Folhas nº
CPL

TERMO DE REFERÊNCIA

1. INFORMAÇÕES PRIMÁRIAS:

Órgão Requerente: *- Secretaria Municipal de Administração.*	Descrição de categoria de investimento: **(x) Aquisição** **(x) Contratação de Serviços**

2. MODALIDADE E O TIPO DE LICITAÇÃO:

Modalidade de Licitação:	**Tipo de Licitação:**
( ) Concorrência - Art. 22 § 1°, Art. 23 incisos I e II alínea c da Lei n° 8.666/93. ( ) Tomada de Preço - Art.22 §2°, Art.23 incisos I e II alínea b da Lei n° 8666/93. ( ) Convite - Art. 22 §3, Art.23 incisos I e II alínea a da Lei n° 8.666/93. ( ) Concurso - Art. 22 § 4° da Lei n° 8.666/93. ( ) Leilão - Art. 22 § 5° da Lei n° 8.666/93. ( ) Dispensa de Licitação - Art. 24 da Lei n° 8.666/93. ( ) Inexigibilidade de Licitação - Art. 25 da Lei n° 8.666/93. **(x) Pregão Eletrônico – SRP - Lei Federal n° 10.520/02 e subsidiariamente, no que couber, as disposições da Lei no 8.666/93.** ( ) Pregão Eletrônico – Tradicional - Lei Federal n° 10.520/02 e subsidiariamente, no que couber, as disposições da Lei no 8.666/93. ( ) Pregão Presencial – SRP - Lei Federal n° 0.520/02 e subsidiariamente, no que couber, as disposições da Lei no 8.666/93. ( ) Pregão Presencial – Tradicional - Lei n° 10.520/2002 e subsidiariamente, no que couber, as disposições da Lei no 8.666/93. ( ) Lei Municipal 2738/2017	Art. 45, incisos I ao IV, da Lei n° 8.666/93: **(X) Menor Preço Global** ( ) Menor Preço por item ( ) Menor Preço Lote ( ) Melhor Técnica ( ) Técnica e Preço ( ) Maior Lance ou Oferta ( ) Não se enquadra. ( ) Maior Percentual de Desconto.

3. DA LEGISLAÇÃO APLICÁVEL:

(x) Lei n° 8.666/93 e suas alterações (Institui normas para Licitações e Contratos da Administração);
(x) Lei Complementar n° 123/2006 (Institui o Estatuto Nacional da Microempresa e Empresa de Pequeno Porte) e alterações posteriores;
(x) Lei n° 10.520/2002 (Institui a modalidade de licitação denominada Pregão);
(x) Decreto Municipal n° 176/2006 e 044/2013 que regulamenta Sistema de Registro de Preços no Município.

(x) Lei Municipal n° 2738/2017 que dispõe sobre tratamento diferenciado as ME e EPP.
(X) Decreto Federal 9.412/2018 (Atualização das modalidades de licitação da Lei 8.666/93.

4. DO OBJETO:

O presente Termo de Referência tem por finalidade definir o conjunto de elementos que nortearão o procedimento para o "**REGISTRO DE PREÇOS PARA FUTURA E EVENTUAL CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE EQUIPAMENTOS DE SEGURANÇA DO TIPO FIREWALL NGFW PARA SEGURANÇA DA INFORMAÇÃO COMPOSTA DE APPLIANCES FÍSICOS E SOFTWARE COM LICENCIAMENTO DE USO PARA 36 MESES, INCLUINDO INSTALAÇÃO, ATUALIZAÇÃO E CONFIGURAÇÃO DA FERRAMENTA COM REPASSE DE CONHECIMENTO PARA 04 COLABORADORES E SUPORTE TÉCNICO SOB DEMANDA",** conforme condições, quantidades necessárias.

5. DA JUSTIFICATIVA:

5.1. FUNDAMENTAÇÃO DA CONTRATAÇÃO

A Tecnologia da Informação é um dos principais agentes de mudanças organizacionais. Sua utilização deve atentar-se para as questões estratégicas de apoio a integração operacional, organizacional e funcional. A correta utilização dos recursos da tecnologia contribui para um ambiente institucional moderno integrando as ações de todos os setores, fazendo da informatização um fator crítico de sucesso institucional.

Nos últimos 4 (quatro) anos nossa preocupação em relação ao controle e gerenciamento de dados em nossa instituição aumentou. Os pilares de segurança da informação sofreram alterações na era da informação, sendo eles caracterizados pelos seguintes atributos: disponibilidade, integridade, confidencialidade, autenticidade e não-repúdio. Segurança é um processo contínuo que não se conclui. Novos tipos de ataques cibernéticos são descobertos quase que diariamente. Vulnerabilidades de softwares são divulgadas todos os dias. Os processos referentes à segurança precisam ser revistos diariamente através de relatórios e acompanhamentos, e obviamente, os softwares envolvidos com a segurança da rede de dados precisam ser atualizados na mesma velocidade.

Firewall é um dispositivo composto de software e/ou hardware, que limita o acesso à rede, dando credenciais de acesso apenas a aqueles que realmente devem fazer o acesso à informação. Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados na rede. O firewall pode ser usado para ajudar a impedir que a rede ou um computador seja acessado sem autorização. Assim, é possível evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers. O firewall é um grande aliado no que se refere à segurança da informação, uma vez que é capaz de bloquear vulnerabilidades que, eventualmente, sejam usadas para a entrada de "pragas digitais", é possível realizar o controle a nível de aplicação através de bloqueio ao acesso de programas não autorizados.

A compra mostra-se imprescindível em virtude da crescente demanda por segurança no acesso à rede mundial de computadores (internet). Atualmente, são diversos os tipos de ataques que são conhecidos na internet e ainda, assim, hackers conseguem obter sucesso pela não prevenção e a presença de equipamentos modernos e ativos que minimizam estes riscos, sendo assim, a Prefeitura de Sorriso, no intuito de aprimorar seus fundamentos de

segurança da informação, tem como objetivo contratar não somente os ativos de rede (firewalls), mas, também, o suporte e garantia da solução, mantendo a base de ameaças atualizada, garantindo assim a proteção de seu bem mais precioso que são as informações armazenadas.

5.2. OBJETIVOS A SEREM ALCANÇADOS

Na estruturação da rede de informática da prefeitura, considerando o avanço da legislação no que se refere às políticas de segurança da informação, é necessário ampliar a estrutura de tecnologia, já que desde 2017 até o momento diversos setores e departamentos surgiram, aumentando o número de usuários e consequentemente a informação que precisa ser tratada.

Dentro desta lógica de avanço tecnológico e obtenção de novas ferramentas que visam tanto a melhoria interna (qualidade e segurança) e externa (melhor atendimento ao contribuinte), o presente processo trata de aquisição de solução completa de FIREWALL NGFW, necessário para atender as necessidades da prefeitura. Além de oferecer um nível maior de segurança à rede, um firewall de próxima geração possibilita a implementação de novos serviços, como por exemplo, análise do tráfego. Com isso seria possível ter uma visualização detalhada da utilização da rede e das aplicações utilizadas. Assim, o processo de identificação de ameaças é facilitado e permite a aplicação de políticas de segurança mais eficientes. Outra funcionalidade importante que pode ser implementada é a identificação de usuários que utilizam a rede e o registro de conexões. Essas informações são extremamente importantes, seja para realizar a adequação ao Marco Civil da Internet ou para realizar o tratamento de incidentes de segurança. No cenário atual, essas informações muitas vezes são ineficientes, visto que a arquitetura implementada não está possibilitando armazenar esses dados. Um firewall de próxima geração oferece isso de forma interessante, sendo possível gerar relatórios de forma rápida e detalhada sobre tudo o que acontece na rede. Dessa forma, o firewall possibilitará atingir os seguintes resultados:

- Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de
- Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);
- Maior visibilidade do tráfego de rede e aplicações em camada 7, possibilitando a detecção e proteção em tempo real contra ameaças;
- Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
- Proteção do ambiente de rede contra ameaças tipo worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.
- Geração de relatórios diversos para rápida análise de informações sobre tráfego, aplicações, ameaças, usuários, etc.
- Criação de políticas de proteção da rede contra eventuais ataques de usuários mal intencionados através do fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
- Criação de políticas e regras de uso de aplicações, acesso a certas categorias de URL, portas de serviços TCP e UDP (por grupo ou usuário);
- Melhor filtro de conteúdo URL, sancionando acesso a sites indesejados de conteúdo ilícito.

6. DA ESPECIFICAÇÃO DOS PRODUTOS/SERVIÇOS:

6.1. Equipamentos de segurança do tipo firewall NGFW para segurança da informação composta de appliances físicos e software com licenciamento de uso para no mínimo 36 meses, incluindo instalação, atualização e configuração da ferramenta com repasse de conhecimento para 04 colaboradores e suporte técnico sob demanda, **CONFORME AS ESPECIFICAÇÕES DO ANEXO I**:

SEQ	COD SIST	COD TCE	NAT DESP	DESCRIÇÃO	UND	MEDIA	QUANT. TOTAL	TOTAL
1	848246	342855-9	449052	EQUIPAMENTO DE PROTECAO DE REDE - SOLUÇÃO DE SEGURANÇA DE REDE APPLIANCE NEXT GENERATION FIREWALL CLUSTER, COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA MÍNIMA DE 03 ANOS	UND	R$ 54.078,67	2	R$ 108.157,34
2	848245	404876-8	339040	SERVICO DE TREINAMENTO NA AREA DE INFORMATICA - SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E REPASSE DE CONHECIMENTO PARA SOLUÇÃO DE SEGURANÇA DE REDE FIREWALL	UND	R$ 11.426,13	1	R$ 11.426,13
								R$ 119.583,47

7. VALOR ESTIMADO DA CONTRATAÇÃO:

7.1. Secretaria Municipal de Administração: R$ 119.583,47 (Cento e dezenove mil quinhentos e oitenta e três reais e quarenta e sete centavos).

