TERMO DE REFERÊNCIA
DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA

1. OBJETO

1.1. Constitui objeto deste Termo de Referência a contratação, por 12 (doze) meses, renováveis por igual de solução de segurança suportada por uma plataforma integrada com um equipamento Next Generation Firewall a fim de gerenciar e controlar acessos e o fluxo de dados cibernéticos através dos links de internet utilizados na autarquia, e a fim de garantir controles que satisfaçam as necessidades de segurança cibernética**.**

2. JUSTIFICATIVAS

2.1. A SAMA possui uma estratégia de segurança em camadas no que diz respeito a segurança da informação e segurança cibernética, e faz parte dessa estratégia uma solução de Firewall, solução esta que deve implementar a segurança necessária para prover um controle de entrada e saída de dados através das conexões de internet utilizadas na autarquia.

2.2. O Departamento de Tecnologia da Informação opta pela utilização de sistemas que, não só concedam o acesso à web, mas possuam funcionalidades que garantam o devido tipo de acesso de acordo com as definições administrativas e ofereçam fortes níveis de segurança.

2.3. São controles necessários: o acesso à Internet; antivírus de borda, que nos garante uma primeira barreira de segurança contra ameaças provenientes da Internet; Serviços de Prevenção a Intrusão, que realizam a detecção de possíveis tentativas de invasão à rede da SAMA; Filtro de Conteúdo, que bloqueia ou permite o acesso dos computadores a sites da internet de acordo com as definições administrativas do SAMA; Serviço de NAT, que redireciona os acessos provenientes da Internet para hosts determinados; Logs de acessos; VPN (Virtual Private Network), dentre outros.

3. RESULTADOS A SEREM ALCANÇADOS

3.1. Garantia do controle de segurança no fluxo de dados trafegados de e para a internet a partir da rede interna da SAMA.

3.2. Melhores índices de disponibilidade dos recursos de TI devido à minimização de impactos causados por possíveis cyber-ataques.

3.3. Monitoramento adequado de ameaças oriundas da web que possam invadir a rede da SAMA, a fim de que estas sejam barradas de forma efetiva.

3.4. Obter suporte adequado para gerenciamento, necessidade de melhoramentos, dúvidas de utilização e resolução de problemas.

4. AMBIENTE COMPUTACIONAL

4.1. Os serviços devem ser dimensionados para atender uma estrutura de rede com aproximadamente 50 usuários/computadores.

4.2. A SAMA utiliza-se de um link dedicado de internet com velocidade de 400 Mbps.

4.3. Um segundo link pode vir a ser contratado pela SAMA a fim de obter redundância no acesso aos serviços de internet.

5. SERVIÇO GERENCIADO DE SEGURANÇA

5.1. ESPECIFICAÇÕES DOS SERVIÇOS DA SOLUÇÃO

5.1.1. Contratação de empresa especializada para fornecimento de hardware, licenças e serviços de **MSS (*Managed Security Services*)**, contemplando instalação, configuração, manutenção, suporte técnico remoto e local, monitoramento e gerenciamento.

6. CARACTERÍSTICAS DOS SERVIÇOS

6.1. SOLUÇÃO DE GERENCIAMENTO COM FORNECIMENTO DE HARDWARE E SOFTWARE

6.1.1. A CONTRATADA deverá fornecer, em regime de comodato, conforme descrito em **ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO**, solução necessária para a realização dos serviços, para a solução ofertada durante a vigência do contrato.

6.1.2. A solução de hardware e software deverá ser compatível com o ambiente operacional da CONTRATANTE.

6.1.3. A CONTRATADA será responsável pela manutenção preventiva e corretiva da solução de hardware e software, sem qualquer ônus para a CONTRATANTE.

6.1.4. Poderá haver redimensionamento das capacidades de hardware e/ou software durante a vigência do contrato em razão de necessidades na estrutura de CONTRATANTE.

6.2. MONITORAMENTO / GERENCIAMENTO / MANUTENÇÃO

6.2.1. O gerenciamento deverá ser em regime de operação 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, inclusive feriados, sobre os serviços, garantindo o melhor resultado nas aplicações da CONTRATANTE e deverá abranger as atividades de manutenção, supervisão e administração, sendo que a abertura de tickets de suporte técnico deverá funcionar de segunda-feira a sexta-feira das 08:00 às 18:00.

6.2.2. O NOC deverá efetuar abertura de chamado junto as operadoras dos links de internet em caso de incidentes.

6.2.3. Enviar relatório mensal, com a quantidade de incidentes de cada link e com informativo de indisponibilidade.

6.2.4. A CONTRATADA deverá efetuar o backup diário das configurações lógica dos firewalls.

6.2.5. A CONTRATADA deverá enviar mensalmente o Relatório de Firewall com um resumo executivo da usabilidade dos usuários.

6.3. SERVIÇO DE COMUNICAÇÃO DE DADOS

6.3.1. A CONTRATADA deverá realizar as configurações necessárias para interligação de seu SOC/NOC (*Security Operation Center* - Centro de Operações de Segurança / *Network Operation Center* - Centro de Operações de Rede) às instalações do CONTRATANTE, por meio de uma linha de comunicação privativa de dados (LP) ou através de uma VPN, com a finalidade exclusiva de realizar a prestação do serviço, durante a vigência do contrato.

