticas baseadas no controle por aplicação:

11.6.16.1. Por tecnologia: cliente-servidor, Browse Based, Network Protocol, etc.;
11.6.16.2. Por nível de risco da aplicação;
11.6.16.3. Por categoria e subcategoria de aplicações;

11.6.17. Baseadas em “traffic shaping” por aplicação, usuário, origem, destino, túnel VPN-IPSEC-SSL;

11.7. PROTEÇÃO IPS

11.7.1. Dispor de IPS integrado a solução de segurança;
11.7.2. Permitir o bloqueio de vulnerabilidades;
11.7.3. Permitir o bloqueio de exploits conhecidos;
11.7.4. Proteção contra ataques de negação de serviços (DoS);
11.7.5. Deverá possuir os seguintes mecanismos de inspeção de IPS:

11.7.5.1. Análise de padrões de estado de conexões;
11.7.5.2. Análise de decodificação de protocolo;
11.7.5.3. Análise para detecção de anomalias de protocolo;
11.7.5.4. Análise heurística;
11.7.5.5. IP Defragmentation;
11.7.5.6. Remontagem de pacotes de TCP;
11.7.5.7. Bloqueio de pacotes malformados;

11.7.6. Possuir assinaturas para bloqueio de ataques "buffer overflow";
11.7.7. Possuir assinaturas para auxílio no bloqueio de ataques distribuídos de negação de serviço (DDoS);
11.7.8. Possuir assinaturas e mecanismos de detecção de anomalias prontas;
11.7.9. Suportar o reconhecimento de ataques em tráfego IPv6;
11.7.10. Possibilitar a criação de assinaturas customizadas;
11.7.11. Possibilitar a criação de exceções/exclusões por hosts para determinadas assinaturas;
11.7.12. Suportar referência cruzada com CVE (Common Vulnerabilities and Exposures);
11.7.13. Possuir granularidade de ajustes com opções para sobrescrever assinaturas individualmente;
11.7.14. Suportar várias técnicas de prevenção, incluindo Drop e TCP-RST (Cliente, Servidor e ambos);
11.7.15. Suportar ações por assinaturas;
11.7.16. Suportar notificações e alertas via e-mail, whatsapp, SNMP traps e log de pacotes;
11.7.17. Suportar a captura de pacotes (PCAP) para fins de forense;
11.7.18. Análise dinâmica de ameaças do ambiente móvel e APK;
11.7.19. Não deve possuir recursos que delimitem a quantidade de bytes da sessão que será inspecionada;
11.7.20. Suportar atualização de assinaturas de ataque;

11.7.21. Possuir mecanismos que permita bloquear um ataque por expressão regular DNS;

11.7.22. Possuir autenticação em query DNS por requisição em TCP;

11.7.23. Prevenir que hosts validos sejam adicionados a blacklists por engano;

11.7.24. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing), ou garantir que esta exigência seja plenamente atendida por meio diverso;

11.8. PROTEÇÃO ANTIVÍRUS E ANTISPYWARE

11.8.1. Incluir módulo de Antivírus e Antispyware integrado na solução de segurança;

11.8.2. Permitir o bloqueio de Malwares e Spywares;

11.8.3. Capacidade de inspeção Antivírus, pelo menos, para os seguintes tipos de tráfegos: HTTP, SMTP, IMAP,POP3 e FTP;

11.8.4. Incluir proteção contra vírus em conteúdo HTML e javascript,software espião (spyware) e worms;

11.8.5. Proteção contra downloads involuntários, usando HTTP, de arquivos executáveis maliciosos;

11.8.6. Rastreamento de vírus em arquivos PDF

11.8.7. Permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, rar, etc.);

11.8.8. Suportar bloqueio de arquivos por tipo;

11.8.9. Suportar notificações e alertas via e-mail, whatsap, SNMP traps e log de pacotes;

11.8.10. Suportar a captura de pacotes (PCAP) para fins de forense;

11.9. ANÁLISE DE MALWARES MODERNOS

11.9.1. Solução ofertada deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria solução de segurança;

11.9.2. 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;

11.9.3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a escopo de proteção, tais como endereço de destino, podendo aplicar regras de exceção por assinaturas, endereço IP e/ou site;

11.9.4. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Microsoft Windows XP e versões mais novas;

11.9.5. Deve suportar a monitoração de arquivos trafegados na internet (HTTPS, HTTP, SMTP, FTP, IMAP, POP3) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

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

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

11.9.8. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;
11.9.9. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;
11.9.10. A solução deve ser fornecida em appliance local, deve possuindo, no mínimo, 10 ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;
11.9.11. Caso seja necessário licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;
11.9.12. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

11.10. FILTRO DE URL

11.10.1. Incluir módulo de filtro de URL integrado a solução de segurança;
11.10.2. Possibilitar a configuração de políticas de filtro de URL baseado em políticas do firewall, individualizado ou agrupado por usuários, grupos de usuários, IP, redes ou zonas de segurança;
11.10.3. Incluir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
11.10.4. Possibilitar base de URL local no appliance, evitando atrasos (delay) de comunicação/validação da URL;
11.10.5. Possuir, pelo menos, 50 categorias de URL;
11.10.6. Possibilitar a criação Categorias de URL customizadas;
11.10.7. Possibilitar a exclusão de URL do bloqueio por categoria;
11.10.8. Possibilitar a customização de página de bloqueio;

11.11. CONTROLE DE TRÁFEGO

11.11.1. Permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.
11.11.2. Controle de políticas QoS por porta, aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações, endereço de origem e de destino, individualizado ou agrupado por usuários, grupos de usuários e IP;
11.11.3. Traffic shaping QoS baseado em políticas (prioridade, garantia e máximo);
11.11.4. Com a finalidade de controlar aplicações e trafego cujo consumo possa ser excessivo, (como youtube, upstream, 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, deva 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.
11.11.5. O QoS deve possibilitar a definição de classes por:

11.11.5.1. Banda Garantida;
11.11.5.2. Banda Máxima;
11.11.5.3. Fila de Prioridade;

11.11.6. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

11.11.7. Suportar marcação de pacotes Diffserv;
11.11.8. Disponibilizar estatísticas em tempo real para classes de QoS;
11.11.9. Permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.
11.11.10. Possibilitar a visualização dos países de origem e destino nos logs dos acessos;

11.12. GERAÇÃO DE LOGS

11.12.1. Os logs do produto devem incluir informações das atividades dos usuários;
11.12.2. Popular todos os logs de tráfego, IPS, URL, Data, Aplicações entre outros com as informações dos usuários;
11.12.3. Os logs de identificação de usuários devem ser feitos em tempo real (e não correlacionado após a ocorrência do tráfego em questão);
11.12.4. Deve suportar protocolo syslog, enviando as informações para um servidor syslog remoto a solução

11.13. MÓDULO VPN:

11.13.1. Suportar VPN Site-to-Site e Cliente-To-Site;
11.13.2. Suportar IPSec VPN;
11.13.3. Suportar SSL VPN;
11.13.4. Suportar atribuição de IP nos clientes remotos de VPN;
11.13.5. Suportar atribuição de DNS nos clientes remotos de VPN;

11.14. IPSEC VPN DEVE SUPORTAR:

11.14.1. 3DES, AES;
11.14.2. Autenticação MD5 e SHA-1;
11.14.3. Diffie-Hellman Group 1, Group 2 e Group 5;
11.14.4. Algoritimo Internet Key Exchange (IKE); e. AES 128, 256 (Advanced Encryption Standard);
11.14.5. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
11.14.6. Dispor de software cliente de VPN-SSL para os sistemas operacionais Windows (XP e mais novos), Linux e MacOS;
11.14.7. Permitir criar políticas para tráfego VPN-SSL;
11.14.8. SSL VPN com suporte a proxy ARP;
11.14.9. Suportar, pelo menos, 200 (duzentos) usuários simultâneos via SSL VPN; 1
11.14.10. Suporte para autenticação de VPN SSL, Ldap, Secure ID e base de dados própria;
11.14.11. Possuir interoperabilidade com, no mínimo, os seguintes fabricantes: Cisco, CheckPoint, Juniper, Palo Alto, Fortinet, SonicWall;

11.15. ROTEAMENTO E NAT

11.15.1. Suportar as seguintes funcionalidades de roteamento:

11.15.1.1. Estático e Dinâmico;
11.15.1.2. RIP v2;
11.15.1.3. OSPF;

11.15.1.4. BGP v4;

11.15.2. Suporte a roteamento IPv6;
11.15.3. Controle de políticas de redirecionamento por porta, aplicação, endereço de origem e de destino, individualizado ou agrupado por usuários, grupos de usuários e IP;

11.16. GERENCIAMENTO

11.16.1. Possuir interface “Out-Of-Band” dedicada para gerenciamento;

11.16.1.1. SSH;
11.16.1.2. HTTPS;

11.16.2. Monitoração de falha de link;
11.16.3. Suportar o gerenciamento por:

11.16.3.1. CLI via SSH;
11.16.3.2. WebUI via HTTPS;
11.16.3.3. Console;

11.16.4. O gerenciamento local do equipamento deve permitir:

11.16.4.1. Criação e administração de políticas;
11.16.4.2. Administração de políticas de IPS, Antivírus e Antispyware;
11.16.4.3. Política de Filtro de Dados e Filtro de URL;
11.16.4.4. Monitoração de logs;
11.16.4.5. Ferramentas de investigação de logs;
11.16.4.6. Debugging;
11.16.4.7. Captura de pacotes;

11.16.5. Possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;
11.16.6. Possibilidade de acessar o equipamento e aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;
11.16.7. Possibilitar gerenciamento do equipamento via protocolos SNMP, SNMP-V2 e SNMP-V3