7.2. Cesta de preços obtida através de cotações em empresas especializadas, sistema RADAR TCE-MT e sistema Banco de Preços, sendo

PRINT SOLUÇÃO EM TECNOLOGIA LTDA –
PROCURADORIA GERAL DE JUSTICA - Pregão Eletrônico 96/2020
PM DE VARZEA GRANDE - Pregão Eletrônico 01/202
MINISTÉRIO DA EDUCAÇÃO - Instituto Federal de Educação, Ciência e Tecnologia do Sudeste de MG - Pregão Eletrônico 21/2020
MINISTÉRIO DA DEFESA - Diretoria de Comunicações e Tecnologia da Informação da Marinha - Pregão Eletrônico 122/2020
Tribunal de Contas do Estado do Rio Grande do Norte - Pregão Eletrônico 1/2020
MINISTÉRIO DAS MINAS E ENERGIA - Companhia Hidroelétrica do São Francisco - Pregão Eletrônico 4805/2020

7.2.1. Após análise e avaliação crítica da cesta de preços realizada, o critério utilizado para a definição do preço de referência foi o menor valor, devido a especificidade do objeto, visto que, o sistema radar TCE MT não encontramos critérios específicos do item, consta em anexo.

8. DOTAÇÃO ORÇAMENTÁRIA:

8.1. Conforme anexo II.

9. PRAZOS E FORMA DE EXECUÇÃO:

9.1. EXECUÇÃO

- Realização da Reunião Inicial

- Após a assinatura do Contrato, o Gestor do contrato deverá convocar a reunião inicial com todos os envolvidos na contratação. A reunião inicial poderá ser realizada de forma presencial ou de forma remota. Na reunião inicial:
  - O representante legal da contratada deverá entregar o Termo de Compromisso e o Termo de Ciência, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade;
  - O representante legal da contratada deverá apresentar o cronograma de execução do projeto;
  - Serão feitos esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.

- Prazos, horários de fornecimento de bens ou prestação dos serviços
  - A entrega de todos os produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato.
  - A implantação completa da solução deverá ser concluída em até 30 (trinta)
  - dias corridos após a entrega do objeto.
  - O(s) equipamento(s) deverão ser entregues e instalados no local indicado pelo departamento de Tecnologia da Informação, conforme ordem de fornecimento emitida. A entrega e instalação deverá ser realizada em dias úteis no horário das 07:00 às 11:00 e das 13:00 às 17:00 (horário local).
  - A entrega deverá ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada.
  - O suporte técnico deverá ser de, no mínimo, 3 anos.
- Documentação mínima exigida
  - A Contratada deverá fornecer:
    - Manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração;
    - Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas.
    - Relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.
- Formas de transferência de conhecimento
  - A fim de promover a transferência de conhecimento, a implantação da solução deverá ocorrer com participação direta dos técnicos da prefeitura de Sorriso que atuarão na solução. Durante a implantação da solução a equipe da Contratada deverá repassar as informações para a equipe responsável da prefeitura apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados.

9.2. CRITÉRIOS DE ACEITAÇÃO

9.2.1. Para Item 1 – SOLUÇÃO DE SEGURANÇA DE REDE FIREWALL COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA DE 03 ANOS:

✓ Serão realizadas consultas diretamente no site do fabricante do equipamento, inclusive em manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste Termo de Referência. Em caso de dúvidas ou divergência na comprovação da

especificação técnica, a prefeitura de Sorriso poderá solicitar uma amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnicos certificados na solução para configuração e comprovação dos itens pendentes, nas dependências do local designado pela prefeitura de Sorriso.

- ✓ Os produtos serão inspecionados no ato da entrega, afim de verificar a conformidade, quantidade e realizar a inspeção visual da solução. Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos usados ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas.
- ✓ A existência de inspeção não isenta a contratada da responsabilidade pela qualidade do material fornecido.
- ✓ A solução será recebida provisoriamente por uma equipe designada pelo Diretor do Centro de Processamento de Dados acompanhados dos fiscais do contrato a fim de permitir a realização dos testes e inspeção.
- ✓ O aceite do bem e recebimento definitivo somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presentes neste Termo de Referência e após aprovação no teste.
- ✓ O processo de implantação deverá ser devidamente documentado pela Contratada, que deverá apresentar relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.

9.2.2. Para Item 2 - SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E REPASSE DE CONHECIMENTO PARA SOLUÇÃO DE SEGURANÇA DE REDE FIREWALL:

- ✓ Referente à instalação, o aceite do serviço somente será dado após comprovação da instalação e o efetivo cumprimento de todas as configurações necessárias para funcionamento do equipamento dentro da estrutura da prefeitura de Sorriso, como, por exemplo, a migração das regras de firewall existentes.
- ✓ Referente ao treinamento e repasse de conhecimento, o aceite do serviço somente será dado após a apresentação de todos os conteúdos esperados e da resolução de possíveis dúvidas da equipe em treinamento.
- ✓ Caso seja verificada alguma inconformidade na aceitação inicial do objeto, a Contratante informará à Contratada os motivos da não aceitação, devolvendo o(s) bem(ns) para correção.
- ✓ Caberá à Contratada sanar as irregularidades identificadas na entrega dos bens, inclusive, substituí-los no prazo de 15 (quinze) dias da notificação, às suas expensas, quando fornecidos com problemas, apresentados fora das especificações técnicas estabelecidas, sob pena de incorrer nas sanções legais cabíveis.

9.2.3. Procedimentos de Teste e Inspeção:

- ✓ Previamente ao recebimento definitivo da solução serão realizados a verificação, testes e inspeção do atendimento integral às especificações técnicas exigidas. Estas ações serão realizadas por equipe designada pelo chefe do departamento de tecnologia acompanhados dos fiscais do contrato.
- ✓ Inicialmente deverá ser realizada a verificação das especificações exigidas através da inspeção física dos equipamentos, análise dos manuais técnicos enviados juntamente com os equipamentos ou disponibilizados de alguma forma e da análise

de informações disponibilizadas no site da fabricante. Para esta etapa deve-se observar a seguinte lista de verificação:

- Verificar se a caixa do equipamento foi entregue lacrada, em embalagem original e apresentando identificações de marca e modelo de acordo a descrição da proposta da CONTRATADA;
- Verificar se o equipamento está novo e sem uso;
- Verificar se o equipamento é o mesmo equipamento que foi ofertado na proposta;
- Verificar se o equipamento foi entregue acompanhado de todos os acessórios previstos nas especificações técnicas (como cabo de energia, conectores, etc.) e descritos na documentação apresentada junto com a proposta da CONTRATADA;
- Verificar se o(s) equipamentos(s) foram entregues na(s) quantidade(s) correta(s);
- Verificar se a documentação mínima exigida foi entregue (exceto relatório de implantação);

Após, deverá ser conduzida a inspeção através da verificação da conformidade da execução dos serviços em relação aos requisitos exigidos nas especificações técnicas. Para avaliação, serão considerados relatórios das ferramentas, verificação das configurações, testes de uso das funcionalidades, documentações de projeto, manuais das soluções e quaisquer outros documentos pertinentes.

Para esta etapa deve-se observar a seguinte lista de verificação:

- Conectar cabos de alimentação e verificar funcionamento dos equipamentos;
- Conectar cabos UTP e fibra óptica, e verificar funcionamentos das portas dos equipamentos;
- Realizar configurações relacionadas à rede (configuração de interfaces, endereços IP, roteamento, resolução de nomes (DNS);
- Realizar a criação de objetos, de políticas de segurança e regras de firewall;
- Realizar a configuração do serviço DHCP;
- Fornecer um firewall em modo ativo e outro em modo passivo;
- Verificar a sincronização entre equipamentos (firewall ativo e passivo);
- Caso o software de gerenciamento seja entregue em appliance virtual, verificar a compatibilidade com o hypervisor KVM, criar máquina virtual e realizar as configurações necessárias;
- Realizar a configuração de SNMP para integrar os equipamentos a ferramenta utilizada na Universidade para monitoramento de ativos de rede;
- Realizar a configuração do software de gerenciamento centralizado e armazenamento de logs, e verificar a integração e sincronismo entre os o firewall e o software;
- Verificar o armazenamento de logs e a criação de relatórios pré-definidos e customizados;
- Testar as seguintes funcionalidades no firewall:
  - Detecção de intrusão (Intrusion Prevention System - IPS) de tráfego malicioso;
  - Decriptografar tráfego SSL para inspeção de conteúdo;
  - Permitir inspeção em camada 7 (nível de aplicação);
  - Permitir inspeção de conteúdo com capacidade de identificar e bloquear vulnerabilidades, vírus, malwares conhecidos e
  - desconhecidos;
  - Permitir a distribuição de endereços IPv4 e IPv6 para clientes, através do serviço DHCP;

- Realizar a tradução de endereços IP: NAT (Network Address Translation);
- Permitir a criação de redes seguras (VPN) de forma simples para que os usuários e os administradores possam utilizar da infraestrutura da Universidade remotamente;
- Permitir autenticação centralizada tanto da rede cabeada como da rede sem fio utilizando-se da base LDAP existente;
- Deverá ser analisada a performance da solução na infraestrutura da prefeitura de Sorriso, verificando principalmente possíveis perdas de pacotes durante o uso da solução com todas as funcionalidades de inspeção e IPS/IDS ativas simultaneamente;
- Realizar testes de performance, com ênfase no throughput, utilizando ferramentas capazes de gerar relatórios relacionados a largura de banda;
- Também deverá ser realizado um método comparativo de verificação entre os requisitos da solução e os prospectos do fabricante.