6.3.2. Todo acesso de monitoração do ambiente, e eventuais intervenções remotas, pela CONTRATADA deverão ser feitos exclusivamente por esse serviço de comunicação de dados.

6.4. INFRAESTRUTURA MÍNIMA NECESSÁRIA.

6.4.1. Responsabilidades do SOC/NOC

6.4.2. A Infraestrutura do SOC/NOC da CONTRATADA deve possuir mecanismos de segurança física e lógica necessários para garantir a segurança das informações e do ambiente operacional, incluindo:

6.4.3. Segurança física: mecanismos de monitoração e registro de todo e qualquer acesso ao SOC/NOC, utilizando-se de câmeras de segurança;

6.4.4. Acesso ao SOC/NOC controlado por mecanismos de autenticação forte (pelo menos autenticação de dois fatores); ambiente isolado de outros que não sejam destinados à operacionalização e controle de segurança;

6.4.5. Mecanismos de prevenção, detecção e combate a incêndios;

6.4.6. Política de acesso lógico: possuir autenticação forte no acesso aos equipamentos que estarão nas dependências da CONTRATANTE, com usuários segregados por função e registros para controle de auditoria;

6.4.7. Possuir políticas definidas para criação, exclusão e manutenção de chaves, senhas e perfis de acesso.

6.5. O SOC/NOC DA CONTRATADA DEVE POSSUIR COMPETÊNCIA PARA A PRESTAÇÃO DE SERVIÇOS, **SENDO**:

6.5.1. MANUTENÇÃO

6.5.1.1. Fornecer apoio técnico necessário para realizar o diagnóstico de eventos de falha em seus ativos de segurança. Através da análise dos logs do equipamento, o SOC/NOC deverá determinar se houve alguma avaria em um dos componentes de hardware da solução e identificar a necessidade ou não de sua substituição.

6.5.1.2. Efetuar o processo de RMA (sigla em inglês de *return merchandise authorization*).

6.5.1.3. Efetuar quando necessário toda a interface com o fabricante, para o RMA e substituição do componente danificado.

6.6. SUPERVISÃO

6.6.1. Efetuar o monitoramento constante da capacidade e da disponibilidade da infraestrutura de segurança contratada.

6.6.2. Compreender as atuais demandas sobre os recursos de segurança e criar previsões para futuras solicitações quando necessário.

6.6.3. Avaliar se o nível de disponibilidade é sustentável, permitindo o negócio atingir seus objetivos de forma consistente.

6.6.4. Identificar que o componente atingiu certo nível de utilização (threshold).

6.6.5. Alertar e encaminhar para os técnicos responsáveis pela administração.

6.6.6. Acompanhar a saúde dos dispositivos supervisionando-os 24x7.

6.6.7. Comunicar à CONTRATANTE, anomalias quando um componente monitorado apresentar índices não usuais.

6.6.8. Prover a monitorização da saúde dos dispositivos através de um número predefinido de itens, conforme abaixo:
6.6.9. Utilização da CPU;
6.6.10. Utilização de memória;
6.6.11. Utilização do disco;
6.6.12. Estado das interfaces de rede;
6.6.13. Temperatura;
6.6.14. Número de sessões de VPN;
6.6.15. Número de pacotes perdidos;
6.6.16. Número de pacotes negados;
6.6.17. Número de conexões;
6.6.18. Estado de serviços.
6.6.19. Estas verificações deverão ser ativadas no momento de implantação do serviço, utilizando definições padrão de *thresholds*.
6.6.20. Estes valores poderão ser ajustados caso necessário, a fim de identificar quais situações normalmente não correspondem à normalidade dos serviços.

6.7. ADMINISTRAÇÃO

6.7.1. Realizar a operação remota, gestão de mudança e gestão de configuração dos dispositivos de segurança contratado.
6.7.2. Resolução nos incidentes de segurança que ocorrem nos elementos administrados, detectados pelo monitoramento ou que sejam informados pela CONTRATANTE.
6.7.3. Planejar e realizar implementação de mudanças no ambiente contratado e gerenciado, sejam elas solicitadas pela CONTRATANTE ou mesmo por recomendação da própria CONTRATADA, baseados nas melhores práticas de gestão.
6.7.4. Efetuar alterações em configurações e políticas de segurança (regra de firewall, alerta IPS, antivírus gateway, filtro web etc.).
6.7.5. Efetuar tarefas operacionais básicas, tais como executar *backup/restore* de configurações e gerenciamento do ambiente contratado.
6.7.6. Garantir o correto funcionamento dos dispositivos administrados.
6.7.7. Manter e atualizar o ambiente contratado com o software do dispositivo na versão mais atual recomendada pelo fabricante.
6.7.8. Efetuar aplicação de patches para a resolução de incidentes, correção de vulnerabilidades e prevenção de incidentes de segurança.
6.7.9. Efetuar atualização de software e patches somente se e quando autorizada pela CONTRATANTE, através do processo de gestão da mudança.
6.7.10. Informar à CONTRATANTE dos possíveis riscos de segurança identificados através da administração da infraestrutura ou através das ferramentas de administração.
6.7.11. Atender as dúvidas e solicitações de segurança da CONTRATANTE.
6.7.12. Acompanhar e encaminhar os chamados através de ferramenta.
6.7.13. Acompanhar tendências de ataques e vulnerabilidades.
6.7.14. Os técnicos da CONTRATANTE devem ter acesso à ferramenta para administração conjunta após serem treinados pela CONTRATADA.