11.17. ADMINISTRAÇÃO DO EQUIPAMENTO

11.17.1. Possibilitar a criação de diferentes profiles de administração separando, pelo menos: Leitura, Alterações, Relatórios e Monitoração;
11.17.2. Deverá ser possível de forma granular, assinar permissões para os administradores criarem outros usuários, alterarem configurações, ler configurações, etc.
11.17.3. Possibilidade de administrar o firewall localmente ou remotamente, sem causar problemas de sincronismo de configurações;
11.17.4. Habilidade de upgrade via SCP e Web-UI;
11.17.5. Suportar rollback de configuração para a última configuração salva;
11.17.6. Suportar rollback de Sistema Operacional para a última versão local;
11.17.7. Validação de regras antes da aplicação;
11.17.8. Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores, quando houver mais de um administrador executando alterações simultaneamente;

11.17.9. Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
11.17.10. Possibilitar a integração com outras soluções de SIEM de mercado (“third-party SIEM vendors”);

11.18. RELATÓRIOS

11.18.1. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos gateways de segurança;
11.18.2. Possuir relatórios de utilização dos recursos por aplicações,URL, Ameaças, etc.;
11.18.3. Prover uma visualização sumarizada de todas as aplicações, ameaças e URL que passaram pela solução;
11.18.4. Possibilidade de identificar o usuário que fez determinado acesso;
11.18.5. Possibilidade de exportar os logs CSV;
11.18.6. Possibilidade de capturar as URL acessadas para todas as sessões HTTP;
11.18.7. Gerar alertas automáticos via:

11.18.7.1. E-mail;
11.18.7.2. SNMP;
11.18.7.3. WhatsApp.

12. NÍVEIS DE SERVIÇO - ITEM 8

12.1. ALOCAÇÃO DE SOLUÇÃO DE SEGURANÇA

12.1.1. Alocação de, no mínimo, 02 (dois) equipamentos (baseado em appliance), idênticos, com função de Next-Generation Firewall (NGFW), Statefull, implementando a solução de alta disponibilidade com tolerância a falhas (HA), podendo ser admitida a configuração ativo-passivo e ativo-ativo; os equipamentos devem atender as funções e funcionalidades, no mínimo:

12.1.1.1. Controle de Aplicações
12.1.1.2. Proteção IPS
12.1.1.3. Proteção Antivírus, Antispyware
12.1.1.4. Análise de Malwares Modernos
12.1.1.5. Filtro de URL
12.1.1.6. Controle de Transferência de Arquivos
12.1.1.7. Controle de Tráfego
12.1.1.8. Módulo VPN
12.1.1.9. Roteamento e NAT

12.2. CARACTERÍSTICAS DA DEMANDA, E CONFIGURAÇÕES MÍNIMAS DOS EQUIPAMENTOS:

12.2.1. O serviço deve incluir as substituições de equipamentos, sem ônus, caso se perceba limitação ou degradação da rede com base nos limites físicos (banda, portas, cabos), conforme demanda especificado neste Termo;
12.2.2. O serviço deve incluir as substituições de equipamentos defeituosos fornecidos na composição da solução;
12.2.3. A solução appliance não irá permitir soluções instaladas e executadas em um sistema operacional regular, como Microsoft Windows, FreeBSD, SUN solaris, GNU/Linux, etc.

12.2.4. Garantir que não haja restrição por número de usuários que utilizem a solução disponibilizada;
12.2.5. Os equipamentos devem ser instalados no endereço indicado pela Contratante, em rack padrão de 19’’;
12.2.6. Incluir todas as licenças de software e de hardware necessárias ao perfeito e completo funcionamento das soluções ofertadas;
12.2.7. Disponibilizar um número de serviço, em língua portuguesa, para abertura de chamados técnicos. Este serviço deverá obrigatoriamente estar disponível 24x7;
12.2.8. Adicionalmente, o serviço deve prever que, ao término do contrato, todos os equipamentos e softwares deverão permanecer à disposição da contratante, sem custos a contratante, por período de até seis meses, a critério da Contratante, para fins de migração da solução para um novo contrato, devendo, durante este período, atender e respeitar todas as cláusulas e regras deste Termo de Referência, bem como de seus anexos, contratos e adendos;

12.3. CARACTERÍSTICAS DA DEMANDA

12.3.1. Banda instalada de link da internet de 50 Mbps (50 megabits por segundo);
12.3.2. Previsão de crescimento para, no mínimo, o dobro (cem megabits por segundo) em até sessenta meses;
12.3.3. Para que o serviço não gere degradação da rede, recomenda-se que a solução instalada suporte, pelo menos, a taxa de transferência (throughput) de no mínimo 50 Mbps (cinquenta megabits por segundo) de DPI total, com todos os recursos necessários, e recomendados pelo fabricante, habilitados (valor medido em sessões HTTP 64k), incluindo:
12.3.4. Todos os serviços web ofertados devem ser suportados por todos os navegadores web e sistemas operacionais disponíveis no mercado;

Especificação Mínima	**Valor**
Throughput de Firewall (Gbps)	0,95
Conexões simultâneas (milhões)	0,9
Novas conexões por segundo (mil)	15
Throughput de IPSec (Gbps)	0,7
Proteção combinada contra ameaças* (Mbps)	150
Quantidade mínima de interfaces (1 Gbps)	2
Políticas de Firewall (mil)	5

* Com funcionalidades habilitadas simultaneamente devidamente atuantes: controle de aplicação, IDS/IPS e controle de malware (antivírus, etc.) medidas com parâmetros de throughput considerando tráfego misto. Não serão aceitas medidas baseadas em condições ideais.

12.4. INSTALAÇÃO, CONFIGURAÇÃO E INTEGRAÇÃO

12.4.1. Executar todos dos serviços de instalação, configuração, integração e testes de funcionalidade, dentro do prazo máximo de 15 (quinze) dias corridos, a contar da data de aceite da solução;

12.4.2. Elaborar conjuntamente com a contratante o planejamento da implantação no ambiente da contratante;

12.4.3. Efetuar a instalação, configuração, integração e testes de funcionalidade dos equipamentos:

12.4.3.1. Instalação física do firewall no ponto de conexão com a Internet e as redes conectadas;

12.4.3.2. Deverão ser efetuadas de acordo com o plano de implantação, a ser elaborada em conjunto com a contratante visando obter o melhor uso dos equipamentos;

12.4.3.3. Realizar, com os técnicos da contratante, testes de funcionalidade para constatar que os equipamentos foram instalados, configurados e integrados de acordo com os requisitos técnicos e parâmetros de configuração solicitados;

12.4.3.4. Elaborar uma documentação técnica, contendo todas as configurações efetuadas e as descrições das características e recursos utilizados;

12.4.4. Colocar à disposição da contratante, analistas técnicos especializados para a execução das soluções a serem implantadas em sua rede corporativa durante o tempo de funcionamento da solução, estes técnicos deverão ser devidamente certificados pelo fabricante da solução, e a certificação não pode estar vencida durante o período o período do contrato:

12.4.5. Configuração do firewall com as políticas de acesso e estrutura de segurança:

12.4.5.1. Integração com o diretório de usuários corporativos (AD) /LDAP;

12.4.5.2. Configuração do controle de aplicações;

12.4.5.3. Configuração das VLAN;

12.4.5.4. Configuração do Filtro de conteúdo WEB;

12.4.5.5. Configuração do anti-malware de gateway;

12.4.5.6. Configuração do IPS;

12.4.5.7. Configuração dos parâmetros de QoS que serão fornecidos pela equipe técnica da contratante;

12.4.5.8. Configuração dos clientes de VPN;

12.4.5.9. Testes e monitoração;

12.5. CONFIGURAÇÕES MÍNIMAS DOS EQUIPAMENTOS

12.5.1. Não deve haver degradação de performance de inspeção de firewall e de controle de aplicação, abaixo dos valores físicos da rede (banda do link e throughput das portas), quando funções de IPS, Antivírus e Antispyware forem habilitadas simultaneamente;

12.5.2. O equipamento não deve ser fator limitante para o tráfego da rede;

12.5.3. Fazer uso de appliance específico para o propósito solicitado;

12.5.4. Prover otimização para análise de conteúdo de aplicações na camada 7 do modelo OSI;

12.5.5. Possuir proteção anti-spoofing;

12.5.6. Suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados de rede;

12.5.7. Fonte de alimentação com operação automática entre 110/220V;

12.5.8. Possuir no mínimo 2 (duas) interfaces 10/100/1000Base-TX autosense, operando em full duplex, com inversão automática de polaridade configuráveis pelo administrador da solução.