✓ A Metodologia de Avaliação da Qualidade será realizada pela Contratante, de acordo com a avaliação das seguintes condições que deverão ser cumpridas pela Contratada:

- O cumprimento dos prazos e outras obrigações assumidas pela contratada;
- Entrega da documentação exigida;
- Atendimento dos critérios de aceitação;
- Execução dos procedimentos corretos para que haja o recebimento dos bens e a atestação dos serviços prestados no suporte técnico e;
- A Metodologia de Avaliação da Qualidade dos serviços prestados ocorrerá através do acompanhamento e avaliação dos atendimentos aos chamados de suporte técnico especializado junto com as solicitações de garantia;
- Durante a vigência do suporte técnico, a fiscalização técnica dos contratos avaliará constantemente a prestação do serviço.
- A CONTRATANTE reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuá-las de maneira presencial ou através de documentação, em qualquer momento da contratação.

10. GERENCIAMENTO E DA FISCALIZAÇÃO:

10.1. Atuarão como fiscais de contrato da presente aquisição os servidores:
TITULAR: JOAO PEDRO RAMOS DE SOUZA
SUBSTITUTO: JARED RODRIGUES CHAGAS

11. DA VALIDADE DA ATA DE REGISTRO DE PREÇO E DA VIGENCIA DO CONTRATO:

11.1. O prazo de validade da Ata Registro de Preço é de **12 (doze) meses**, contados da data de assinatura.
11.2. A vigência do contrato do Contrato de acordo com a Minuta do Edital será de **36 (trinta e seis) meses**, contados a partir da data de sua assinatura.

12. DAS SANÇÕES/PENALIDADES:

12.1. Conforme disposto na Lei n° 8.666/93 e suas alterações (Institui normas para Licitações e Contratos da Administração) e Lei n° 10.520/2002 (Institui a modalidade de licitação denominada Pregão).

13. DAS DISPOSIÇÕES GERAIS:

14.1. É vedado caucionar ou utilizar a Ata de Registro de Preços e/ou contrato decorrente do presente instrumento para qualquer operação financeira, sem prévia e expressa autorização da Administração.
14.2. A licitante vencedora deverá prestar os serviços quando solicitados, de acordo com as necessidades do Prefeitura de Sorriso, em estrita conformidade com disposições e especificações deste termo e pelo preço registrado.
14.3. Correrão por conta da CONTRATADA todas as despesas de seguros, transporte, tributos, encargos trabalhistas e previdenciários, decorrentes da entrega e da própria aquisição dos produtos, correndo a cargo da CONTRATANTE absolutamente os valores referentes ao efetivo fornecimento do objeto ao preço cotado na proposta da CONTRATADA.
14.4. Os preços ofertados devem ser expressos em real, unitários e totais e devem compreender todos os custos e despesas que, direta ou indiretamente decorra do cumprimento pleno e integral do objeto deste edital, tais como todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, e quaisquer outras taxas, custos ou emolumentos que incidam ou venham a incidir sobre os produtos.

14. DOS REQUISITOS PARA PARTICIPAÇÃO:

14.1. HABILITAÇÃO JURIDICA: Conforme disposto na Lei n° 8.666/93 e suas alterações (Institui normas para Licitações e Contratos da Administração) e Lei n° 10.520/2002 (Institui a modalidade de licitação denominada Pregão).
14.2. REGULARIDADE FISCAL: Conforme disposto na Lei n° 8.666/93 e suas alterações (Institui normas para Licitações e Contratos da Administração) e Lei n° 10.520/2002 (Institui a modalidade de licitação denominada Pregão).
14.3. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA: Conforme disposto na Lei n° 8.666/93 e suas alterações (Institui normas para Licitações e Contratos da Administração) e Lei n° 10.520/2002 (Institui a modalidade de licitação denominada Pregão).
14.1. **14.4. QUALIFICAÇÃO TÉCNICA PESSOA JURIDICA:** Conforme disposto na Lei n° 8.666/93 e suas alterações (Institui normas para Licitações e Contratos da Administração) e Lei n° 10.520/2002 (Institui a modalidade de licitação denominada Pregão).

Sorriso – MT, 12 de julho de 2021.

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO
Secretário (a): Estevam Húngaro Calvo Filho

ANEXO I – ESPECIFICAÇÃO DOS ITENS

ITEM	CÓDIGO ÁGILE	COD TCE	DESCRIÇÃO	UND	MEDIA	QTD	TOTAL
1	848246	342855-9	EQUIPAMENTO DE PROTECAO DE REDE - SOLUÇÃO DE SEGURANÇA DE REDE APPLIANCE NEXT GENERATION FIREWALL CLUSTER, COM SUPORTE, GARANTIA E LICENÇAS DE PROTEÇÃO COM VIGÊNCIA MÍNIMA DE 03 ANOS	UND	R$ 54.078,67	2	R$ 108.157,34
2	848245	404876-8	SERVICO DE TREINAMENTO NA AREA DE INFORMATICA - SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E REPASSE DE CONHECIMENTO PARA SOLUÇÃO DE SEGURANÇA DE REDE FIREWALL	UND	R$ 11.426,13	1	R$ 11.426,13
					TOTAL:		R$ 119.583,47

ITEM 1: NEXT GENERATION FIREWALL
QUANTIDADE: 02 UNIDADES

- **CARACTERÍSTICAS DO EQUIPAMENTO**
  - O CLUSTER DEVERÁ SER COMPOSTO DE UMA **APPLIANCE FÍSICO E UM APPLIANCE PASSIVO (ESPERA), O QUE CARACTERIZA O QUANTITATIVO DE 02 (DOIS) EQUIPAMENTOS**.
  - DEVE SUPORTAR, NO MÍNIMO, 10 GBPS COM A FUNCIONALIDADE DE FIREWALL HABILITADA PARA TRÁFEGO IPV4 E IPV6
  - DEVE SUPORTAR, NO MÍNIMO, 6.5 Gbps DE THROUGHPUT DE VPN IPSEC
  - DEVE SUPORTAR, NO MÍNIMO, 950 Mbps DE THROUGHPUT DE VPN SSL
  - DEVE SUPORTAR, NO MÍNIMO, 700 Mbps DE THROUGHPUT DE INSPEÇÃO SSL
  - DEVE SUPORTAR, NO MÍNIMO, 1.7 Gbps DE THROUGHPUT DE CONTROLE DE APLICAÇÃO
  - SUPORTE A, NO MÍNIMO, 1.45 MILHÕES DE CONEXÕES SIMULTÂNEAS
  - SUPORTE A, NO MÍNIMO, 42 MIL NOVAS CONEXÕES POR SEGUNDO
  - ESTAR LICENCIADO PARA, OU SUPORTAR SEM O USO DE LICENÇA, 200 TÚNEIS DE VPN IPSEC SITE-TO-SITE SIMULTÂNEOS
  - ESTAR LICENCIADO PARA, OU SUPORTAR SEM O USO DE LICENÇA, 2.5 MIL TÚNEIS DE CLIENTES VPN IPSEC SIMULTÂNEOS
  - ESTAR LICENCIADO PARA, OU SUPORTAR SEM O USO DE LICENÇA, 200 CLIENTES DE VPN SSL SIMULTÂNEOS
  - PERMITIR GERENCIAR AO MENOS 96 ACCESS POINTS
  - POSSUIR AO MENOS 8 INTERFACES 1GBPS
  - ESTAR LICENCIADO E/OU TER INCLUÍDO SEM CUSTO ADICIONAL, NO MÍNIMO, 10 SISTEMAS VIRTUAIS LÓGICOS (CONTEXTOS) POR APPLIANCE
  - SUPORTE A, NO MÍNIMO, 10 SISTEMAS VIRTUAIS LÓGICOS (CONTEXTOS) POR APPLIANCE
  - POSSUIR FONTE DE ALIMENTAÇÃO 100-240V AC
  - POSSUIR NO MÁXIMO 1 RU DE ALTURA

- **REQUISITOS MÍNIMOS DE FUNCIONALIDADE**
  - **CARACTERÍSTICAS GERAIS**
    - A SOLUÇÃO DEVE CONSISTIR EM PLATAFORMA BASEADA EM APPLIANCE COM FUNCIONALIDADES DE SD-WAN, E CONSOLE DE GERÊNCIA E MONITORAÇÃO;

- 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;
- A PLATAFORMA DEVE SER OTIMIZADA PARA ANÁLISE DE CONTEÚDO DE APLICAÇÕES EM CAMADA 7;
- TODOS OS EQUIPAMENTOS FORNECIDOS DEVEM SER PRÓPRIOS PARA MONTAGEM EM RACK 19", INCLUINDO KIT TIPO TRILHO PARA ADAPTAÇÃO SE NECESSÁRIO E CABOS DE ALIMENTAÇÃO;
- A GESTÃO DO EQUIPAMENTO DEVE SER COMPATÍVEL ATRAVÉS DA INTERFACE DE GESTÃO WEB NO MESMO DISPOSITIVO DE PROTECÇÃO DA REDE;
- OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A 4094 VLAN TAGS 802.1Q;
- OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A AGREGAÇÃO DE LINKS 802.3AD E LACP;
- OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A POLICY BASED ROUTING OU POLICY BASED FORWARDING;
- OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A ROTEAMENTO MULTICAST (PIM-SM E PIM-DM);
- OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A DHCP RELAY;
- OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A DHCP SERVER;
- OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM SUPORTAR SFLOW;
- OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM POSSUIR SUPORTE A JUMBO FRAMES;
- OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVEM SUPORTAR SUB-INTERFACES ETHERNET LOGICAS;
- DEVE SUPORTAR NAT DINÂMICO (MANY-TO-1);
- DEVE SUPORTAR NAT DINÂMICO (MANY-TO-MANY);
- DEVE SUPORTAR NAT ESTÁTICO (1-TO-1);
- DEVE SUPORTAR NAT ESTÁTICO (MANY-TO-MANY);
- DEVE SUPORTAR NAT ESTÁTICO BIDIRECIONAL 1-TO-1;
- DEVE SUPORTAR TRADUÇÃO DE PORTA (PAT);
- DEVE SUPORTAR NAT DE ORIGEM;
- DEVE SUPORTAR NAT DE DESTINO;
- DEVE SUPORTAR NAT DE ORIGEM E NAT DE DESTINO SIMULTANEAMENTE;
- DEVE PODER COMBINAR NAT DE ORIGEM E NAT DE DESTINO NA MESMA POLITICA
- DEVE IMPLEMENTAR NETWORK PREFIX TRANSLATION (NPTV6) OU NAT66, PREVENINDO PROBLEMAS DE ROTEAMENTO ASSIMÉTRICO;
- DEVE SUPORTAR NAT64 E NAT46;
- DEVE IMPLEMENTAR O PROTOCOLO ECMP;
- DEVE PERMITIR MONITORAR VIA SNMP FALHAS DE HARDWARE, USO DE RECURSOS POR NÚMERO ELEVADO DE SESSÕES, CONEXÕES POR SEGUNDO, NÚMERO DE TÚNEIS ESTABELECIDOS NA VPN, CPU, MEMÓRIA, STATUS DO CLUSTER, ATAQUES E ESTATÍSTICAS DE USO DAS INTERFACES DE REDE;