6.8. IMPLANTAÇÃO DA SOLUÇÃO:

6.8.1. A implantação da solução de hardware e software deverá ser realizada no prazo de até 30 (trinta) dias da contratação, mediante entrega de cronograma, detalhando as fases do projeto de implantação e com analista presencial na sede da SAMA. Esse cronograma deverá ser aprovado pela CONTRATANTE, sendo a implantação iniciada somente após esta aprovação.

6.8.2. Este prazo pode ser prorrogado por igual período mediante apresentação de justificativa plausível.

6.8.3. A infraestrutura para instalação da solução (energia elétrica, sistema de aterramento, rack para acomodar equipamentos, cabeamento estruturado, sistema de refrigeração, entre outros) é de responsabilidade da CONTRATANTE.

6.8.4. As fases do projeto, bem como os respectivos documentos mínimos necessários para cada fase, estão descritas a seguir:

6.8.4.1. A implantação da solução será realizada pela CONTRATADA e o planejamento e a execução de todas as atividades envolvidas serão acompanhados, autorizados e coordenados por servidores designados pela CONTRATANTE.

6.8.4.2. A implantação da solução, quando realizada no ambiente de produção, poderá envolver, a critério da CONTRATANTE, atividades fora do horário de expediente (horários noturnos ou em finais de semana e feriados).

6.8.4.3. A CONTRATADA será responsável por efetuar as atividades de integração da solução ofertada com o ambiente operacional da CONTRATANTE, sem provocar qualquer prejuízo aos serviços desta.

6.8.4.4. Após a implantação da solução e estando tudo de acordo com este Termo de Referência, a CONTRATANTE irá emitir o termo de aceite da implantação.

7. PRESTAÇÃO DOS SERVIÇOS

7.1. Os serviços serão realizados pela CONTRATADA na modalidade 24x7x365 (vinte e quatro horas por dia, sete dias na semana, 365 dias por ano).

7.2. CONTROLE DOS SERVIÇOS REALIZADOS PELA CONTRATADA

7.2.1. Para o controle e administração dos serviços realizados pela CONTRATADA, a CONTRATANTE indicará pelo menos 01 (um) representantes autorizados a interagir com aquela. Tais representantes serão responsáveis por:

7.2.1.1. Manter as informações técnicas (configuração do ambiente) atualizadas, bem como dar suporte na implantação e manutenção da solução;

7.2.1.2. Definir as estratégias, políticas e regras a serem implantadas, e analisar/aprovar as solicitações;

7.2.1.3. Tomar as providências necessárias, em caso da ocorrência de algum incidente (análise dos logs, rastreamento da ocorrência).

7.2.2. A CONTRATANTE poderá indicar até 2 (dois) técnicos para a administração da solução.

7.2.3. A CONTRATANTE poderá realizar inspeção nas instalações do SOC/NOC da CONTRATADA, a qualquer tempo, com o objetivo de verificar a segurança física e lógica do ambiente.

7.3. OCORRÊNCIA DE INCIDENTES

No caso de detecção de algum incidente de segurança, a CONTRATADA deverá notificar a CONTRATANTE dentro do período estabelecido no SLA, para que sejam tomadas as medidas corretivas e legais necessárias.

São considerados incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade ou a disponibilidade dos serviços da CONTRATANTE.

A CONTRATADA comunicará imediatamente a CONTRATANTE, para que possam ser tomadas ações preventivas, nos casos de tentativas, sem sucesso, de acessos indevidos, de instalação de códigos maliciosos, ou de qualquer outra ação que venha pôr em risco a segurança do ambiente da CONTRATANTE, em que seja evidenciada a insistência, por parte da pessoa mal-intencionada.

7.3.1. A CONTRATADA disponibilizará todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs etc.) para que sejam apurados os incidentes de segurança reportados.

7.4. ENCERRAMENTO DOS SERVIÇOS DE MONITORAÇÃO REMOTA DA SEGURANÇA

7.4.1. Quando do encerramento da prestação do serviço de monitoração remota da segurança, a CONTRATADA retirará os componentes da solução.

7.4.2. Todas as informações de customização, políticas e regras, logs de auditoria serão disponibilizadas para a CONTRATANTE e, em seguida, eliminadas da base de dados da CONTRATADA.