12.5.9. Possuir 02 (duas) interfaces de 1 Gbps (SFP+);
12.5.10. Suportar funcionamento em:

12.5.10.1. Tap (via porta espelhada, Tap ou SPAN port);
12.5.10.2. Transparente (Bridge ou similar);
12.5.10.3. Layer2;
12.5.10.4. Layer3;

12.5.11. Suportar Vlan Tagging (802.1Q) em todas os cenários de implementação acima (Transparente, Layer2 e Layer3);
12.5.12. Suportar controle de aplicações IPv6 em todas os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3);
12.5.13. Suportar os seguintes tipos de NAT:

12.5.13.1. Porta/IP Nat dinâmico (Many-to-1 e Many-to-Many);
12.5.13.2. Nat dinâmico (Many-to-Many);
12.5.13.3. Nat estático (1-to-1, Many-to-Many, Ips);
12.5.13.4. Nat estático bidirecional 1-to-1;
12.5.13.5. Tradução de porta (PAT);
12.5.13.6. NAT de Origem;
12.5.13.7. NAT de Destino;
12.5.13.8. Suportar NAT de Origem e NAT de Destino, individualmente e simultaneamente;

12.5.14. A solução deve sincronizar:

12.5.14.1. Todas as sessões;
12.5.14.2. Certificados decriptogafados;
12.5.14.3. Todas associações de segurança das VPN;
12.5.14.4. Todas as assinaturas de Antivírus, Antispyware e Aplicações;
12.5.14.5. Todas as configurações;
12.5.14.6. Tabelas FIB;

12.5.15. Possuir algoritmos de análise de comportamento e perfil do tráfego, detectando ações estranhas ao comportamento normal prevenindo as ações de invasão da rede;
12.5.16. Compatibilidade e integração, em todos os seus módulos, com o Microsoft Active Directory (AD) e LDAP, para fins de identificação e controle de acessos individualizados por usuário ou por grupo de usuários;
12.5.17. Capacidade de operar, de forma simultânea, mediante o uso das suas interfaces físicas nos seguintes modos:

12.5.17.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
12.5.17.2. Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
12.5.17.3. Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
12.5.17.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
12.5.17.5. Redes Virtuais, vLans 802.1q, 802.3ad link aggregation;

12.5.18. Tradução de endereços da rede (NAT) por origem e destino, por endereços IP dinâmicos e pool de portas;
12.5.19. Suportar Jumbo Frames, BGP, OSPF e RIP2, DHCP Server e DHCP Relay;
12.5.20. Suportar protocolos de encriptação IKE, AES (com criptografia de 128 e
12.5.21. 256 bits), 3Des, SHA1 e MD5;
12.5.22. Suportar os protocolos de VoIP: H.323, SIP, SCCP e MGCP;

12.5.23. Em caso de protocolos e aplicações desconhecidos, poderão designar-se assinaturas próprias;
12.5.24. Detecção de aplicações dinâmicas dentro de sessões de proxy HTTP;
12.5.25. Controle de tráfego IPv4 e IPv6, ambos incluem, visibilidade e inspeção de ameaças em aplicações e controle de conteúdo. O IPv6 deve ser suportado em interfaces trabalhando em L2 e L3;
12.5.26. Suporte a objetos e regras IPv6 e Multicast;
12.5.27. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 (aplicação);
12.5.28. Suportar a atribuição de agendamento das políticas, com o objetivo de habilitar e desabilitar políticas em horários predefinidos automaticamente;
12.5.29. Suporte a identificação de usuários em ambiente virtualizado (Citrix, Microsoft Terminal Server, etc.), permitindo visibilidade e controle granular por usuário;
12.5.30. Suportar e realizar a sincronização dos equipamentos da solução via protocolo NTP;
12.5.31. Atualização de assinaturas:

12.5.31.1. Sob demanda (diária, semanal e de emergência);
12.5.31.2. Suportar atualização automática das assinaturas através de conexão segura;
12.5.31.3. Não devem depender de reboot do equipamento para efetivação;
12.5.31.4. Todos os equipamentos devem utilizar as mesmas assinaturas;

12.6. CONTROLE DE APLICAÇÕES

12.6.1. Deverá contar com ferramentas de visibilidade e controle que permitam administrar o tráfego de aplicações, permitindo o tráfego de aplicações autorizadas e bloqueio de aplicações não autorizadas;
12.6.2. Reconhecer no mínimo 2100 aplicações diferentes;
12.6.3. Controle de políticas por porta, protocolo, aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações, individualizado ou agrupado por usuários, grupos de usuários, IP, Redes;
12.6.4. Suportar controle de políticas baseada em geolocalização (países);
12.6.5. Capacidade de identificar as aplicações, independente das portas e protocolos, assim como técnicas de evasão utilizadas;
12.6.6. Incluir a capacidade de atualização para identificar novas aplicações;
12.6.7. Atualizar a base de assinaturas de aplicações automaticamente;
12.6.8. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas do fabricante;
12.6.9. Alertar o usuário quando uma aplicação foi bloqueada;
12.6.10. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
12.6.11. Possibilitar a diferenciação de aplicações Proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;
12.6.12. Possibilitar a diferenciação e bloqueio de tráfegos P2P (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos;
12.6.13. Possibilitar a diferenciação e bloqueio de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, Whatsapp, etc.) possuindo granularidade de controle/políticas para os mesmos;
12.6.14. Possibilitar a diferenciação e controle de partes das aplicações, como, por exemplo, permitir o Gtalk, mas bloquear a transferência de arquivos por ele;

12.6.15. 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);

12.6.16. Capacidade de criação de políticas baseadas no controle por aplicação:

12.6.16.1. Por tecnologia: cliente-servidor, Browse Based, Network Protocol, etc.;

12.6.16.2. Por nível de risco da aplicação;

12.6.16.3. Por categoria e subcategoria de aplicações;

12.6.17. Baseadas em “traffic shaping” por aplicação, usuário, origem, destino, túnel VPN-IPSEC-SSL;

12.7. PROTEÇÃO IPS

12.7.1. Dispor de IPS integrado a solução de segurança;

12.7.2. Permitir o bloqueio de vulnerabilidades;

12.7.3. Permitir o bloqueio de exploits conhecidos;

12.7.4. Proteção contra ataques de negação de serviços (DoS);

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

12.7.5.1. Análise de padrões de estado de conexões;

12.7.5.2. Análise de decodificação de protocolo;

12.7.5.3. Análise para detecção de anomalias de protocolo;

12.7.5.4. Análise heurística;

12.7.5.5. IP Defragmentation;

12.7.5.6. Remontagem de pacotes de TCP;

12.7.5.7. Bloqueio de pacotes malformados;

12.7.6. Possuir assinaturas para bloqueio de ataques "buffer overflow";

12.7.7. Possuir assinaturas para auxílio no bloqueio de ataques distribuídos de negação de serviço (DDoS);

12.7.8. Possuir assinaturas e mecanismos de detecção de anomalias prontas;

12.7.9. Suportar o reconhecimento de ataques em tráfego IPv6;

12.7.10. Possibilitar a criação de assinaturas customizadas;

12.7.11. Possibilitar a criação de exceções/exclusões por hosts para determinadas assinaturas;

12.7.12. Suportar referência cruzada com CVE (Common Vulnerabilities and Exposures);

12.7.13. Possuir granularidade de ajustes com opções para sobrescrever assinaturas individualmente;

12.7.14. Suportar várias técnicas de prevenção, incluindo Drop e TCP-RST (Cliente, Servidor e ambos);

12.7.15. Suportar ações por assinaturas;

12.7.16. Suportar notificações e alertas via e-mail, whatsapp, SNMP traps e log de pacotes;

12.7.17. Suportar a captura de pacotes (PCAP) para fins de forense;

12.7.18. Análise dinâmica de ameaças do ambiente móvel e APK;

12.7.19. Não deve possuir recursos que delimitem a quantidade de bytes da sessão que será inspecionada;

12.7.20. Suportar atualização de assinaturas de ataque;

12.7.21. Possuir mecanismos que permita bloquear um ataque por expressão regular DNS;

12.7.22. Possuir autenticação em query DNS por requisição em TCP;

12.7.23. Prevenir que hosts validos sejam adicionados a blacklists por engano;

12.7.24. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing), ou garantir que esta exigência seja plenamente atendida por meio diverso;

12.8. PROTEÇÃO ANTIVÍRUS E ANTISPYWARE

12.8.1. Incluir módulo de Antivírus e Antispyware integrado na solução de segurança;

12.8.2. Permitir o bloqueio de Malwares e Spywares;

12.8.3. Capacidade de inspeção Antivírus, pelo menos, para os seguintes tipos de tráfegos: HTTP, SMTP, IMAP,POP3 e FTP;

12.8.4. Incluir proteção contra vírus em conteúdo HTML e javascript,software espião (spyware) e worms;

12.8.5. Proteção contra downloads involuntários, usando HTTP, de arquivos executáveis maliciosos;

12.8.6. Rastreamento de vírus em arquivos PDF

12.8.7. Permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, rar, etc.);

12.8.8. Suportar bloqueio de arquivos por tipo;

12.8.9. Suportar notificações e alertas via e-mail, whatsap, SNMP traps e log de pacotes;

12.8.10. Suportar a captura de pacotes (PCAP) para fins de forense;

12.9. ANÁLISE DE MALWARES MODERNOS

12.9.1. Solução ofertada deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria solução de segurança;

12.9.2. 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;

12.9.3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a escopo de proteção, tais como endereço de destino, podendo aplicar regras de exceção por assinaturas, endereço IP e/ou site;

12.9.4. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Microsoft Windows XP e versões mais novas;

12.9.5. Deve suportar a monitoração de arquivos trafegados na internet (HTTPS, HTTP, SMTP, FTP, IMAP, POP3) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

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

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

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

12.9.9. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

12.9.10. A solução deve ser fornecida em appliance local, deve possuindo, no mínimo, 10 ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;
12.9.11. Caso seja necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;
12.9.12. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

12.10. FILTRO DE URL

12.10.1. Incluir módulo de filtro de URL integrado a solução de segurança;
12.10.2. Possibilitar a configuração de políticas de filtro de URL baseado em políticas do firewall, individualizado ou agrupado por usuários, grupos de usuários, IP, redes ou zonas de segurança;
12.10.3. Incluir a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
12.10.4. Possibilitar base de URL local no appliance, evitando atrasos (delay) de comunicação/validação da URL;
12.10.5. Possuir, pelo menos, 50 categorias de URL;
12.10.6. Possibilitar a criação Categorias de URL customizadas;
12.10.7. Possibilitar a exclusão de URL do bloqueio por categoria;
12.10.8. Possibilitar a customização de página de bloqueio;