- ENVIAR LOG PARA SISTEMAS DE MONITORAÇÃO EXTERNOS, SIMULTANEAMENTE;
- DEVE HAVER A OPÇÃO DE ENVIAR LOGS PARA OS SISTEMAS DE MONITORAÇÃO EXTERNOS VIA PROTOCOLO TCP E SSL;
- PROTEÇÃO ANTI-SPOOFING;
- SUPORTAR OTIMIZAÇÃO DO TRÁFEGO ENTRE DOIS EQUIPAMENTOS;
- PARA IPV4, DEVE SUPORTAR ROTEAMENTO ESTÁTICO E DINÂMICO (RIPV2, BGP E OSPFV2);
- PARA IPV6, DEVE SUPORTAR ROTEAMENTO ESTÁTICO E DINÂMICO (RIPNG, OSPFV3, BGP4+);
- SUPORTAR OSPF GRACEFUL RESTART;
- DEVE SUPORTAR MODO SNIFFER, PARA INSPEÇÃO VIA PORTA ESPELHADA DO TRÁFEGO DE DADOS DA REDE;
- DEVE SUPORTAR MODO CAMADA – 2 (L2), PARA INSPEÇÃO DE DADOS EM LINHA E VISIBILIDADE DO TRÁFEGO;
- DEVE SUPORTAR MODO CAMADA – 3 (L3), PARA INSPEÇÃO DE DADOS EM LINHA E VISIBILIDADE DO TRÁFEGO;
- DEVE SUPORTAR MODO MISTO DE TRABALHO SNIFFER, L2 E L3 EM DIFERENTES INTERFACES FÍSICAS;
- SUPORTE A CONFIGURAÇÃO DE ALTA DISPONIBILIDADE ATIVO/PASSIVO E ATIVO/ATIVO: EM MODO TRANSPARENTE;
- SUPORTE A CONFIGURAÇÃO DE ALTA DISPONIBILIDADE ATIVO/PASSIVO E ATIVO/ATIVO: EM LAYER 3;
- SUPORTE A CONFIGURAÇÃO DE ALTA DISPONIBILIDADE ATIVO/PASSIVO E ATIVO/ATIVO: EM LAYER 3 E COM NO MÍNIMO 3 EQUIPAMENTOS NO CLUSTER;
- A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR: SESSÕES;
- A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR: CONFIGURAÇÕES, INCLUINDO, MAS NÃO LIMITADO AS POLÍTICAS DE FIREWALL, NAT, QOS E OBJETOS DE REDE;
- A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR: ASSOCIAÇÕES DE SEGURANÇA DAS VPNS;
- A CONFIGURAÇÃO EM ALTA DISPONIBILIDADE DEVE SINCRONIZAR:TABELAS FIB;
- O HA (MODO DE ALTA-DISPONIBILIDADE) DEVE POSSIBILITAR MONITORAÇÃO DE FALHA DE LINK;
- DEVE POSSUIR SUPORTE A CRIAÇÃO DE SISTEMAS VIRTUAIS NO MESMO APPLIANCE;
- EM ALTA DISPONIBILIDADE, DEVE SER POSSÍVEL O USO DE CLUSTERS VIRTUAIS, SEJA ATIVO-ATIVO OU ATIVO-PASSIVO, PERMITINDO A DISTRIBUIÇÃO DE CARGA ENTRE DIFERENTES CONTEXTOS;
- DEVE PERMITIR A CRIAÇÃO DE ADMINISTRADORES INDEPENDENTES, PARA CADA UM DOS SISTEMAS VIRTUAIS EXISTENTES, DE MANEIRA A POSSIBILITAR A CRIAÇÃO DE CONTEXTOS VIRTUAIS QUE PODEM SER ADMINISTRADOS POR EQUIPES DISTINTAS;
- O GERENCIAMENTO DA SOLUÇÃO DEVE SUPORTAR ACESSO VIA SSH E INTERFACE WEB (HTTPS), INCLUINDO, MAS NÃO LIMITADO À, EXPORTAR CONFIGURAÇÃO DOS SISTEMAS VIRTUAIS (CONTEXTOS) POR AMBAS INTERFACES;

- CONTROLE, INSPEÇÃO E DESCRIPTOGRAFIA DE SSL PARA TRÁFEGO DE ENTRADA (INBOUND) E SAÍDA (OUTBOUND), SENDO QUE DEVE SUPORTAR O CONTROLE DOS CERTIFICADOS INDIVIDUALMENTE DENTRO DE CADA SISTEMA VIRTUAL, OU SEJA, ISOLAMENTO DAS OPERAÇÕES DE ADIÇÃO, REMOÇÃO E UTILIZAÇÃO DOS CERTIFICADOS DIRETAMENTE NOS SISTEMAS VIRTUAIS (CONTEXTOS);
- A SOLUÇÃO DEVE IDENTIFICAR POTENCIAIS VULNERABILIDADES E DESTACAR AS MELHORES PRÁTICAS QUE PODERIAM SER USADAS PARA MELHORAR A SEGURANÇA E O DESEMPENHO GERAL DE UMA REDE;
- O CONSOLE DE ADMINISTRAÇÃO DEVE SUPORTAR PELO MENOS INGLÊS, ESPANHOL E PORTUGUÊS.
- O CONSOLE DEVE SUPORTAR O GERENCIAMENTO DE SWITCHES E PONTOS DE ACESSO WIRELESS PARA MELHORAR O NÍVEL DE SEGURANÇA
- A SOLUÇÃO DEVE OFERECER SUPORTE À INTEGRAÇÃO NATIVA DE EQUIPAMENTOS DE PROTEÇÃO DE EMAIL, FIREWALL DE APLICATIVOS, PROXY, CACHE E AMEAÇAS AVANÇADAS.

- **CONTROLE POR POLÍTICA DE FIREWALL**
  - DEVERÁ SUPORTAR CONTROLES POR ZONA DE SEGURANÇA;
  - CONTROLES DE POLÍTICAS POR PORTA E PROTOCOLO;
  - CONTROLE DE POLÍTICAS POR APLICAÇÕES, GRUPOS ESTÁTICOS DE APLICAÇÕES, GRUPOS DINÂMICOS DE APLICAÇÕES (BASEADOS EM CARACTERÍSTICAS E COMPORTAMENTO DAS APLICAÇÕES) E CATEGORIAS DE APLICAÇÕES;
  - CONTROLE DE POLÍTICAS POR USUÁRIOS, GRUPOS DE USUÁRIOS, IPS, REDES E ZONAS DE SEGURANÇA;
  - SOLUÇÃO DEVE SER CAPAZ DE APLICAR A INSPEÇÃO DE CONTROLE DE APLICAÇÃO DIRETAMENTE ÀS POLÍTICAS DE SEGURANÇA;
  - ALÉM DOS ENDEREÇOS E SERVIÇOS DE DESTINO, OBJETOS DE SERVIÇOS DE INTERNET DEVEM PODER SER ADICIONADOS DIRECTAMENTE ÀS POLÍTICAS DE FIREWALL;
  - DEVE SUPORTAR O PADRÃO DE INDÚSTRIA 'SYSLOG' PROTOCOL PARA ARMANAZEMENTO USANDO O FORMATO COMMON EVENT FORMAT (CEF);
  - DEVE HAVER UMA MANEIRA DE ASSEGURAR QUE O ARMAZENAMENTO DOS LOGS EM TEMPO REAL NÃO SUPERAM A VELOCIDADE DE UPLOAD;
  - DEVE SUPORTAR O PROTOCOLO PADRÃO DA INDÚSTRIA VXLAN;
  - DEVE SUPORTAR OBJETOS DE ENDEREÇO IPV4 E IPV6, CONSOLIDADOS NA MESMA REGRA/POLÍTICA DE FIREWALL
  - DEVE POSSUIR BASE COM OBJETOS DE ENDEREÇO IP, DE SERVIÇOS DA INTERNET COMO GOOGLE E OFFICE 365, ATUALIZADOS DINAMICAMENTE PELA SOLUÇÃO
  - A SOLUÇÃO DEVE OFERECER SUPORTE À INTEGRAÇÃO NATIVA COM A SOLUÇÃO DE SANDBOX, PROTEÇÃO DE EMAIL, CACHE E FIREWALL DE APLICATIVOS DA WEB.