7.5. CONFIDENCIALIDADE DA INFORMAÇÃO.

7.5.1. Todas as informações que trafegam nos equipamentos, bem como todas e quaisquer informações originadas pela CONTRATANTE, que a CONTRATADA venha a ter acesso serão consideradas “Informações Confidenciais”.

7.5.2. A CONTRATADA se compromete a guardar confidencialidade e a não utilizar qualquer tipo de Informação Confidencial para propósitos estranhos àqueles definidos neste Termo de Referência ou em benefício próprio ou de terceiros.

7.5.3. A CONTRATADA se compromete a adotar as medidas necessárias para que seus dirigentes, empregados, e em geral todas as pessoas que trabalham sob sua responsabilidade, que precisem conhecer a Informação Confidencial, mantenham a confidencialidade acordada neste instrumento, sendo responsável pela ruptura do compromisso de confidencialidade pelos seus colaboradores.

7.5.4. A CONTRATADA se obriga a devolver ou destruir imediatamente todo o material que contenha Informações Confidenciais, tão logo ocorra a rescisão ou término da vigência do contrato firmado entre as partes.

7.5.5. A CONTRATANTE também se compromete a tratar como confidenciais todas as informações de propriedade da CONTRATADA, que vier a ter conhecimento, durante a vigência do contrato.

8. ACORDO DE NÍVEIS DE SERVIÇO – SLA (*SERVICE LEVEL AGREEMENT*)

8.1. SLO (*Service Level Objectives* - Objetivos de Nível de Serviço) para serviços gerenciados

8.1.1. SLO de Solicitações e Consultas:

Serviço	Definição	Médio
Todos	Tempo de atendimento a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC	4h
Todos	Tempo de resolução a partir da comunicação do cliente até que o SOC comunique a resolução do mesmo	8h

9. ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

9.1. SOLUÇÃO DE SEGURANÇA DE REDE E COM AS SEGUINTES FUNCIONALIDADES

9.2. O Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, *malwares*, Filtro de URL, criptografia de e-mail, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em nuvem ou hardware específico ou virtualizado.

9.3. A console de gerenciamento em nuvem, deve estar no Brasil;

9.4. A console de gerenciamento deve ser possível atribuir configurações de concentradores de SD-WAN;

9.5. A console de gerenciamento deve dispor de configurações globais para replicação nos firewalls;

9.6. Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / malwares, endpoints, softwares de criptografia de armazenamento em nuvem e assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional.

9.7. Para os itens que representem bens materiais, a **CONTRATADA** deverá fornecer produtos novos, sem uso anterior.

9.8. Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.

9.9. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

9.10. Deve possuir processadores próprios e para fins específicos, desenvolvidos exclusivamente pelo fabricante da solução, com a finalidade de processar tráfegos de redes e acelerar o processamento destes pacotes de redes, permitindo o uso de diversas funcionalidades de segurança ao mesmo tempo sem diminuir a performance do equipamento.

9.11. Todos os equipamentos de rede deverão possuir certificado de homologação expedido pela Agência Nacional de Telecomunicações (ANATEL).

9.12. O Firewall e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

9.13. A CONTRATADA deverá fornecer 02 (dois) equipamento acess point com poe da mesma marca do Fabricante do Firewall, com o mínimo de performance exigido:

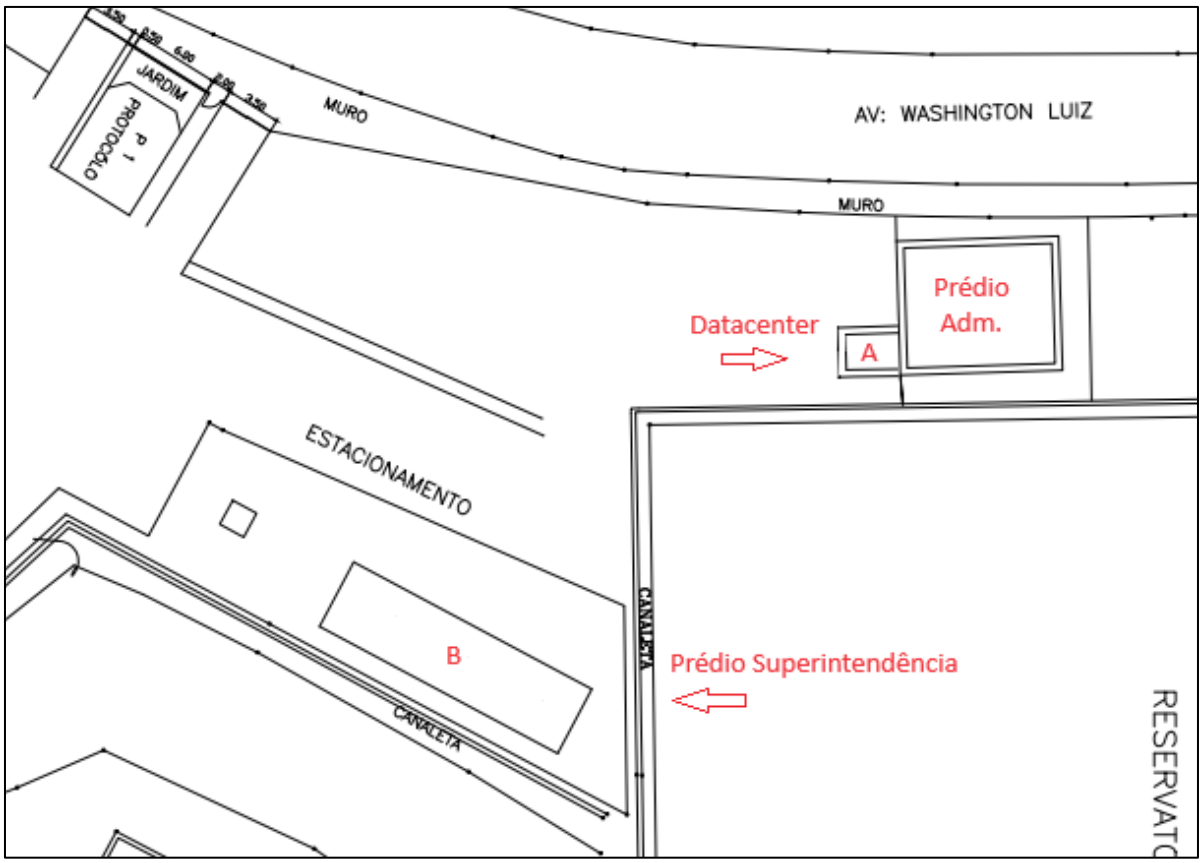
Radios:1x 2.4 GHz single-band e 1x 5 GHz single-band