12.11. CONTROLE DE TRÁFEGO

12.11.1. Permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.
12.11.2. Controle de políticas QoS por porta, aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações, endereço de origem e de destino, individualizado ou agrupado por usuários, grupos de usuários e IP;
12.11.3. Traffic shaping QoS baseado em políticas (prioridade, garantia e máximo);
12.11.4. Com a finalidade de controlar aplicações e trafego cujo consumo possa ser excessivo, (como youtube, upstream, 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, deva 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.
12.11.5. O QoS deve possibilitar a definição de classes por:

12.11.5.1. Banda Garantida;
12.11.5.2. Banda Máxima;
12.11.5.3. Fila de Prioridade;

12.11.6. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
12.11.7. Suportar marcação de pacotes Diffserv;
12.11.8. Disponibilizar estatísticas em tempo real para classes de QoS;
12.11.9. Permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

12.11.10. Possibilitar a visualização dos países de origem e destino nos logs dos acessos;

12.12. GERAÇÃO DE LOGS

12.12.1. Os logs do produto devem incluir informações das atividades dos usuários;
12.12.2. Popular todos os logs de tráfego, IPS, URL, Data, Aplicações entre outros com as informações dos usuários;
12.12.3. Os logs de identificação de usuários devem ser feitos em tempo real (e não correlacionado após a ocorrência do tráfego em questão);
12.12.4. Deve suportar protocolo syslog, enviando as informações para um servidor syslog remoto a solução

12.13. MÓDULO VPN:

12.13.1. Suportar VPN Site-to-Site e Cliente-To-Site;
12.13.2. Suportar IPSec VPN;
12.13.3. Suportar SSL VPN;
12.13.4. Suportar atribuição de IP nos clientes remotos de VPN;
12.13.5. Suportar atribuição de DNS nos clientes remotos de VPN;

12.14. IPSEC VPN DEVE SUPORTAR:

12.14.1. 3DES, AES;
12.14.2. Autenticação MD5 e SHA-1;
12.14.3. Diffie-Hellman Group 1, Group 2 e Group 5;
12.14.4. Algoritimo Internet Key Exchange (IKE); e. AES 128, 256 (Advanced Encryption Standard);
12.14.5. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
12.14.6. Dispor de software cliente de VPN-SSL para os sistemas operacionais Windows (XP e mais novos), Linux e MacOS;
12.14.7. Permitir criar políticas para tráfego VPN-SSL;
12.14.8. SSL VPN com suporte a proxy ARP;
12.14.9. Suportar, pelo menos, 200 (duzentos) usuários simultâneos via SSL VPN; 1
12.14.10. Suporte para autenticação de VPN SSL, Ldap, Secure ID e base de dados própria;
12.14.11. Possuir interoperabilidade com, no mínimo, os seguintes fabricantes: Cisco, CheckPoint, Juniper, Palo Alto, Fortinet, SonicWall;

12.15. ROTEAMENTO E NAT

12.15.1. Suportar as seguintes funcionalidades de roteamento:

12.15.1.1. Estático e Dinâmico;
12.15.1.2. RIP v2;
12.15.1.3. OSPF;
12.15.1.4. BGP v4;

12.15.2. Suporte a roteamento IPv6;
12.15.3. Controle de políticas de redirecionamento por porta, aplicação, endereço de origem e de destino, individualizado ou agrupado por usuários, grupos de usuários e IP;

12.16. GERENCIAMENTO

12.16.1. Possuir interface “Out-Of-Band” dedicada para gerenciamento;

12.16.1.1. SSH;
12.16.1.2. HTTPS;

12.16.2. Monitoração de falha de link;
12.16.3. Suportar o gerenciamento por:

12.16.3.1. CLI via SSH;
12.16.3.2. WebUI via HTTPS;
12.16.3.3. Console;

12.16.4. O gerenciamento local do equipamento deve permitir:

12.16.4.1. Criação e administração de políticas;
12.16.4.2. Administração de políticas de IPS, Antivírus e Antispyware;
12.16.4.3. Política de Filtro de Dados e Filtro de URL;
12.16.4.4. Monitoração de logs;
12.16.4.5. Ferramentas de investigação de logs;
12.16.4.6. Debugging;
12.16.4.7. Captura de pacotes;

12.16.5. Possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;
12.16.6. Possibilidade de acessar o equipamento e aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;
12.16.7. Possibilitar gerenciamento do equipamento via protocolos SNMP, SNMP-V2 e SNMP-V3

12.17. ADMINISTRAÇÃO DO EQUIPAMENTO

12.17.1. Possibilitar a criação de diferentes profiles de administração separando, pelo menos: Leitura, Alterações, Relatórios e Monitoração;
12.17.2. Deverá ser possível de forma granular, assinar permissões para os administradores criarem outros usuários, alterarem configurações, ler configurações, etc.
12.17.3. Possibilidade de administrar o firewall localmente ou remotamente, sem causar problemas de sincronismo de configurações;
12.17.4. Habilidade de upgrade via SCP e Web-UI;
12.17.5. Suportar rollback de configuração para a última configuração salva;
12.17.6. Suportar rollback de Sistema Operacional para a última versão local;
12.17.7. Validação de regras antes da aplicação;
12.17.8. Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores, quando houver mais de um administrador executando alterações simultaneamente;
12.17.9. Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
12.17.10. Possibilitar a integração com outras soluções de SIEM de mercado (“third-party SIEM vendors”);

12.18. RELATÓRIOS

12.18.1. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos gateways de segurança;
12.18.2. Possuir relatórios de utilização dos recursos por aplicações,URL, Ameaças, etc.;
12.18.3. Prover uma visualização sumarizada de todas as aplicações, ameaças e URL que passaram pela solução;
12.18.4. Possibilidade de identificar o usuário que fez determinado acesso;
12.18.5. Possibilidade de exportar os logs CSV;
12.18.6. Possibilidade de capturar as URL acessadas para todas as sessões HTTP;
12.18.7. Gerar alertas automáticos via:

12.18.7.1. E-mail;
12.18.7.2. SNMP;
12.18.7.3. WhatsApp.

13. GESTÃO DOS EQUIPAMENTOS E SERVIÇO DE SEGURANÇA DA INFORMAÇÃO – ITENS 5 ,6, 7, 8

13.1. Os serviços deverão ser prestados remotamente, a partir de Centros de Operação de Segurança (SOC) próprios, com atendimento em Português do Brasil, de acordo com as especificações mínimas deste Termo;

13.1.1. A viabilização da operação remota será feita através de comunicação segura entre um agente de monitoramento instalado na rede da contratante, e o SOC;

13.2. Disponibilizar Central de Atendimento 0800 ou equivalente a ligação local, web e e-mail, para abertura de chamados referentes a:

13.2.1. Solicitação de mudanças no sistema de monitoramento para que este reflita mudanças na infraestrutura da Contratante;
13.2.2. Solicitação de programação de períodos de manutenção;
13.2.3. Solicitação de relatórios de histórico de eventos e métricas de performance de recursos como links de comunicação e memória;
13.2.4. Solicitação de relatório de tendências para prevenção de indisponibilidade futura;
13.2.5. Aberturas de chamados de suporte técnico à solução de segurança fornecida;
13.2.6. Disponibilizar um número de serviço, em língua portuguesa, para abertura de chamados técnicos. Este serviço deverá obrigatoriamente estar disponível 24x7;

13.3. Atuar, de forma proativa, no monitoramento e gestão de eventos de segurança 24x7, para detectar precocemente incidentes e mitigar possíveis vulnerabilidades e/ou ataques que a contratante esteja sofrendo naquele momento;
13.4. Incluir todas as licenças de software e de hardware necessárias ao perfeito e completo funcionamento das soluções ofertadas;

14. MANUTENÇÃO DE SERVIÇO E PRAZO DE ATENDIMENTO - ITENS 5, 6, 7, 8

14.1. A manutenção preventiva ou atualização dos recursos técnicos utilizados na prestação do serviço, quando necessárias interrupções programadas, deverá ser realizada através de comunicação escrita e prévia de no mínimo 7 (dias) dias úteis, a qual deverá ser agendadas com a equipe técnica da CONTRATANTE e que será efetuada no período compreendido entre 00:00 e 06:00 horas, horário de Brasília, de domingo e/ou segunda-feira.

14.2. A CONTRATADA disponibilizará um número telefônico para abertura de chamados no regime 24x7x365. Ademais, a CONTRATADA deverá providenciar uma alternativa ao chamado telefônico para o registro do chamado através de sistema Web ou e-mail.

14.3. O suporte técnico deverá ser prestado à Prefeitura de Maceió, no endereço da Secretaria Municipal de Finanças – Maceió/AL ou nas demais localidades que tenham a solução de segurança instalada;

14.4. O suporte técnico ocorrerá sem qualquer ônus para a Prefeitura de Maceió;

14.5. A Prefeitura de Maceió fará a abertura e acompanhamento de chamados técnicos por telefone 0800 e e-mail ou área em sítio da Web;

14.6. Para operacionalização do disposto anteriormente, a CONTRATADA deverá informar os números de telefone, endereços de correio eletrônico ou área em sítio da Web, disponíveis para a abertura e acompanhamento dos chamados técnicos;

14.7. O prazo de atendimento para resolução de possíveis indisponibilidade no uso dos serviços, deverá abranger três níveis de solução definitiva, quais sejam:

a) Severidade Alta: Esse nível de severidade é aplicado quando há a indisponibilidade total no uso dos serviços;

Solução Definitiva: ALTA
Indisponibilidade Total do Serviço:
1. Prazo Solução Definitiva: 2 (duas) horas

a.1. Entende-se indisponibilidade total, a prestação de serviços inaproveitáveis, conformes os seguintes parâmetros:

a.2. Quebra ou defeito dos equipamentos pertencentes a solução de segurança;

a.3. Queda total da conectividade dos serviços dependentes da solução de segurança;

b) **Severidade Média**: Esse nível de severidade é aplicado quando há falha, simultânea ou não, no uso dos serviços, estando ainda disponíveis, porém apresentando problemas;

Solução Definitiva: MÉDIA
Serviços disponíveis, mas apresentando conectividade intermitente e/ou instabilidade da solução de segurança:
2. Prazo Solução Definitiva: 3 (quatro) horas

b.1 Entende-se indisponibilidade, a prestação de serviço fora dos Níveis de Serviço, conformes os seguintes parâmetros:

b.2 Bloqueio parcial ou total de regras de segurança preestabelecidas anteriormente;

b.3 Interferência direta da solução de segurança, totalizando a latência dos circuitos dependentes da solução de 60 MS (setenta e cinco milissegundos) até 300 MS (trezentos milissegundos)

c) **Severidade Baixa**: Esse nível de severidade é aplicado para problemas que não afetem o desempenho e disponibilidade dos serviços, bem como para atualizações de software e solicitações de alteração nas configurações da solução de segurança contratada

Solução Definitiva: BAIXA
Serviços disponíveis e atualização:
3. Prazo Solução Definitiva: 4 (quatro) dias úteis

d) **Prestação de Esclarecimentos Técnicos**: é aplicado quando a CONTRATADA solicitar formalmente esclarecimentos técnicos relativos às ocorrências, ao uso e ao aprimoramento dos serviços.