- **CONTROLE DE APLICAÇÕES**

- OS DISPOSITIVOS DE PROTEÇÃO DE REDE DEVERÃO POSSUIR A CAPACIDADE DE RECONHECER APLICAÇÕES, INDEPENDENTE DE PORTA E PROTOCOLO;
- RECONHECER PELO MENOS 1700 APLICAÇÕES DIFERENTES, INCLUINDO, MAS NÃO LIMITADO A: TRÁFEGO RELACIONADO A PEER-TO-PEER, REDES SOCIAIS, ACESSO REMOTO, UPDATE DE SOFTWARE, PROTOCOLOS DE REDE, VOIP, ÁUDIO, VÍDEO, PROXY, MENSAGEIROS INSTANTÂNEOS, COMPARTILHAMENTO DE ARQUIVOS, E-MAIL;
- RECONHECER PELO MENOS AS SEGUINTES APLICAÇÕES: BITTORRENT, GNUTELLA, SKYPE, FACEBOOK, LINKED-IN, TWITTER, CITRIX, LOGMEIN, TEAMVIEWER, MS-RDP, VNC, GMAIL, YOUTUBE, HTTP-PROXY, HTTP-TUNNEL, FACEBOOK CHAT, GMAIL CHAT, WHATSAPP, 4SHARED, DROPBOX, GOOGLE DRIVE, SKYDRIVE, DB2, MYSQL, ORACLE, ACTIVE DIRECTORY, KERBEROS, LDAP, RADIUS, ITUNES, DHCP, FTP, DNS, WINS, MSRPC, NTP, SNMP, RPC OVER HTTP, GOTOMEETING, WEBEX, EVERNOTE, GOOGLE-DOCS;
- IDENTIFICAR O USO DE TÁTICAS EVASIVAS, OU SEJA, DEVE TER A CAPACIDADE DE VISUALIZAR E CONTROLAR AS APLICAÇÕES E OS ATAQUES QUE UTILIZAM TÁTICAS EVASIVAS VIA COMUNICAÇÕES CRIPTOGRAFADAS, TAIS COMO SKYPE E UTILIZAÇÃO DA REDE TOR;
- PARA TRÁFEGO CRIPTOGRAFADO SSL, DEVE DE-CRIPTOGRAFAR PACOTES A FIM DE POSSIBILITAR A LEITURA DE PAYLOAD PARA CHECAGEM DE ASSINATURAS DE APLICAÇÕES CONHECIDAS PELO FABRICANTE;
- IDENTIFICAR O USO DE TÁTICAS EVASIVAS VIA COMUNICAÇÕES CRIPTOGRAFADAS;
- ATUALIZAR A BASE DE ASSINATURAS DE APLICAÇÕES AUTOMATICAMENTE;
- LIMITAR A BANDA (DOWNLOAD/UPLOAD) USADA POR APLICAÇÕES (TRAFFIC SHAPING), BASEADO NO IP DE ORIGEM, USUÁRIOS E GRUPOS;
- PARA MANTER A SEGURANÇA DA REDE EFICIENTE, DEVE SUPORTAR O CONTROLE SOBRE APLICAÇÕES DESCONHECIDAS E NÃO SOMENTE SOBRE APLICAÇÕES CONHECIDAS;
- PERMITIR NATIVAMENTE A CRIAÇÃO DE ASSINATURAS PERSONALIZADAS PARA RECONHECIMENTO DE APLICAÇÕES PROPRIETÁRIAS NA PRÓPRIA INTERFACE GRÁFICA DA SOLUÇÃO, SEM A NECESSIDADE DE AÇÃO DO FABRICANTE;
- O FABRICANTE DEVE PERMITIR A SOLICITAÇÃO DE INCLUSÃO DE APLICAÇÕES NA BASE DE ASSINATURAS DE APLICAÇÕES;
- DEVE POSSIBILITAR A DIFERENCIAÇÃO DE TRÁFEGOS PEER2PEER (BITTORRENT, EMULE, ETC) POSSUINDO GRANULARIDADE DE CONTROLE/POLÍTICAS PARA OS MESMOS;
- DEVE POSSIBILITAR A DIFERENCIAÇÃO DE TRÁFEGOS DE INSTANT MESSAGING (AIM, HANGOUTS, FACEBOOK CHAT, ETC) POSSUINDO GRANULARIDADE DE CONTROLE/POLÍTICAS PARA OS MESMOS;
- DEVE POSSIBILITAR A DIFERENCIAÇÃO E CONTROLE DE PARTES DAS APLICAÇÕES COMO POR EXEMPLO PERMITIR O HANGOUTS CHAT E BLOQUEAR A CHAMADA DE VÍDEO;
- DEVE POSSIBILITAR A DIFERENCIAÇÃO DE APLICAÇÕES PROXIES (PSIPHON, FREEGATE, ETC) POSSUINDO GRANULARIDADE DE CONTROLE/POLÍTICAS PARA OS MESMOS;

- DEVE SER POSSÍVEL A CRIAÇÃO DE GRUPOS DINÂMICOS DE APLICAÇÕES BASEADOS EM CARACTERÍSTICAS DAS APLICAÇÕES COMO: TECNOLOGIA UTILIZADA NAS APLICAÇÕES (CLIENT-SERVER, BROWSE BASED, NETWORK PROTOCOL, ETC);
- DEVE SER POSSÍVEL A CRIAÇÃO DE GRUPOS DINÂMICOS DE APLICAÇÕES BASEADOS EM CARACTERÍSTICAS DAS APLICAÇÕES COMO: NÍVEL DE RISCO DA APLICAÇÃO;
- DEVE SER POSSÍVEL A CRIAÇÃO DE GRUPOS ESTÁTICOS DE APLICAÇÕES BASEADOS EM CARACTERÍSTICAS DAS APLICAÇÕES COMO: CATEGORIA DA APLICAÇÃO;
- DEVE SER POSSÍVEL CONFIGURAR APPLICATION OVERRIDE PERMITINDO SELECIONAR APLICAÇÕES INDIVIDUALMENTE

➢ **IDENTIFICAÇÃO DE USUÁRIOS**

- DEVE INCLUIR A CAPACIDADE DE CRIAÇÃO DE POLÍTICAS BASEADAS NA VISIBILIDADE E CONTROLE DE QUEM ESTÁ UTILIZANDO QUAIS APLICAÇÕES ATRAVÉS DA INTEGRAÇÃO COM SERVIÇOS DE DIRETÓRIO, AUTENTICAÇÃO VIA LDAP, ACTIVE DIRECTORY, E-DIRECTORY E BASE DE DADOS LOCAL;
- DEVE POSSUIR INTEGRAÇÃO COM MICROSOFT ACTIVE DIRECTORY PARA IDENTIFICAÇÃO DE USUÁRIOS E GRUPOS PERMITINDO GRANULARIDADE DE CONTROLE/POLITICAS BASEADAS EM USUÁRIOS E GRUPOS DE USUÁRIOS;
- DEVE POSSUIR INTEGRAÇÃO COM MICROSOFT ACTIVE DIRECTORY PARA IDENTIFICAÇÃO DE USUÁRIOS E GRUPOS PERMITINDO GRANULARIDADE DE CONTROLE/POLITICAS BASEADAS EM USUÁRIOS E GRUPOS DE USUÁRIOS, SUPORTANDO SINGLE SIGN-ON. ESSA FUNCIONALIDADE NÃO DEVE POSSUIR LIMITES LICENCIADOS DE USUÁRIOS OU QUALQUER TIPO DE RESTRIÇÃO DE USO COMO, MAS NÃO LIMITADO À, UTILIZAÇÃO DE SISTEMAS VIRTUAIS, SEGMENTOS DE REDE, ETC;
- DEVE POSSUIR INTEGRAÇÃO COM RADIUS PARA IDENTIFICAÇÃO DE USUÁRIOS E GRUPOS PERMITINDO GRANULARIDADE DE CONTROLE/POLITICAS BASEADAS EM USUÁRIOS E GRUPOS DE USUÁRIOS;
- DEVE POSSUIR INTEGRAÇÃO COM LDAP PARA IDENTIFICAÇÃO DE USUÁRIOS E GRUPOS PERMITINDO GRANULARIDADE DE CONTROLE/POLITICAS BASEADAS EM USUÁRIOS E GRUPOS DE USUÁRIOS;
- DEVE PERMITIR O CONTROLE, SEM INSTALAÇÃO DE CLIENTE DE SOFTWARE, EM EQUIPAMENTOS QUE SOLICITEM SAÍDA A INTERNET PARA QUE ANTES DE INICIAR A NAVEGAÇÃO, EXPANDA-SE UM PORTAL DE AUTENTICAÇÃO RESIDENTE NO FIREWALL (CAPTIVE PORTAL);
- DEVE POSSUIR SUPORTE A IDENTIFICAÇÃO DE MÚLTIPLOS USUÁRIOS CONECTADOS EM UM MESMO ENDEREÇO IP EM AMBIENTES CITRIX E MICROSOFT TERMINAL SERVER, PERMITINDO VISIBILIDADE E CONTROLE GRANULAR POR USUÁRIO SOBRE O USO DAS APLICAÇÕES QUE ESTÃO NESTES SERVIÇOS;
- DEVE IMPLEMENTAR A CRIAÇÃO DE GRUPOS CUSTOMIZADOS DE USUÁRIOS NO FIREWALL, BASEADO EM ATRIBUTOS DO LDAP/AD;

- PERMITIR INTEGRAÇÃO COM TOKENS PARA AUTENTICAÇÃO DOS USUÁRIOS, INCLUINDO, MAS NÃO LIMITADO A ACESSO A INTERNET E GERENCIAMENTO DA SOLUÇÃO;
- PROVER NO MÍNIMO UM TOKEN NATIVAMENTE, POSSIBILITANDO AUTENTICAÇÃO DE DUPLO FATOR;