Antenas: 2x internal dual-band antenna for Radio-0 and 1

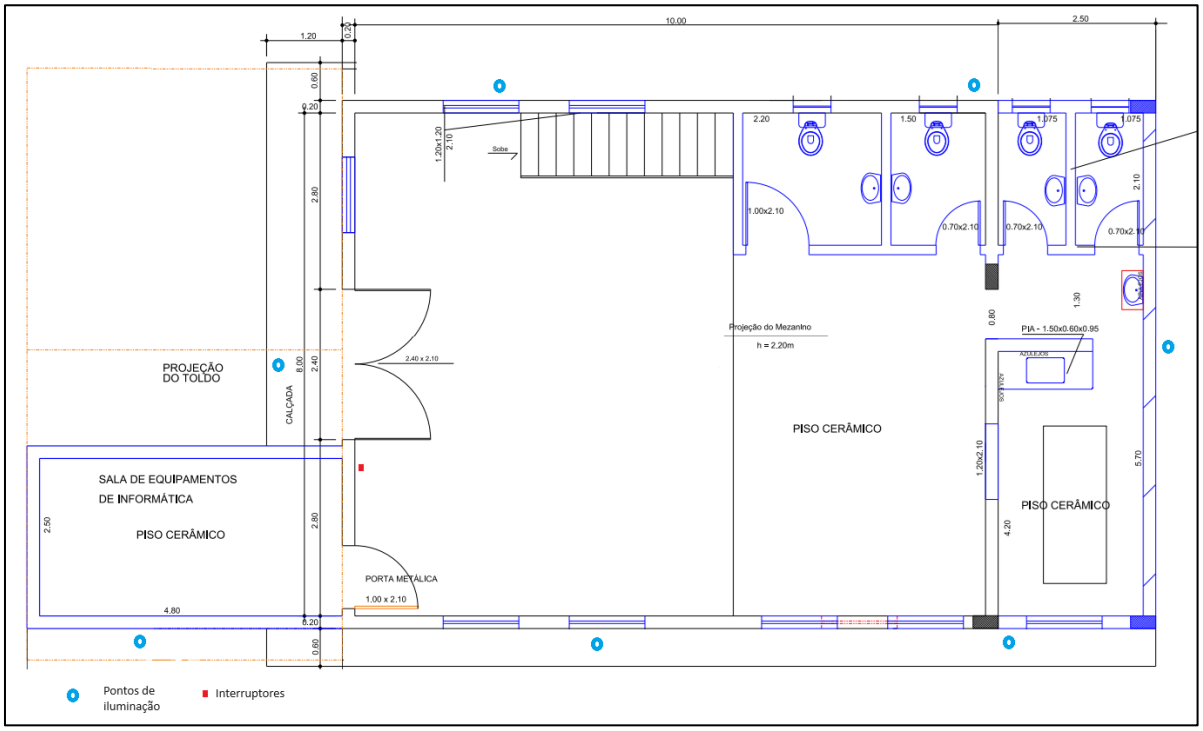
Performance: 2x2:2 MU-MIMO

Interfaces: 1x 12V DC-in: 1x 12V DC-in (power supply not included) 1x RJ45 10/100/1000 Ethernet w/PoE.