Prazo de Resposta
Esclarecimentos técnicos:
4. Prazo Solução Definitiva: 4 (quatro) dias úteis

14.8. Será considerado como prazo de solução definitiva, o tempo decorrido entre a abertura do chamado técnico - efetuado por equipe técnica da Prefeitura de Maceió e a efetiva recolocação dos serviços em seu pleno estado de funcionamento;

14.9. A contagem do prazo de solução definitiva de cada chamado iniciar-se-á a partir da abertura do chamado, em um dos canais de atendimento disponibilizados pela CONTRATADA, até o momento da comunicação da resolução definitiva do problema e o aceite pela equipe técnica da Prefeitura de Maceió;

14.10. Depois de concluído o chamado, a CONTRATADA comunicará o fato à equipe técnica da Prefeitura de Maceió e solicitará autorização para o fechamento do mesmo. Caso a Prefeitura de Maceió não confirme que o problema foi de fato resolvido, o chamado permanecerá aberto até que seja efetivamente solucionado. Neste caso, a Prefeitura de Maceió fornecerá as pendências relativas ao chamado aberto;

14.11. A relação de chamados deverá estar disponível nos relatórios encaminhados mensalmente ao fiscal do contrato, atendendo aos seguintes tópicos:

14.11.1. Chamados Abertos no Período: listagem de todas as ocorrências registradas e ainda não solucionadas, durante o mês, com a indicação das ações já tomadas pela CONTRATADA;

14.11.2. Chamados Concluídos no Período: listagem de todas as ocorrências registradas e solucionadas, durante o mês, com a indicação das ações tomadas pela CONTRATADA.

14.12. O descumprimento dos prazos de atendimento implicará a aplicação de glosas conforme tabela 3:

Tabela 3: Tabela de aplicação de Glosas

Resultado esperados e níveis de qualidade exigidos	Unidade de cálculo	Fórmula de cálculo da glosa	Limite da glosa
1 – Alta	1 h	NHAT * 0,50% * VMF	10% da VMF
2 – Média	1 h	NHAT * 0,25% * VMF	10% da VMF
3 – Baixo	1 h	NHAT * 0,05% * VMF	10% da VMF
4 – Esclarecimentos	1 d	NDAT * 0,6% * VMF	10% da VMF

Onde:

VMF: Valor mensal da fatura;

NHAT: número de horas decorridas após o término de atendimento.

NDAT: número de dias decorridos após o término de atendimento.

14.13. A glosa será contada a partir do tempo decorrido e identificado no item "Prazo Solução Definitiva" de acordo com a severidade prevista no item 14.

14.14. A CONTRATADA deverá fornecer em meio eletrônico, documentação/formulário padronizado para cada solução de segurança ativada, desativada ou para cada alteração ocorrida, contendo no mínimo, os seguintes dados:

14.14.1. Código de Identificação do Acesso;
14.14.2. Número do Contrato;
14.14.3. Endereço de instalação;
14.14.4. Data de solicitação;
14.14.5. Data de ativação/desativação/alteração;
14.14.6. Valor da mensalidade.

15. GERENCIAMENTO DE SEGURANÇA - ITENS 5, 6, 7, 8

15.1. Administração da Solução: definição e implantação de políticas de acesso, regras de acesso (NAT, DNAT, Roteamento), filtros de conteúdo, IPS, GeoIP, AppControl, Botnet, VPN e Gateway Antivírus;

15.2. Realizar a função de gerência em um equipamento exclusivo;

15.3. Continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos gerenciados com o serviço de gerência;

15.4. Gerenciamento de Operação: backup de configuração (regras), aplicação de "patches" e novas atualizações de software, gerenciamento de modificações e análise de logs;

15.5. Monitoração da Solução: análise de comportamento de usuários, análise de tráfego atípico, alertas e detecção de ataques ou tentativa de invasão, incluindo "Port Scan", "Denial of Services" (DOS), e ataques de autenticação;

15.6. Ações corretivas: relacionadas a eventos de emergências as quais podem ser uma falha nos equipamentos, uma possível intrusão que possa comprometer a política de segurança da empresa, ou ainda uma não resposta dos equipamentos;

15.7. Manutenção da Solução: compreende a atualização de software e a manutenção de hardware maximizando o perfeito funcionamento dos dispositivos;

15.8. Mitigação de incidentes: ações voltadas à solução dos alertas identificados na monitoração (incluindo ataques e intrusões);

15.9. Emitir, no mínimo, alertas de:

15.9.1. Ataques de força bruta com e sem sucesso;
15.9.2. Infecção de equipamentos por vírus;
15.9.3. Comprometimento / invasão de ativos da rede;
15.9.4. Realização de ações suspeitas por parte de usuários privilegiados;
15.9.5. Alertas de operação de serviços, como interrupções e falhas;
15.9.6. Ataques de negação de serviço (DoS e DdoS);
15.9.7. Falhas de autenticação;
15.9.8. Autenticações concorrentes de múltiplas regiões ou cidades com as mesmas credenciais (roubo de identidade);
15.9.9. Ataques comuns em aplicações WEB, como XSS e SQL injection;
15.9.10. Atividades de botnets;

15.10. Identificar, em tempo real e de maneira automatizada, a origem dos eventos de segurança, identificando cidade, estados e países e não somente os endereços IP de origem;
15.11. Implantação de novas regras de segurança conforme solicitação da contratante;
15.12. Implantação de novas arquiteturas de segurança conforme solicitação da contratante;

16. RELATÓRIOS E VISIBILIDADE – ITENS 5, 6, 7, 8

16.1. Prestar esclarecimentos por escrito a Contratante, através de relatórios, sobre eventuais falhas ou interrupções de serviços;
16.2. Emitir recomendações técnicas para a melhoria da rede e da infraestrutura de segurança da Contratante.
16.3. Emitir relatórios de incidentes
16.4. Disponibilizar portal para acesso seguro WEB (através do protocolo HTTPS) disponível na plataforma de acompanhamento;

16.4.1. A Contratante deverá possuir credenciais de acesso ao portal Web do ambiente de monitoramento, para acompanhamento em tempo real de indicadores, alarmes e métricas de monitoramento;
16.4.2. Dispor de informações gráficas contendo o status, alarmes e métricas dos sistemas monitorados e a ferramenta de relatórios;
16.4.3. Possuir visões (Dashboards) pré-configuradas;
16.4.4. Permitir a criação de visões (Dashboards) conforme o perfil do usuário;
16.4.5. Ser acessível via navegadores de mercado, tais como Microsoft Internet Explorer, Google Chrome e Mozila Firefox, independente do sistema operacional do cliente;

16.5. O sistema de relatórios deve conter relatórios prontos para uso com temas sobre utilização, capacidade ou disponibilidade;
16.6. Os relatórios devem conter gráficos, tabelas ou objetos gráficos contendo dados de desempenho;
16.7. Deve permitir a geração de relatórios para adequação a requerimentos de auditoria para a norma ISO 27001:2005;
16.8. Deverão ser previstos os seguintes tipos de relatórios:

16.8.1. Relatório de utilização e filtragem WEB;
16.8.2. Relatório de ataques e incidentes de segurança;
16.8.3. Relatório de configurações;
16.8.4. Relatório com informações de classificação de eventos de segurança;
16.8.5. Relatório para consultas de eventos, logs e alarmes em tempo real;
16.8.6. Possibilidade de sumarização dos dados por hora, dia, semana ou mês;
16.8.7. Dados históricos (mínimo de 1 ano), na mesma granularidade dos demais relatórios;

16.9. Os relatórios devem permitir:

16.9.1. Acesso discriminado e controlado;
16.9.2. Emitir nos formatos Excel, CSV e PDF;
16.9.3. Ser enviados via e-mail;
16.9.4. Agendamento de relatórios;
16.9.5. Envio de relatórios pelo sistema de agendamento a usuários internos cadastrados no sistema;