➢ **QOS E TRAFFIC SHAPING**

- COM A FINALIDADE DE CONTROLAR APLICAÇÕES E TRÁFEGO CUJO CONSUMO POSSA SER EXCESSIVO, (COMO YOUTUBE, USTREAM, ETC) E TER UM ALTO CONSUMO DE LARGURA DE BANDA, SE REQUER QUE A SOLUÇÃO, ALÉM DE PODER PERMITIR OU NEGAR ESSE TIPO DE APLICAÇÕES, DEVE TER A CAPACIDADE DE CONTROLÁ-LAS POR POLÍTICAS DE MÁXIMA LARGURA DE BANDA QUANDO FOREM SOLICITADAS POR DIFERENTES USUÁRIOS OU APLICAÇÕES, TANTO DE ÁUDIO COMO DE VÍDEO STREAMING;
- SUPORTAR A CRIAÇÃO DE POLÍTICAS DE QOS E TRAFFIC SHAPING POR ENDEREÇO DE ORIGEM;
- SUPORTAR A CRIAÇÃO DE POLÍTICAS DE QOS E TRAFFIC SHAPING POR ENDEREÇO DE DESTINO;
- SUPORTAR A CRIAÇÃO DE POLÍTICAS DE QOS E TRAFFIC SHAPING POR USUÁRIO E GRUPO;
- SUPORTAR A CRIAÇÃO DE POLÍTICAS DE QOS E TRAFFIC SHAPING POR APLICAÇÕES, INCLUINDO, MAS NÃO LIMITADO A SKYPE, BITTORRENT, YOUTUBE E AZUREUS;
- SUPORTAR A CRIAÇÃO DE POLÍTICAS DE QOS E TRAFFIC SHAPING POR PORTA;
- O QOS DEVE POSSIBILITAR A DEFINIÇÃO DE TRÁFEGO COM BANDA GARANTIDA;
- O QOS DEVE POSSIBILITAR A DEFINIÇÃO DE TRÁFEGO COM BANDA MÁXIMA;
- O QOS DEVE POSSIBILITAR A DEFINIÇÃO DE FILA DE PRIORIDADE;
- SUPORTAR MARCAÇÃO DE PACOTES DIFFSERV, INCLUSIVE POR APLICAÇÃO;
- SUPORTAR MODIFICAÇÃO DE VALORES DSCP PARA O DIFFSERV;
- SUPORTAR PRIORIZAÇÃO DE TRÁFEGO USANDO INFORMAÇÃO DE TYPE OF SERVICE;
- DEVE SUPORTAR QOS (TRAFFIC-SHAPPING), EM INTERFACE AGREGADAS OU REDUNDANTES;

➢ **FILTRO DE DADOS**

- PERMITIR A CRIAÇÃO DE FILTROS PARA ARQUIVOS E DADOS PRÉ-DEFINIDOS;
- OS ARQUIVOS DEVEM SER IDENTIFICADOS POR EXTENSÃO E TIPO;
- PERMITIR IDENTIFICAR E OPCIONALMENTE PREVENIR A TRANSFERÊNCIA DE VÁRIOS TIPOS DE ARQUIVOS (MS OFFICE, PDF, ETC) IDENTIFICADOS SOBRE APLICAÇÕES (HTTP, FTP, SMTP, ETC);
- SUPORTAR IDENTIFICAÇÃO DE ARQUIVOS COMPACTADOS OU A APLICAÇÃO DE POLÍTICAS SOBRE O CONTEÚDO DESSES TIPOS DE ARQUIVOS;
- SUPORTAR A IDENTIFICAÇÃO DE ARQUIVOS CRIPTOGRAFADOS E A APLICAÇÃO DE POLÍTICAS SOBRE O CONTEÚDO DESSES TIPOS DE ARQUIVOS;

- PERMITIR IDENTIFICAR E OPCIONALMENTE PREVENIR A TRANSFERÊNCIA DE INFORMAÇÕES SENSÍVEIS, INCLUINDO, MAS NÃO LIMITADO A NÚMERO DE CARTÃO DE CRÉDITO, POSSIBILITANDO A CRIAÇÃO DE NOVOS TIPOS DE DADOS VIA EXPRESSÃO REGULAR;

- **GEO LOCALIZAÇÃO**
  - SUPORTAR A CRIAÇÃO DE POLÍTICAS POR GEO-LOCALIZAÇÃO, PERMITINDO O TRAFEGO DE DETERMINADO PAIS/PAÍSES SEJAM BLOQUEADOS;
  - DEVE POSSIBILITAR A VISUALIZAÇÃO DOS PAÍSES DE ORIGEM E DESTINO NOS LOGS DOS ACESSOS;
  - DEVE POSSIBILITAR A CRIAÇÃO DE REGIÕES GEOGRÁFICAS PELA INTERFACE GRÁFICA E CRIAR POLÍTICAS UTILIZANDO AS MESMAS;

- **VPN**
  - SUPORTAR VPN SITE-TO-SITE E CLIENTE-TO-SITE;
  - SUPORTAR IPSEC VPN;
  - SUPORTAR SSL VPN;
  - A VPN IPSEC DEVE SUPORTAR AUTENTICAÇÃO MD5 E SHA-1;
  - A VPN IPSEC DEVE SUPORTAR DIFFIE-HELLMAN GROUP 1, GROUP 2, GROUP 5 E GROUP 14;
  - A VPN IPSEC DEVE SUPORTAR ALGORITMO INTERNET KEY EXCHANGE (IKEV1 E V2);
  - A VPN IPSEC DEVE SUPORTAR AES 128, 192 E 256 (ADVANCED ENCRYPTION STANDARD);
  - DEVE POSSUIR INTEROPERABILIDADE COM OS SEGUINTES FABRICANTES: CISCO, CHECK POINT, JUNIPER, PALO ALTO NETWORKS, FORTINET, SONICWALL;
  - SUPORTAR VPN EM EM IPV4 E IPV6, ASSIM COMO TRÁFEGO IPV4 DENTRO DE TÚNEIS IPSEC IPV6;
  - DEVE PERMITIR HABILITAR E DESABILITAR TÚNEIS DE VPN IPSEC A PARTIR DA INTERFACE GRÁFICA DA SOLUÇÃO, FACILITANDO O PROCESSO DE THROUBLESHOOTING;
  - DEVE PERMITIR QUE TODO O TRÁFEGO DOS USUÁRIOS REMOTOS DE VPN SEJA ESCOADO PARA DENTRO DO TÚNEL DE VPN, IMPEDINDO COMUNICAÇÃO DIRETA COM DISPOSITIVOS LOCAIS COMO PROXIES;
  - DEVER PERMITIR CRIAR POLÍTICAS DE CONTROLE DE APLICAÇÕES, IPS, ANTIVÍRUS, ANTIPYWARE E FILTRO DE URL PARA TRÁFEGO DOS CLIENTES REMOTOS CONECTADOS NA VPN SSL;
  - SUPORTAR AUTENTICAÇÃO VIA AD/LDAP, SECURE ID, CERTIFICADO E BASE DE USUÁRIOS LOCAL;
  - PERMITIR A APLICAÇÃO DE POLÍTICAS DE SEGURANÇA E VISIBILIDADE PARA AS APLICAÇÕES QUE CIRCULAM DENTRO DOS TÚNEIS SSL;
  - DEVERÁ MANTER UMA CONEXÃO SEGURA COM O PORTAL DURANTE A SESSÃO;
  - O AGENTE DE VPN SSL OU IPSEC CLIENT-TO-SITE DEVE SER COMPATÍVEL COM PELO MENOS: WINDOWS 7 (32 E 64 BIT), WINDOWS 8 (32 E 64 BIT), WINDOWS 10 (32 E 64 BIT) E MAC OS X (V10.10 OU SUPERIOR);
  - DEVE SUPORTAR AUTO-DISCOVERY VIRTUAL PRIVATE NETWORK (ADVPN)

- DEVE SUPORTAR AGREGAÇÃO DE TÚNEIS IPSEC
- DEVE SUPORTAR ALGORITMO DE BALANCEAMENTO DO TIPO WRR (WEIGHTED ROUND ROBIN) EM AGREGAÇÃO DE TÚNEIS IPSEC
- A VPN IPSEC DEVE SUPORTAR FORWARD ERROR CORRECTION (FEC)
- DEVE SUPORTAR TLS 1.3 EM VPN SSL

➢ **WIRELESS CONTROLLER**

- DEVERÁ ADMINISTRAR E CONTROLAR DE MANEIRA CENTRALIZADA OS PONTOS DE ACESSO WIRELESS DO MESMO FABRICANTE DA SOLUÇÃO OFERTADA;
- QUAISQUER LICENÇAS E/OU SOFTWARES NECESSÁRIOS PARA PLENA EXECUÇÃO DE TODAS AS CARACTERÍSTICAS DESCRITAS NESTE TERMO DE REFERÊNCIA DEVERÃO SER FORNECIDOS;
- DEVE PERMITIR A CONEXÃO DE DISPOSITIVOS WIRELESS QUE IMPLEMENTEM OS PADRÕES IEEE 802.11A/B/G/N/AC E QUE TRANSMITAM TRÁFEGO IPV4 E IPV6 ATRAVÉS DO CONTROLADOR;
- A SOLUÇÃO DEVERÁ SER CAPAZ DE GERENCIAR PONTOS DE ACESSO DO TIPO INDOOR E OUTDOOR;
- O CONTROLADOR WIRELESS DEVE PERMITIR SER DESCOBERTO AUTOMATICAMENTE PELOS PONTOS DE ACESSO ATRAVÉS DE BROADCAST, DHCP E CONSULTA DNS;
- A SOLUÇÃO DEVE OTIMIZAR O DESEMPENHO E A COBERTURA WIRELESS (RF) NOS PONTOS DE ACESSO POR ELA GERENCIADOS, REALIZANDO AUTOMATICAMENTE O AJUSTE DE POTÊNCIA E A DISTRIBUIÇÃO ADEQUADA DE CANAIS A SEREM UTILIZADOS. A SOLUÇÃO DEVE PERMITIR AINDA DESABILITAR O AJUSTE AUTOMÁTICO DE POTÊNCIA E CANAIS QUANDO NECESSÁRIO;
- PERMITIR AGENDAR DIA E HORÁRIO EM QUE OCORRERÁ A OTIMIZAÇÃO DO PROVISIONAMENTO AUTOMÁTICO DE CANAIS NOS ACCESS POINTS;
- O ENCAMINHAMENTO DE TRÁFEGO DOS DISPOSITIVOS CONECTADOS À REDE SEM FIO DEVE OCORRER DE FORMA CENTRALIZADA ATRAVÉS DE TÚNEL ESTABELECIDO ENTRE O PONTO DE ACESSO E CONTROLADOR WIRELESS. NESTE MODO TODOS OS PACOTES DEVEM SER TUNELADOS ATÉ O CONTROLADOR WIRELESS;
- QUANDO TUNELADO, O TRÁFEGO DEVE SER CRIPTOGRAFADO ATRAVÉS DE DTLS OU IPSEC;
- DEVE PERMITIR O GERENCIAMENTO DE PONTOS DE ACESSO CONECTADOS REMOTAMENTE ATRAVÉS DE LINKS WAN. NESTE CENÁRIO O ENCAMINHAMENTO DE TRÁFEGO DOS DISPOSITIVOS CONECTADOS À REDE SEM FIO DEVE OCORRER DE FORMA DISTRIBUÍDA (LOCAL SWITCHING), OU SEJA, O TRÁFEGO DEVE SER COMUTADO LOCALMENTE NA INTERFACE LAN DO PONTO DE ACESSO E NÃO NECESSITARÁ DE TUNELAMENTO ATÉ O CONTROLADOR WIRELESS;
- QUANDO O ENCAMINHAMENTO DO TRÁFEGO FOR DISTRIBUÍDO (LOCAL SWITCHING) E A AUTENTICAÇÃO VIA PSK, CASO HAJA FALHA NA COMUNICAÇÃO ENTRE OS PONTOS DE ACESSO E O CONTROLADOR WIRELESS, OS USUÁRIOS ASSOCIADOS DEVEM PERMANECER ASSOCIADOS AOS PONTOS DE ACESSO E AO MESMO SSID. DEVE SER POSSÍVEL AINDA PERMITIR A CONEXÃO DE NOVOS USUÁRIOS À REDE WIRELESS;