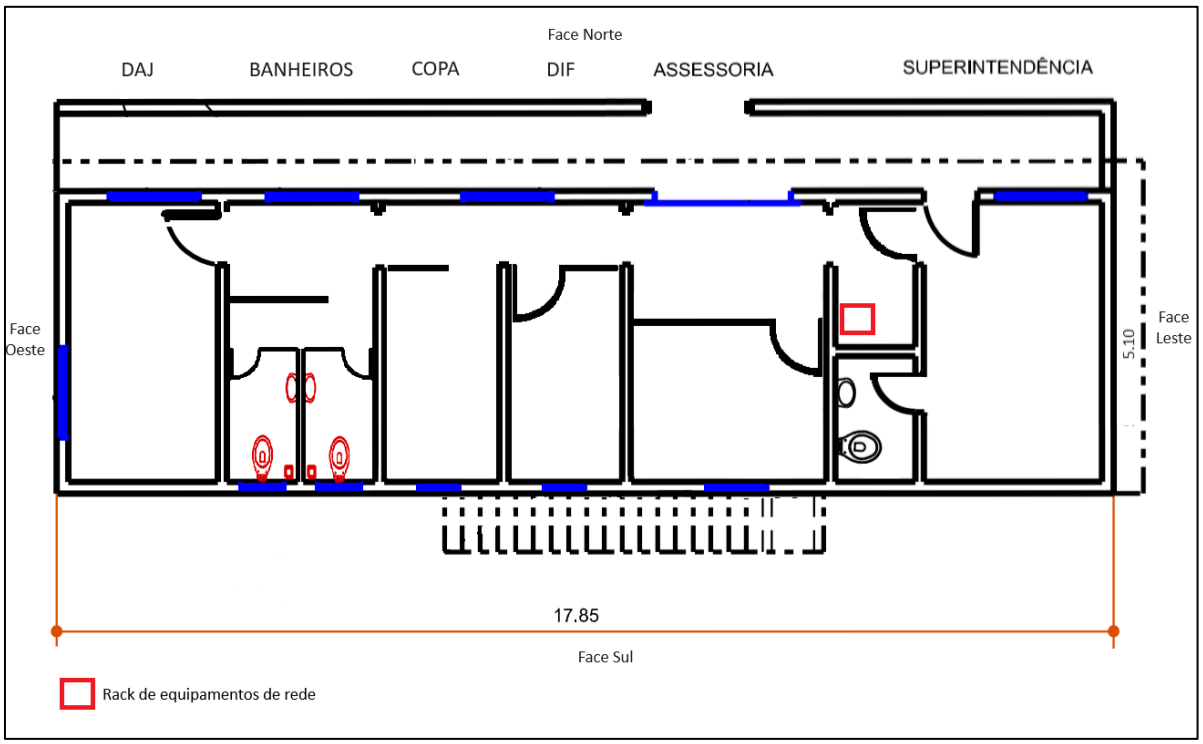
9.14. Seguem plantas do terreno e prédios onde os equipamentos deverão ser instalados.



Terreno com os prédios Administrativo e Superintendência, com cerce de 30 metros de distância entre estes, cuja rede está interligada através de cabo de fibra ótica.



Planta do prédio administrativo. O firewall e um access point deverão ser instalados na sala de equipamentos de informática.



Planta do prédio Superintendência com rack para equipamentos de rede, onde deverá ser instalado o segundo access point.

10. QUANTIDADES PREVISTAS

10.1. Contratação de solução de segurança, conforme tabela abaixo:

Item	Descrição	Quant.
HARDWARE DE FIREWALL		
1	Firewall NGFW com relatórios de acessos e VPN'S nativos e 02 antenas wireless (Access Point)	1
SOFTWARE FIREWALL		
2	Recursos Firewall: Gateway de antivírus, antispyware, ips/ids, filtro web, filtro de aplicação, sandbox, sd-wan.	1
TREINAMENTO		
3	Treinamento Hands on	1

11. CARACTERÍSTICAS ESPECÍFICAS DE DESEMPENHO E HARDWARE DA SOLUÇÃO DE FIREWALL

11.1.1. A solução deve consistir em *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência, monitoração e logs.

11.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

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

11.2. Taxa de transferência de dados com total das funcionalidades de segurança habilitadas (firewall throughput) deve ser, no mínimo, 12,500 Mbps;

11.3. Deverá suportar no mínimo 4,190,000 conexões simultâneas;

11.4. Deverá suportar no mínimo, 53,000 novas conexões por segundo;

11.5. Deverá suportar no mínimo 1,000 Mbps de tráfego de VPN;

11.6. Suportar no mínimo 1,000 tuneis VPN (sendo ao menos 70 tuneis SSLVPN já licenciados);

11.6.1. A Solução física deverá apresentar compatibilidade com modens USB (3G/4G), onde apenas seja acionado na eventualidade de falha no link principal;

11.7. Equipamento deve ter a possibilidade de ser configurado em alta disponibilidade, se futuramente solicitado pela SAMA;

11.8. Possuir no mínimo 6 x 2.5 GE copper 1 x SFP fiber

11.9. O equipamento deve permitir acomodação em rack, através de fixadores próprios ou de bandeja, ocupando 1U ou 2U.

11.10. Equipamento deve ter a possibilidade de ser configurado em alta disponibilidade;

11.11. O equipamento deve ser novo, sem uso anterior;

11.12. Deverá ser Baseado em Hardware e desenvolvido com está finalidade, ou seja, não sendo aceita soluções baseadas em plataforma PC ou equivalente;