16.10. Relatórios gerenciais semanais e mensais ou sob demanda de acordo com o período solicitado, incluindo:

16.10.1. Tempo total de disponibilidade/indisponibilidade de cada ativo e serviço;
16.10.2. Histórico de alertas para ativos e serviços;
16.10.3. Histórico de métricas de utilização de recursos, incluindo, canais de comunicações de dados internos e externos (Internet), CPU e Memória;
16.10.4. Relatório de disponibilidade e performance dos ativos e métricas monitoradas;
16.10.5. Classificação dos eventos de segurança (ataques, reconhecimento, malware, atividades suspeitas, etc.);
16.10.6. Eventos de segurança por direção (externo, interno e local);
16.10.7. TOP aplicações mais impactadas, TOP origens dos eventos de segurança;
16.10.8. TOP endereços de destino das ameaças;
16.10.9. TOP países e cidades de origem das ameaças;
16.10.10. TOP atacantes, vulnerabilidades, ameaças, alarmes, violações de auditoria;
16.10.11. Além dos metadados processados pela solução, deve oferecer opção de entrega dos logs originais coletados;

17. TRANSFERÊNCIA DE CONHECIMENTO – ITENS 5, 6, 7, 8

17.1. Serviço presencial de no mínimo, 24 (vinte e quatro) horas por mês;

17.1.1. Suporte presencial de vistoria e acompanhamento da solução aplicada;
17.1.2. Repasse de atividades e ações tomadas;
17.1.3. Workshops de operação e de resolução de problemas;
17.1.4. Palestras de atualização tecnológica, novos conceitos e lançamentos;
17.1.5. Apresentar plano de Treinamento de todas as partes envolvidas sobre a solução de segurança implantada, contendo Carga Horária, Conteúdo, Local e Perfil do Profissional;

18. DA IMPLANTAÇÃO, INSTALAÇÃO, CONFIGURAÇÃO E TESTES DE ACEITE DOS LINKS INSTALADOS – ITENS 1, 2,3 e 4

18.1. DA IMPLANTAÇÃO:

18.1.1. Contratante e Contratada deverão elaborar, no prazo máximo de 15 (quinze) dias úteis contados a partir do 3º (terceiro) dia útil após a assinatura do contrato, um plano conjunto de implantação gradual dos links de acesso à Internet, por ITEM;
18.1.2. A Contratante garante a contratação de 1 link de 1 Gbps e 1 Link de 300 mbps, ficando os outros links elencados neste Termo de Referência sem previsão de instalação.
18.1.3. O período de implantação total dos links de acesso à Internet elencados no Plano de Implantação será de 30 dias a partir da sua entrega formal pela Contratada:

18.1.3.1. A data de início da implantação poderá ser postergada pelo Contratante por até 60 (sessenta) dias em caso de situações que possam impactar no projeto, como, por exemplo, a realização de eleições. Em havendo essa necessidade, o Contratante

informará à Contratada durante as discussões da etapa de elaboração do Plano de Implantação;

18.1.3.2. O Plano de Implantação deverá detalhar o cronograma de instalação do link de 1 Gbps e de um link de 300 Mbps;

18.1.3.3. Até a assinatura do contrato e durante o período de implantação dos links, poderão ocorrer mudanças de endereços dos locais de instalação constantes no ANEXO A;

18.1.4. O Plano de Implantação deverá estar em conformidade com os requisitos deste Termo de Referência e seus anexos, bem como ser aprovado e assinado por ambas as partes, sendo o Contratante representado pelo Gestor do Contrato e a Contratada por seu responsável legal;

18.2. DA INSTALAÇÃO:

18.2.1. Após a fase de implantação, a Contratada realizará a instalação dos links de acesso dedicado à Internet considerando as localidades listadas no ANEXO I deste Termo de Referência;

18.2.2. A cada link de acesso dedicado à Internet está implicitamente associado o serviço de instalação com seu custo específico;

18.2.3. O fornecimento e a passagem de cabos (fiação interna para ligação entre o quadro de "distribuição geral" (DG) e a sala em que os equipamentos serão acomodados nas localidades) será de responsabilidade da Contratada;

18.2.4. A Contratada deverá fornecer os links obrigatoriamente terrestres, implementados por meio de fibra óptica;

18.2.5. Não serão permitidos acessos à Internet via satélite;

18.2.6. A Contratada deve ajustar seu plano de trabalho em conjunto com a equipe técnica do Contratante, de maneira a adequar horários e procedimentos de configuração e testes;

18.2.7. A Contratada deve recompor obras civis e pintura eventualmente afetadas quando da passagem dos cabos, mantendo o padrão local;

18.2.8. A instalação dos links de acesso à Internet será acompanhada pelas equipes de gestão e fiscalização do contrato e pela DTI/SEMGE;

18.2.9. As visitas técnicas nos locais de instalação devem ser previamente agendadas com o Contratante;

18.3. DA CONFIGURAÇÃO:

18.3.1. A Contratada será responsável pela configuração dos equipamentos necessários para o correto funcionamento do link de acesso dedicado à Internet.

18.4. Dos testes para aceitação dos links instalados:

18.4.1. Os seguintes procedimentos relacionados aos testes para aceitação dos links de acesso à Internet serão necessários:

18.4.1.1. Realização de testes de funcionamento de cada link de acesso à Internet e aprovado pela equipe técnica do Contratante;

18.4.1.2. O aceite técnico dos links instalados se dará por meio da aprovação dos seguintes testes pelo Contratante:

i. Aferição, pela equipe da Contratada, da velocidade do link instalado, tanto para download quanto para upload, em conformidade com as especificações constantes neste Termo de Referência e deverá oferecer latência máxima não superior à 60 ms, considerando a transmissão de um pacote de dados de 64 bytes, entre ponto de interconexão do serviço de acesso à internet à rede local da sede do CONTRATANTE e o nó de acesso à rede (backbone) da Contratada;

ii. Confirmação do efetivo acesso à Internet pela equipe técnica do Contratante;

iii. Verificação do desempenho, pela equipe técnica do Contratante, dos links instalados;

18.4.2. A Contratada fica responsável por viabilizar as condições para realização dos testes;

18.4.3. O link aprovado estará liberado para faturamento da sua utilização mensal;

19. GRUPO GESTOR

19.1. Para o acompanhamento do processo de contratação, implantação e operacionalização da Nova Rede Maceió, será nomeado um Grupo Gestor com a seguinte composição:

19.1.1. Diretoria de Tecnologia de Informação (DTI/SEMGE): 03 (três) servidores técnicos na área em Tecnologia da Informação;

19.1.2. Secretaria Municipal de Educação - SEMED: 02 (dois) servidores técnicos na área em Tecnologia da Informação;

19.1.3. Secretaria Municipal de Saúde - SMS: 02 (dois) servidores técnicos na área em Tecnologia da Informação;

19.2. O grupo gestor tem autonomia para aprovar e recusar n todo ou em parte os serviços prestados e atestar as notas de serviços.

20. QUALIFICAÇÃO TÉCNICA

20.1. **ITENS 1, 2,3 e 4**

20.1.1. Além dos documentos exigidos no edital, referentes à regularidade com Seguridade Social, FGTS, Fazenda Federal e ao cumprimento no disposto no art. 27, inciso V, da Lei no 8.666/1993, deverá o licitante apresentar:

20.1.1.1. Pelo menos 1 (um) atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando que prestou satisfatoriamente, serviços de comunicação de dados para acesso a Internet, incluindo instalação e manutenção, devidamente acompanhado de ART e Certidão de Acervo Técnico com Atestado (CAT) do CREA;

20.1.1.2. Apresentar 1 (uma) declaração de existência de parceria Anti DDoS;

20.1.1.3. Capacitação Técnico-Profissional, para os serviços de engenharia, através de atestado(s) de responsabilidade técnica de profissional ou profissionais pertencente(s) ao quadro permanente da Empresa, na data de apresentação da documentação de habilitação e propostas, registrado(s) pelo CREA e acompanhado das respectivas CAT’s, que comprove(m) ter sido, o(s) referido(s) profissional(ais), o(s) responsável(eis) pela execução de obras e serviços de características semelhantes, para todos os itens do objeto licitado;

20.1.1.4. Apresentar documento emitido pela ANATEL que comprove ser a PROPONENTE autorizada a prestar os serviços SCM (Serviço de Comunicação Multimídia);

20.1.1.5. Comprovar que possui estações de telecomunicação em operação no Estado de Alagoas através da apresentação de cópia da licença de autorização de funcionamento de estação emitido pela Anatel (Agência Nacional de Telecomunicações);

20.1.1.6. Apresentar o projeto técnico da solução proposta, onde constem as informações dos equipamentos utilizados, detalhamento da infraestrutura e circuitos de acesso, onde sejam representados os nós de acesso à rede (backbone) da CONTRATADA, de acordo com as características técnicas do serviço;

20.1.1.7. Visto a grande complexidade e o alto grau de criticidade do ambiente e tecnologias envolvidas, com o objetivo de garantir a perfeita execução dos serviços requeridos neste termo de referência, o PROPONENTE, para efeito de comprovação da capacitação técnica, deverá entregar no envelope de habilitação documentação que comprove possuir equipe técnica composta pela quantidade de profissionais certificados e/ou documentação que comprove o compromisso de contratação de profissionais com a certificação e na quantidade especificada. Neste caso devem ser apresentados:

20.1.1.7.1. currículo do profissional;

20.1.1.7.2. Certificação obrigatória com data de validade com no mínimo 30 dias após a data de abertura do certame licitatório;

20.1.1.7.3. Declaração assinada, com firma reconhecida pelo profissional indicado, declarando estar ciente de sua indicação pela PROPONENTE para a prestação dos serviços, comprometendo-se a compor a equipe da PROPONENTE, caso esta venha a ser a vencedora.

20.1.1.8. Comprovação do serviço Anti-DDoS através de apresentação de declaração da empresa fornecedora e cópia de contrato com Scrubbing Center no Brasil onde este comprove:

20.1.1.8.1. possuir no mínimo 1 centro de limpeza nacional e 3 centros de limpeza internacional com capacidade de ingestão igual ou superior ao descrito no no Termo de Referência;

20.1.1.8.2. possuir aderência a todos os parâmetros técnicos descritos no no Termo de Referência.