- A SOLUÇÃO DEVE PERMITIR DEFINIR QUAIS REDES SERÃO TUNELADAS ATÉ A CONTROLADORA E QUAIS REDES SERÃO COMUTADAS DIRETAMENTE PELA INTERFACE DO PONTO DE ACESSO;
- A SOLUÇÃO DEVE SUPORTAR RECURSO DE SPLIT-TUNNELING DE FORMA QUE SEJA POSSÍVEL DEFINIR, ATRAVÉS DAS SUBREDES DE DESTINO, QUAIS PACOTES SERÃO TUNELADOS ATÉ A CONTROLADORA E QUAIS SERÃO COMUTADOS LOCAMENTE NA INTERFACE DO PONTO DE ACESSO;
- A SOLUÇÃO DEVE IMPLEMENTAR RECURSOS QUE POSSIBILITEM A IDENTIFICAÇÃO DE INTERFERÊNCIAS PROVENIENTES DE EQUIPAMENTOS QUE OPEREM NAS FREQUÊNCIAS DE 2.4GHZ E 5GHZ;
- A SOLUÇÃO DEVERÁ DETECTAR RECEIVER START OF PACKET (RX-SOP) EM PACOTES WIRELESS E SER CAPAZ DE IGNORAR OS PACOTES QUE ESTEJAM ABAIXO DE DETERMINADO LIMIAR ESPECIFICADO DBM;
- A SOLUÇÃO DEVE PERMITIR O BALANCEAMENTO DE CARGA DOS USUÁRIOS CONECTADOS À INFRAESTRUTURA WIRELESS DE FORMA AUTOMÁTICA. A DISTRIBUIÇÃO DOS USUÁRIOS ENTRE OS PONTOS DE ACESSO PRÓXIMOS DEVE OCORRER SEM INTERVENÇÃO HUMANA E BASEADA EM CRITÉRIOS COMO NÚMERO DE DISPOSITIVOS ASSOCIADOS EM CADA PONTO DE ACESSO;
- A SOLUÇÃO DEVE POSSUIR MECANISMOS PARA DETECÇÃO E MITIGAÇÃO DE PONTOS DE ACESSO NÃO AUTORIZADOS, TAMBÉM CONHECIDOS COMO ROGUE APS. A MITIGAÇÃO DEVERÁ OCORRER DE FORMA AUTOMÁTICA E BAEADA EM CRITÉRIOS, TAIS COMO: INTENSIDADE DE SINAL OU SSID. OS PONTOS DE ACESSO GERENCIADOS PELA SOLUÇÃO DEVEM EVITAR A CONEXÃO DE CLIENTES EM PONTOS DE ACESSO NÃO AUTORIZADOS;
- A SOLUÇÃO DEVE IDENTIFICAR AUTOMATICAMENTE PONTOS DE ACESSO INTRUSOS QUE ESTEJAM CONECTADOS NA REDE CABEADA (LAN). A SOLUÇÃO DEVE SER CAPAZ DE IDENTIFICAR O PONTO DE ACESSO INTRUSO MESMO QUANDO O MAC ADDRESS DA INTERFACE LAN FOR LIGEIRAMENTE DIFERENTE (ADJACENTE) DO MAC ADDRESS DA INTERFACE WLAN;
- A SOLUÇÃO DEVE DETECTAR OS PONTOS DE ACESSO NÃO AUTORIZADOS E/OU INTRUSOS ATRAVÉS DE RÁDIOS DEDICADOS PARA A FUNÇÃO DE ANÁLISE OU ATRAVÉS DE OFF-CHANNEL/BACKGROUND SCANNING. QUANDO REALIZADA ATRAVÉS DE OFF-CHANNEL/BACKGROUND SCANNING, A SOLUÇÃO DEVE SER CAPAZ DE IDENTIFICAR A UTILIZAÇÃO DO PONTO DE ACESSO PARA, CASO NECESSÁRIO, ATRASAR A ANÁLISE E DESTA FORMA NÃO PREJUDICAR OS CLIENTES CONECTADOS;
- A SOLUÇÃO DEVE PERMITIR A CONFIGURAÇÃO INDIVIDUAL DOS RÁDIOS DO PONTO DE ACESSO PARA QUE OPEREM NO MODO MONITOR, OU SEJA, COM FUNÇÃO DEDICADA PARA DETECTAR AMEAÇAS NA REDE SEM FIO E COM ISSO PERMITIR MAIOR FLEXBILIDADE NO DESIGN DA REDE WIRELESS;
- A SOLUÇÃO DEVE PERMITIR A ADIÇÃO DE CONTROLADOR REDUNDANTE OPERANDO EM N+1. NESTE MODO, O CONTROLADOR REDUNDANTE DEVE MONITORAR A DISPONIBILIDADE E SINCRONIZAR AS CONFIGURAÇÕES DO PRINCIPAL, ALÉM DE

ASSUMIR TODAS AS FUNÇÕES EM CASO DE FALHA DO CONTROLADOR PRIMÁRIO. DESTA FORMA, TODOS OS PONTOS DE ACESSO DEVEM SE ASSOCIAR AUTOMATICAMENTE AO CONTROLADOR REDUNDANTE QUE PASSARÁ A TER FUNÇÃO DE PRIMÁRIO DE FORMA TEMPORÁRIA;

- A SOLUÇÃO DEVE PERMITIR O AGRUPAMENTO DE VLANS PARA QUE SEJAM DISTRIBUÍDAS MÚLTIPLAS SUBREDES EM UM DETERMINADO SSID, REDUZINDO ASSIM O BROADCAST E AUMENTANDO A DISPONIBILIDADE DE ENDEREÇOS IP;
- A SOLUÇÃO DEVE PERMITIR A CRIAÇÃO DE MÚLTIPLOS DOMÍNIOS DE MOBILIDADE (SSID) COM CONFIGURAÇÕES DISTINTAS DE SEGURANÇA E REDE. DEVE SER POSSÍVEL ESPECIFICAR EM QUAIS PONTOS DE ACESSO OU GRUPOS DE PONTOS DE ACESSO QUE CADA DOMÍNIO SERÁ HABILITADO;
- A SOLUÇÃO DEVE GARANTIR AO ADMINISTRADOR DA REDE DETERMINAR OS HORÁRIOS E DIAS DA SEMANA QUE AS REDES (SSIDS) ESTARÃO DISPONÍVEIS AOS USUÁRIOS;
- DEVE PERMITIR RESTRINGIR O NÚMERO MÁXIMO DE DISPOSITIVOS CONECTADOS POR PONTO DE ACESSO E POR RÁDIO;
- A SOLUÇÃO DEVE IMPLEMENTAR O PADRÃO IEEE 802.11R PARA ACELERAR O PROCESSO DE ROAMING DOS DISPOSITIVOS ATRAVÉS DO RECURSO CONHECIDO COMO FAST ROAMING;
- A SOLUÇÃO DEVE IMPLEMENTAR O PADRÃO IEEE 802.11K PARA PERMITIR QUE UM DISPOSITIVO CONECTADO À REDE WIRELESS IDENTIFIQUE RAPIDAMENTE OUTROS PONTOS DE ACESSO DISPONÍVEIS EM SUA ÁREA PARA QUE ELE EXECUTE O ROAMING;
- A SOLUÇÃO DEVE IMPLEMENTAR O PADRÃO IEEE 802.11V PARA PERMITIR QUE A REDE INFLUENCIE AS DECISÕES DE ROAMING DO CLIENTE CONECTADO ATRAVÉS DO FORNECIMENTO DE INFORMAÇÕES COMPLEMENTARES, TAL COMO A CARGA DE UTILIZAÇÃO DOS PONTOS DE ACESSO QUE ESTÃO PRÓXIMOS;
- A SOLUÇÃO DEVE IMPLEMENTAR O PADRÃO IEEE 802.11W PARA PREVENIR ATAQUES À INFRAESTRUTURA WIRELESS;
- A SOLUÇÃO DEVE SUPORTAR PRIORIZAÇÃO VIA WMM E PERMITIR A TRADUÇÃO DOS VALORES PARA DSCP QUANDO OS PACOTES FOREM DESTINADOS À REDE CABEADA;
- A SOLUÇÃO DEVE IMPLEMENTAR TÉCNICAS DE CALL ADMISSION CONTROL PARA LIMITAR O NÚMERO DE CHAMADAS SIMULTÂNEAS;
- A SOLUÇÃO DEVE APRESENTAR INFORMAÇÕES SOBRE OS DISPOSITIVOS CONECTADOS À INFRAESTRUTURA WIRELESS E INFORMAR AO MENOS AS SEGUINTES INFORMAÇÕES: NOME DO USUÁRIO CONECTADO AO DISPOSITIVO, FABRICANTE E SISTEMA OPERACIONAL DO DISPOSITIVO, ENDEREÇO IP, SSID AO QUAL ESTÁ CONECTADO, PONTO DE ACESSO AO QUAL ESTÁ CONECTADO, CANAL AO QUAL ESTÁ CONECTADO, BANDA TRANSMITIDA E RECEBIDA (EM KBPS), INTENSIDADE DO SINAL CONSIDERANDO O RUÍDO EM DB (SNR), CAPACIDADE MIMO E HORÁRIO DA ASSOCIAÇÃO;
- PARA GARANTIR UMA MELHOR DISTRIBUÇÃO DE DISPOSITIVOS ENTRE AS FREQUÊNCIAS DISPONÍVEIS E RESULTAR EM MELHORIAS NA UTILIZAÇÃO DA RADIOFREQUÊNCIA, A SOLUÇÃO DEVE SER CAPAZ DE DISTRIBUIR AUTOMATICAMENTE OS DISPOSITIVOS DUAL-