12. Características de gerenciamento:

12.1. Gestão centralizada a partir de uma console de administração baseada na Web e a partir da qual deve ser possível o acesso, configuração e monitoramento de todos os equipamentos de segurança contemplados na solução;

12.2. Será aceito solução de gerenciamento local, desde que, considerado redundância de toda parte de hardware, software e funcionalidades, além do licenciamento completo para todas as funcionalidades exigidas nesse documento;

12.3. Por meio da console de gerenciamento deve ser possível a configuração de todas as funcionalidades descritas;

12.4. Na plataforma de gerência deve ser possível identificar cada uma das localidades remotas com uma identificação administrativa para posteriormente ser usada como filtro de pesquisa;

12.5. O acesso ao console de gerenciamento deve ser realizado com o uso de um método de autenticação de dois fatores;

12.6. O acesso a console deve ser por HTTPS (portas 8080 e 443) e seus certificados de segurança devem ser emitidos por entidades reconhecidas na Internet;

12.7. A console de gerenciamento deve suportar a definição de contas de administrador com base em funções, relatar as alterações às mesmas em um log de eventos e alertas que podem ser consultados por meio da mesma console;

12.8. O administrador com acesso total pode efetuar as seguintes operações dentro da organização a qual ele pertence:

12.9. Criar, editar e excluir contas de acesso total e somente leitura para a organização.

12.10. Redefinição de senhas.

12.11. Criar, editar e excluir redes.

12.12. As alterações de configuração, remoção ou adição de equipamentos deve ser registrada com dia, hora, e nome do adm que a realizou;

12.13. Deve ser possível identificar tentativas, com sucesso, ou não de login na plataforma de gerência;

12.14. Deve haver um sistema automatizado de upgrade de firmware a fim dos equipamentos estarem sempre com a última versão estável de firmware;

12.15. Deve ser possível bloquear o acesso a plataforma após falhas de login;

12.16. Deve ser possível configurar logout da plataforma após período sem atividade;

12.17. Deve ser possível permitir que a plataforma de gerenciamento seja acessível apenas de IP's permitidos;

12.18. Deve apresentar inventário de equipamentos da solução que estão, ou não, em utilização;

12.19. A console de administração deve possuir ferramenta integrada para captura de pacotes que passam pelos equipamentos de segurança gerenciados. Caso não haja funcionalidade nativa será aceita solução externa;

12.20. Capacidade de identificação de dispositivos que se conectam por meio do appliance, com fio ou sem fio através do endereço IP ou MAC;

12.21. Suporte para a criação e o gerenciamento de VLANs utilizando o protocolo IEEE 802.1Q;

12.22. Deve suportar criação de rotas estáticas;

12.23. Serviço de DNS dinâmico incluído;
12.24. Serviço de NAT para a WAN para tradução de segmentos de rede internos;
12.25. Deve ter a capacidade de criar múltiplas instâncias de servidores DHCP. No caso de a Contratante desejar preservar seu DHCP interno, o equipamento deve ser capaz de se integrar em modo bridge para propagar este serviço para o interior da rede;
12.26. A contratante deverá ter acesso de gerenciamento à ferramenta para criação e alteração das configurações

13. Serviços de segurança:
13.1. Firewall Stateful;
13.2. A solução deverá suportar a definição de regras de firewall de camada 3 e camada 7;
13.3. Regras de políticas de acesso de camada 3 definidas por:
13.4. Protocolo (UDP ou TCP);
13.5. Host, sub-rede ou rede de origem;
13.6. Porta TCP ou UDP de origem;
13.7. Host, sub-rede ou rede de destino;
13.8. Porta TCP ou UDP de destino;
13.9. Através das regras da camada 7, deve suportar a restrição de tráfego a partir de categorias definidas, incluindo:
13.10. Blog / E-mail / Compartilhamento de arquivos / Jogos / Noticias / Backup on-line / Ponto a ponto / Redes sociais / Atualizações de softwares e antivírus / Esportes / Videoconferência e VoIP / Compartilhamento de arquivos via Web / Hostname http;
13.11. Suporte a NAT 1:1 e o redirecionamento de portas (Port Forwarding) para a publicação de sistemas específicos para a Internet;
13.12. Suporte para a criação de zonas desmilitarizadas (DMZ);
13.13. Deve implementar funcionalidade de criação automatizada de tuneis IPSEC VPN entre equipamentos dentro da mesma organização;
13.14. As VPNs site-to-site devem poder ser configuradas em modo hub-spoke ou full-mesh;
13.15. Deve permitir a criação de tuneis VPN com equipamentos de terceiros;
13.16. Deve permitir a conexão com client VPN;
13.17. Deve permitir a integração com active directory;

14. OBRIGAÇÕES DA SAMA

14.1. Fornecer à CONTRATADA, em tempo hábil, as informações necessárias à execução dos serviços.
14.2. Levar ao conhecimento da CONTRATADA, por escrito, qualquer fato extraordinário ou anormal que ocorrer na execução do objeto desta proposição, bem como imperfeições, falhas ou irregularidades constatadas no objeto pactuado, para que sejam adotadas as medidas corretivas necessárias.
14.3. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA.
14.4. Verificar e atestar as faturas da CONTRATADA.