20.1.1.9. Para licitante que possua Scrubbing Center no Brasil próprio, apresentar declaração do fabricante da solução Anti-DDoS proposta, comprovando que a solução atende as especificações do Termo de Referência;

20.1.1.10. A ARREMATANTE deverá apresentar documentação técnica da solução, descrevendo:

20.1.1.10.1. diagrama de fornecimento da solução;

20.1.1.10.2. relação detalhada de equipamentos ativos que serão fornecidos e instalados, indicando marca e modelo de cada equipamento;

20.1.1.10.3. cronograma detalhado de execução da implantação inicial;

20.1.1.10.4. projeto de encaminhamentos e implantação inicial do serviço, indicando trajeto da(s) fibra(s) óptica(s) entre o backbone da rede da LICITANTE até o edifício-sede da CONTRATANTE;

20.1.1.11. A ARREMATANTE deverá apresentar documentos de especificações técnicas oficiais dos fabricantes que comprovem que os equipamentos da solução fornecida atende integralmente aos requisitos exigidos no Termo de Referência e neste edital;

20.2. ITENS 5, 6, 7, 8

20.2.1. 01(um) profissional certificado/treinado na solução de gerenciamento / monitoramento proposta para a prestação dos serviços de gerenciamento / monitoramento, pelo fabricante do equipamento;

20.2.2. 01 (um) profissional certificado na solução objeto deste termo, pelo fabricante do equipamento.

20.3. **COMPROVAÇÃO DE VÍNCULO**

20.3.1. A comprovação do vínculo da equipe técnica com a CONTRATADA dar-se-á mediante a apresentação da CTPS, contrato social, livro de registro ou documento que substitua legalmente a CTPS. Não serão aceitos contratos de prestação de serviços com profissionais terceirizados, devendo este(s) profissional (ais) ser (em) o(s) responsável (eis) pela execução dos serviços e pertencer(em) ao quadro permanente da CONTRATADA.

20.4. DEVERES E RESPONSABILIDADE DA CONTRATADA:

20.4.1. Assumir inteira responsabilidade pelos serviços.

20.4.2. Submeter à aprovação da Prefeitura Municipal de Maceió toda e qualquer alteração ocorrida nas especificações, em face de imposições técnicas, de cunho administrativo legal.

20.4.3. Não transferir, total ou parcialmente, os direitos e obrigações vinculadas à contratação.

20.4.4. Sujeitar-se à fiscalização da Prefeitura Municipal de Maceió, no tocante à verificação das especificações exigidas neste Termo de Referência, prestando todos os esclarecimentos solicitados e atendendo às reclamações procedentes, caso ocorram.

20.4.5. Responder por perdas e danos que vier a sofrer a Prefeitura Municipal de Maceió ou terceiros, em razão de sua ação ou omissão, dolosa ou culposa, independentemente de outras cominações contratuais ou legais a que estiver sujeita, garantido o contraditório e a ampla defesa, nos termos da legislação aplicável.

20.4.6. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários no objeto licitado, até o limite previsto no § 1º do art. 65 da Lei nº 8.666/1993.

20.4.7. Assegurar a execução dos serviços de assistência técnica aos equipamentos e acessórios, quando necessários, garantindo o perfeito funcionamento durante a vigência do contrato.

20.4.8. Substituir os equipamentos recusados ou que apresentem vícios redibitórios durante o período de prestação de serviços, de forma a garantir a disponibilidade da conexão conforme previsto neste Termo de Referência.

20.5. DEVERES E RESPONSABILIDADE DA CONTRATANTE

20.5.1. No ato da assinatura do contrato, a CONTRATANTE deverá indicar os locais de instalação dos equipamentos;

20.5.2. Efetuar os pagamentos devidos à CONTRATADA, nas condições estipuladas neste Termo de Referência;

20.5.3. Designar Gestor (es) do Contrato que será(ão) o(s) representante(s) da CONTRATANTE junto à CONTRATADA;

20.5.4. Notificar à CONTRATADA qualquer irregularidade constatada na entrega dos equipamentos;

20.5.5. Proporcionar todas as condições para que a CONTRATADA possa executar fielmente o objeto desta contratação.

21. DA PROVA DE CONCEITO

21.1. Declarado provisoriamente o vencedor do Certame, o Pregoeiro irá suspender a sessão pública para realização de PROVA DE CONCEITO (POC). A prova visa averiguar de forma prática os requisitos descritos neste edital.

21.2. A prova ocorrerá nas dependências da CONTRATANTE, DTI/SEMGE.

21.3. A prova será convocada com antecedência mínima de 02 (dois) dias úteis da data agendada para a sua realização.

21.4. A Prova terá duração máxima de até 1 (um) dia útil.

21.5. A prova será executada e julgada pelos membros da Equipe de Apoio da Licitação, formada por técnicos da DTI/SEMGE.

21.6. Toda a infraestrutura de hardware e software necessária para demonstração do atendimento aos requisitos é de responsabilidade da LICITADA, assim como as massas de dados necessárias para a demonstração.

21.7. Cabe à LICITANTE apenas a disponibilização do local para realização da prova prática de conceito.

21.8. A LICITADA será considerado reprovado nas seguintes condições:

21.8.1. Não comparecimento para execução da prova na data e hora marcada;

21.8.2. Não atendimento (total ou parcial) de algum item constante dos requisitos funcionais da solução, durante a Prova de Conceito.

21.8.3. Caberá à LICITANTE pronunciar-se sobre a conformidade da proposta com os requisitos exigidos, da referida Prova e será divulgado em ato público.

21.9. Para a Prova de Conceito – POC será considerado requisitos funcionais apresentação de solução que contemple os requisitos:

21.9.1. A LICITADA deverá disponibilizar à Prefeitura de Maceió um portal na Internet, para acompanhamento dos níveis de serviços prestados em tempo real;

21.9.2. A LICITADA deverá fornecer pelo menos 4 (quatro) usuário/senha para acesso ao portal de acompanhamento dos serviços de Internet e Segurança;

21.9.3. O portal de acompanhamento dos serviços deverá possibilitar que sejam visualizados e impressos os relatórios das informações de desempenho do link de conectividade;

21.9.4. Deverá ser fornecido, mensalmente, relatório contendo os registros das ocorrências no referido período;

21.9.5. A LICITADA deverá divulgar, no portal de acompanhamento dos serviços, relatórios detalhando os valores das medições dos parâmetros de qualidade do link de conectividade, conforme detalhamento deste Termo de Referência. Devem ser feitas medições a cada 5 (cinco) minutos. Para cada medição o relatório deve apresentar pelo menos os seguintes valores:

21.9.5.1. Dia e hora da medição;

21.9.5.2. Total de pacotes trafegados;
21.9.5.3. Total de pacotes com erros;
21.9.5.4. Latência nédia do intervalo de 5 minutos de coleta;

21.9.6. Suportar notificações e alertas via e-mail, Whatsapp, SNMP traps e log de pacotes;

21.9.7. A licitante deverá simular a abertura de chamado por Tefone 0800, e-mail e por área no em sítio da Web;

21.9.8. Para operacionalização do disposto anteriormente, a LICITADA deverá informar os números de telefone, endereços de correio eletrônico e área em sítio da Web, disponíveis para a abertura e acompanhamento dos chamados técnicos;

21.9.9. A relação de chamados deverá estar disponível nos relatórios encaminhados mensalmente ao fiscal do contrato, atendendo aos seguintes tópicos:

21.9.9.1. Chamados Abertos no Período: listagem de todas as ocorrências registradas e ainda não solucionadas, durante o mês, com a indicação das ações já tomadas pela LICITADA;
21.9.9.2. Chamados Concluídos no Período: listagem de todas as ocorrências registradas e solucionadas, durante o mês, com a indicação das ações tomadas pela LICITADA.
21.9.9.3. A LICITADA deverá fornecer em meio eletrônico, documentação/formulário padronizado para cada circuito ativado, desativado ou para cada alteração ocorrida, contendo no mínimo, os seguintes dados:

21.9.9.3.1. Código de Identificação do Acesso;
21.9.9.3.2. Número do Contrato;
21.9.9.3.3. Endereço do Ponto de Acesso;
21.9.9.3.4. Velocidade de Acesso;
21.9.9.3.5. Data de solicitação do circuito;
21.9.9.3.6. Data de ativação/desativação/alteração do circuito;

21.9.9.3.7. Tipo/padrão de interface utilizada no circuito;
21.9.9.3.8. Meio de transmissão utilizado;
21.9.9.3.9. Valor da mensalidade.
21.9.9.3.10. Disponibilizar um número de serviço, em língua portuguesa, para abertura de chamados técnicos. Este serviço deverá obrigatoriamente estar disponível 24x7;

22. DO CRITÉRIO DE AVALIAÇÃO DAS PROPOSTAS

22.1. O Critério de avaliação das propostas orçamentárias apresentadas pelas empresas concorrentes deverá ser o de menor preço por grupo de itens;

22.2. A opção por se agrupar os equipamentos e serviços se justificar por:

22.2.1. Se tratarem de itens da mesma natureza e serem estes inter-relacionados;
22.2.2. Pela dinamização do processo de execução e uniformização dos serviços, fiscalização dos serviços e gestão da Ata de Registro de Preços
22.2.3. Coaduna com o interesse público de atingir os melhores preços em possíveis negociações;
22.2.4. Pela inexistência de prejuízo ao caráter competitivo do certame
22.2.5. Pela importunidade de contratação de múltiplos licitantes

23. CONDIÇÕES GERAIS

23.1. Deverão estar inclusos no preço proposto todos os equipamentos necessários para a implementação da rede objeto do edital, incluindo o aluguel de equipamentos, roteadores, obras de adequação, etc;

23.2. Deverão estar inclusos no preço proposto, os custos de manutenção de todos os circuitos e equipamentos;

23.3. Os proponentes deverão garantir em suas propostas a concessão automática de descontos nos valores mensais, em decorrência de interrupções nos serviços contratados, desde que não atribuíveis ao CONTRATANTE;

23.4. Em caso de futura necessidade de mudança de endereço de qualquer acesso da rede, após esta ter sido implantada, a CONTRATADA fica obrigado a executar e concluir a transferência dos equipamentos e do circuito de dados e ativar o acesso da rede IP no novo endereço em um prazo máximo de 30 (trinta) dias corridos, desde que a alteração seja para endereço dentro dos limites urbanos da mesma cidade onde o circuito se encontra instalado. No caso do não cumprimento deste prazo, será aplicada multa diária de 5% (cinco por cento) sobre o valor do circuito.