14.5. Efetuar o pagamento devido pela execução dos serviços, no prazo estabelecido, desde que cumpridas todas as formalidades e exigências previstas no contrato.

15. OBRIGAÇÕES DA CONTRATADA

15.1. Responsabilizar-se integralmente pelo objeto contratado, nas quantidades e padrões estabelecidos, sendo vedada a subcontratação, vindo a responder pelos danos causados diretamente à SAMA ou a terceiros, decorrentes de sua culpa ou dolo, nos termos da legislação vigente, não excluindo ou reduzindo essa responsabilidade a fiscalização ou acompanhamento pelo órgão interessado, conforme Lei nº 14.133/2021.

15.2. Encaminhar à unidade fiscalizadora todas as faturas dos objetos.

15.3. Encaminhar relatório mensal de chamados abertos e concluídos.

15.4. Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes do fornecimento do objeto.

15.5. Reportar à SAMA imediatamente qualquer anormalidade, erro ou irregularidades que possa comprometer a execução dos serviços e o bom andamento das atividades da Autarquia.

15.6. Guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços ou da relação mantida com a Autarquia.

15.7. Obedecer rigorosamente às normas e procedimentos de segurança implementados no ambiente de TI e institucional da SAMA.

16. PRAZOS E CONDIÇÕES

16.1. A entrega, instalação e configuração dos equipamentos e serviços deverá ocorrer no horário das 08:00 às 17:00h, de segunda a sexta-feira, exceto nos feriados, no Departamento de TI (11) 4514-0307 localizado no Saneamento Básico do Município de Mauá, Av. Washington Luiz, nº 2.923, Vila Magini, Mauá - SP, CEP: 09390-140.

16.2. A implantação da solução de hardware e software deverá ser realizada no prazo de até 30 (trinta) dias da contratação, mediante entrega de cronograma, detalhando as fases do projeto de implantação. Esse cronograma deverá ser aprovado pela CONTRATANTE, sendo a implantação iniciada somente após esta aprovação.

16.3. O prazo de vigência do presente contrato é de 12 (doze) meses, a partir da data de sua assinatura, podendo ser prorrogado por iguais e sucessivos períodos até o limite estabelecido na Lei nº 14.133/2021.

17. CONDIÇÕES DE ACEITE

17.1. O recebimento do objeto, será realizado da seguinte forma:

17.2. Provisoriamente, assim que efetuada a entrega, para efeito de posterior verificação da conformidade com as especificações.

17.3. Definitivamente, até 10 (dez) dias úteis da entrega, após verificação da qualidade e quantidade, e consequente aceitação.

17.4. No caso de consideradas insatisfatórias as condições do objeto recebido provisoriamente, será lavrado Termo de Recusa, no qual se consignarão as desconformidades, devendo o produto ser recolhido e substituído.

17.5. Após a notificação à CONTRATADA, o prazo decorrido até então será desconsiderado, iniciando-se nova contagem tão logo sanada a situação.

17.6. A CONTRATADA terá prazo de 10 (dez) dias úteis para providenciar a substituição do objeto, a partir da comunicação oficial feita pela SAMA, sem qualquer custo adicional para a SAMA.

17.7. Caso a substituição não ocorra no prazo determinado, estará a CONTRATADA incorrendo em atraso na entrega e sujeita à aplicação das sanções previstas.

17.8. O recebimento provisório e definitivo do objeto não exclui a responsabilidade civil a ele relativa, nem a ético-profissional, pela sua perfeita execução e dar-se-á se satisfeitas as seguintes condições:

17.9. Objeto de acordo com as especificações técnicas contidas neste Termo de Referência e na Proposta Comercial vencedora;

17.10. Quantidades em conformidade com o estabelecido na Nota de Empenho/Ordem de Serviço;

18. FISCALIZAÇÃO E GERENCIAMENTO

18.1. Nos termos da Lei nº 14.133/2021, o gerenciamento da execução será efetuado pela SAMA através do servidor designado, que também será responsável pelo recebimento e atesto do documento de cobrança.

18.2. A fiscalização efetuada pela SAMA não exime nem diminui a completa responsabilidade da CONTRATADA por qualquer inobservância ou omissão às cláusulas do Edital, deste Termo de Referência ou do Contrato.

18.3. A omissão, total ou parcial, da fiscalização não eximirá o fornecedor da integral responsabilidade pelos encargos ou serviços que são de sua competência.

19. CRITÉRIO DE JULGAMENTO

19.1. O critério de julgamento é o MENOR PREÇO GLOBAL, sobre o valor total estimado.

20. SANÇÕES

20.1. Pela inexecução total ou parcial do objeto da licitação, a Administração aplicará à contratada as sanções previstas na legislação.

Marcelo Augusto de Oliveira
Diretor de Administração e Finanças