24. DA VIGÊNCIA

24.1. O prazo da contratação será de 36 (trinta e seis meses), podendo ser renovado, por sucessivos períodos, caso haja interesse das partes, até o limite de 60 (sessenta) meses, nos termos do art. 57, II, da Lei 8.666/93.

25. LOCAL DA INSTALAÇÃO

25.1. O serviço contratado deverá ser instalado na sede da Diretoria de Tecnologia da Informação, localizado na Rua Pedro Monteiro, nº 47, bairro Centro, CEP: 57020-380, Maceió-AL. E nas unidades constantes no ANEXO A deste termo.

_____

Fernando Antônio Dantas Gomes Pinto
Diretor de Tecnologia da Informação / SEMGE

_____

Felipe Gomes de Oliveira
Coordenador Geral de Controle e Acompanhamento de Serviços / SEMGE

_____

Marlo Cezar de Aleluia
Gerência de Rede / SEMGE

_____

João Geraldo de Oliveira Lima
Coordenador Geral de Desenvolvimento de Projetos / SEMGE

_____

José Romulo Ribeiro da Silva

Coordenador de TI/SMS

_____

José Max Deivys Alves de Moura
Coordenador TI/SEMED

_____

Marcelo Santos Silva
Analista Sistema/SEMAS

ANEXO A

POSSÍVEIS LOCAIS DE INSTALAÇÃO DOS LINKS DE INTERNET

Nº	SIGLA	ENDEREÇO
1	SEMGE/DTI	Rua Pedro Monteiro, 5, Centro. CEP 57020-150
2	SEMAS	Rua Melo Moraes, 63, Centro. CEP 57020-330
3	SECOM	Rua Jangadeiros Alagoanos, Pajuçara, Nº 1481. CEP: 57030-000 2º andar da Galeria Città office
4	SMCI	Av. Aristeu de Andrade, 406, Farol. CEP 57051-090
5	SEMED	Rua General Hermes, 1199, Cambona. CEP 57017-000
6	SEMELJ	Sede administrativa: Rua São Francisco de Assis, 305, Jatiúca
7	SEMELJ	Vila Olímpica: Av. Alice Karoline, 43, Cidade Universitária
8	SEMEC	Rua Pedro Monteiro, nº 47, Centro - Maceió/AL. CEP: 57020-380
9	SMG	Rua Desembargador Almeida Guimarães, 87, Pajuçara, Maceió – AL. CEP: 57030-16
10	SMHPS	Rua Voluntário da Pátria, 102, Centro. CEP 57020-410
11	SEMINFRA	Rua do Imperador, 307, Centro. CEP 57023-060
12	GGOV	- Rua Marquês de Abrantes, s/n, Bebedouro. CEP 57018-655
13	SEMPLA	Praça Visconde de Sinimbu, 141, Centro. CEP.: 57020-670
14	GP/SMG	Rua Desembargador Almeida Guimarães, 87, Pajuçara, Maceió – AL. CEP: 57030-160
15	PGM	Rua Dr. Pedro Monteiro, 291, Centro. CEP 57020-380

16	SMS	Rua Dias Cabral, 569, Centro. CEP 57020-250
17	SEMSC	Avenida Theobaldo Barbosa, s/n, Conjunto Joaquim Leão, Vergel. CEP 570145-10
18	SEMTABES	Rua Barão de Anadia, 85, Centro. CEP 57020-630
19	SEMPTUR	Avenida da Paz, 1422, Centro. CEP 57020-440
20	GVP	Rua Jornalista Lafaiete Belo, 47, Poço. CEP 57025-690
21	COMARHP	Rua General Hermes, 281, Cambona. CEP 57017-010
22	FMAC	Av. da Paz, 900, Jaraguá. CEP 57025-050
23	COMDEC	Avenida Governador Afrânio Lages, 297, Farol. CEP 57050-015
24	IPREV	Rua Comendador Palmeira, 502, Farol. CEP 57051-150
25	SMTT	Avenida Durval de Góes Monteiro, 829, KM 10, Tabuleiro do Martins. CEP 57061-000
26	SEDET	Avenida Governador Afrânio Lages, 297, Farol CEP 57050-015
27	SLUM	Praça Ciro Acioly, 96, Ponta Grossa. CEP 57014-710
28	SIMA	Rua Marquês de Abrantes, s/n, Bebedouro. CEP 57018-330

Obs.: Estes endereços podem sofrer alterações dentro da conveniência e necessidade da Contratante.

Obs2.: Os endereços confirmados de instalação do link de 1Gb é o Nº1 e o link de 300 Mb é o Nº 16.

ANEXO B

GRUPO DE CNPJ DA PREFEITURA MUNICIPAL DE MACEIÓ

No.	NOME	CNPJ
1	PREFEITURA DE MACEIÓ	12.200.135/0001-80
2	SECRETARIA MUNICIPAL DE SAÚDE	00.204.125/0001-33
3	SECRETARIA MUNICIPAL DE SAÚDE	00.204.125/0002-14
4	SECRETARIA MUNICIPAL DE EDUCAÇÃO	19.406.627/0001-75
5	SECRETARIA MUNICIPAL DE GESTÃO	18.113.955/0001-10
6	SECRETARIA MUNICIPAL DE ASSISTÊNCIA SOCIAL	15.369.322/0001-80

ANEXO C

PROPOSTA DE PREÇO

	ITEM	SERVIÇOS	VELOCIDADE	QUANT.	NÚMEROS IP-V4	NÚMEROS /64 IP-V6	PAGAMENTO	VALOR UNITÁRIO / MÊS	VALOR TOTAL
	1	Link dedicado de conectividade com a Internet com velocidade de 1 Gbps, suporte completo para roteamento dos protocolo IPV4 e IPV6 e velocidades simétricas para *upstream* e *downstream*.	1 Gbps *Full*	1	30	1	Mensal		
		Link dedicado de conectividade	300 Mbps	5	20		Mensal		

	2	com a Internet com velocidade de 300 Mbps, suporte completo para roteamento dos protocolo IPV4 e IPV6 e velocidades simétricas para *upstream* e *downstream*.							
	3	Link dedicado de conectividade com a Internet com velocidade de 200 Mbps, suporte completo para roteamento dos protocolo IPV4 e IPV6 e velocidades simétricas para *upstream* e *downstream*.	200 Mbps	5	10		Mensal		
	4	Link dedicado de conectividade	50 Mbps	15	10		Mensal		

		com a Internet com velocidade de 50 Mbps, suporte completo para roteamento dos protocolo IPV4 e IPV6 e velocidades simétricas para *upstream* e *downstream*.							
	ITEM	DESCRIÇÃO	QUANTITATIVO						
	5	Solução para atuar, de forma proativa, no monitoramento e gestão de eventos de segurança para detectar precocemente incidentes e mitigar possíveis vulnerabilidades e/ou ataques que a Prefeitura esteja sofrendo naquele	2						

		momento, incluindo solução de equipamentos (hardwares) e seus programas (softwares), objetivando uma melhor integração entre os equipamentos e os serviços já existentes,			
	6	Solução para atuar, de forma proativa, no monitoramento e gestão de eventos de segurança para detectar precocemente incidentes e mitigar possíveis vulnerabilidades e/ou ataques que a Contratante	1		

		esteja sofrendo naquele momento, incluindo solução de equipamentos (hardwares) e seus programas (softwares), objetivando uma melhor integração entre os equipamentos e os serviços já existentes, para um link de 300 Mbps			
	7	Solução para atuar, de forma proativa, no monitoramento e gestão de eventos de segurança para detectar precocemente incidentes e mitigar	0		

		possíveis vulnerabilidades e/ou ataques que a Contratante esteja sofrendo naquele momento, incluindo solução de equipamentos (hardwares) e seus programas (softwares), objetivando uma melhor integração entre os equipamentos e os serviços já existentes, para um link de 200 Mbps			
	8	Solução para atuar, de forma proativa, no monitoramento e gestão de eventos de segurança para	0		

		detectar precocemente incidentes e mitigar possíveis vulnerabilidades e/ou ataques que a Contratante que esteja sofrendo naquele momento, incluindo solução de equipamentos (hardwares) e seus programas (softwares), objetivando uma melhor integração entre os equipamentos e os serviços já existentes, para um link de 50 Mbps			
SUBTOTAL ITEM 1 (R$)					
SUBTOTAL ITEM 2 (R$)					

SUBTOTAL ITEM 3 (R$)	
SUBTOTAL ITEM 4 (R$)	
SUBTOTAL ITEM 5 (R$)	
SUBTOTAL ITEM 6 (R$)	
SUBTOTAL ITEM 7 (R$)	
SUBTOTAL ITEM 8 (R$)	
SUBTOTAL DA SOMA DE ITENS X 12 MESES (R$)	
TOTAL DA PROPOSTA	

* Escreva (Não participar) no item que a empresa não irá participar da proposta