BAND PARA QUE CONECTEM PRIMARIAMENTE EM 5GHZ ATRAVÉS DO RECURSO CONHECIDO COMO BAND STEERING;

- A SOLUÇÃO DEVE PERMITIR A CONFIGURAÇÃO DE QUAIS DATA RATES ESTARÃO ATIVOS NA FERRAMENTA E QUAIS SERÃO DESABILITADOS PARA AS FREQUÊNCIAS DE 2.4 E 5GHZ E PADRÕES 802.11A/B/G/N/AC;
- A SOLUÇÃO DEVE POSSUIR RECURSO CAPAZ DE CONVERTER PACOTES MULTICAST EM PACOTES UNICAST QUANDO FOREM ENCAMINHADOS AOS DISPOSITIVOS QUE ESTIVEREM CONECTADOS À INFRAESTRUTURA WIRELESS, MELHORANDO ASSIM O CONSUMO DE AIRTIME;
- A SOLUÇÃO DEVE SUPORTAR RECURSO QUE IGNORE PROBE REQUESTS DE CLIENTES QUE ESTEJAM COM SINAL FRACO OU DISTANTES. DEVE PERMITIR DEFINIR O LIMIAR PARA QUE OS PROBE REQUESTS SEJAM IGNORADOS;
- A SOLUÇÃO DEVE PERMITIR A CONFIGURAÇÃO DO VALOR DE SHORT GUARD INTERVAL PARA 802.11N E 802.11AC EM 5GHZ;
- A SOLUÇÃO DEVE IMPLEMENTAR RECURSO CONHECIDO COMO AIRTIME FAIRNESS (ATF) PARA CONTROLAR O USO DE AIRTIME ALOCANDO PORCENTAGENS A SEREM UTILIZADAS NOS SSIDS;
- A SOLUÇÃO DEVE IMPLEMENTAR REGRAS DE FIREWALL (STATEFUL) PARA CONTROLE DO TRÁFEGO PERMITINDO OU DESCARTANDO PACOTES DE ACORDO COM A POLÍTICA CONFIGURADA, REGRAS ESTAS QUE DEVE USAR COMO CRITÉRIO ENDEREÇOS DE ORIGEM E DESTINO (IPV4 E IPV6), PORTAS E PROTOCOLOS;
- A SOLUÇÃO DEVE IMPLEMENTAR RECURSO DE WEB FILTERING PARA CONTROLE DE WEBSITES ACESSADOS NA REDE WIRELESS. DEVE POSSUIR UMA BASE DE CONHECIMENTO PARA CATEGORIZAÇÃO DOS SITES E PERMITIR CONFIGURAR QUAIS CATEGORIAS DE SITES SERÃO PERMITIDO E BLOQUEADOS PARA CADA PERFIL DE USUÁRIO E SSID;
- A SOLUÇÃO DEVE POSSUIR CAPACIDADE DE RECONHECIMENTO DE APLICAÇÕES ATRAVÉS DA TÉCNICA DE DPI (DEEP PACKET INSPECTION) QUE PERMITA AO ADMINISTRADOR DA REDE MONITORAR O PERFIL DE ACESSO DOS USUÁRIOS E IMPLEMENTAR POLÍTICAS DE CONTROLE. DEVE PERMITIR O FUNCIONAMENTO DESTE RECURSO E A ATUALIZAÇÃO PERIÓDICA DA BASE DE APLICAÇÕES DURANTE TODO O PERÍODO DE GARANTIA DA SOLUÇÃO;
- A BASE DE RECONHECIMENTO DE APLICAÇÕES ATRAVÉS DE DPI DEVE IDENTIFICAR COM, NO MÍNIMO, 1500 (MIL E QUINHENTAS) APLICAÇÕES;
- A SOLUÇÃO DEVE PERMITIR A CRIAÇÃO DE REGRAS PARA BLOQUEIO E LIMITE DE BANDA (EM MBPS, KBPS OU BPS) PARA AS APLICAÇÕES RECONHECIDAS ATRAVÉS DA TÉCNICA DE DPI;
- A SOLUÇÃO DEVE AINDA, ATRAVÉS DA TÉCNICA DE DPI, RECONHECER APLICAÇÕES SENSÍVEIS AO NEGÓCIO E PERMITIR A PRIORIZAÇÃO DESTE TRÁFEGO COM MARCAÇÃO QOS;
- "A SOLUÇÃO DEVE IMPLEMENTAR MECANISMOS DE PROTEÇÃO PARA IDENTIFICAR ATAQUES À INFRAESTRUTURA WIRELESS. AO MENOS OS SEGUINTES ATAQUES DEVEM SER IDENTIFICADOS:
- - ATAQUES DE FLOOD CONTRA O PROTOCOLO EAPOL (EAPOL FLOODING);

- - OS SEGUINTES ATAQUES DE NEGAÇÃO DE SERVIÇO: ASSOCIATION FLOOD, AUTHENTICATION FLOOD, BROADCAST DEAUTHENTICATION E SPOOFED DEAUTHENTICATION;
- - ASLEAP;
- - NULL PROBE RESPONSE / NULL SSID PROBE RESPONSE;
- - LONG DURATION;
- - ATAQUES CONTRA WIRELESS BRIDGES;
- - WEAK WEP;
- - INVALID MAC OUI."
- A SOLUÇÃO DEVE IMPLEMENTAR MECANISMOS DE PROTEÇÃO PARA MITIGAR ATAQUES À INFRAESTRUTURA WIRELESS. AO MENOS ATAQUES DE NEGAÇÃO DE SERVIÇO DEVEM SER MITIGADOS PELA INFRAESTRUTURA ATRAVÉS DO ENVIO DE PACOTES DE DEAUTHENTICATION;
- A SOLUÇÃO DEVE IMPLEMENTAR MECANISMOS DE PROTEÇÃO CONTRA ATAQUES DO TIPO ARP POISONING NA REDE WIRELESS;
- A SOLUÇÃO DEVE MONITORAR E CLASSIFICAR O RISCO DAS APLICAÇÕES ACESSADAS PELOS CLIENTES WIRELESS;
- PERMITIR CONFIGURAR O BLOQUEIO NA COMUNICAÇÃO ENTRE OS CLIENTES WIRELESS CONECTADOS A UM DETERMINADO SSID;
- DEVE IMPLEMENTAR AUTENTICAÇÃO ADMINISTRATIVA ATRAVÉS DO PROTOCOLO RADIUS;
- EM CONJUNTO COM OS PONTOS DE ACESSO, A SOLUÇÃO DEVE IMPLEMENTAR OS SEGUINTES MÉTODOS DE AUTENTICAÇÃO: WPA (TKIP) E WPA2 (AES);
- EM CONJUNTO COM OS PONTOS DE ACESSO, A SOLUÇÃO DEVE SER COMPATÍVEL E IMPLEMENTAR O MÉTODO DE AUTENTICAÇÃO WPA3;
- A SOLUÇÃO DEVE PERMITIR A CONFIGURAÇÃO DE MÚLTPLAS CHAVES DE AUTENTICAÇÃO PSK PARA UTILIZAÇÃO EM UM DETERMINADO SSID;
- QUANDO USANDO O RECURSO DE MÚLTIPLAS CHAVES PSK, A SOLUÇÃO DEVE PERMITIR A DEFINIÇÃO DE LIMITE QUANTO AO NÚMERO DE CONEXÕES SIMULTÂNEAS PARA CADA CHAVE CRIADA;
- A SOLUÇÃO DEVE IMPLEMENTAR O PROTOCOLO IEEE 802.1X COM ASSOCIAÇÃO DINÂMICA DE VLANS PARA OS USUÁRIOS COM BASE NOS ATRIBUTOS FORNECIDOS PELOS SERVIDORES RADIUS;
- A SOLUÇÃO DEVE IMPLEMENTAR O MECANISMO DE MUDANÇA DE AUTORIZAÇÃO DINÂMICA PARA 802.1X, CONHECIDO COMO RADIUS COA (CHANGE OF AUTHORIZATION) PARA AUTENTICAÇÕES 802.1X;
- A SOLUÇÃO DEVE SUPORTAR OS SEGUINTES MÉTODOS DE AUTENTICAÇÃO EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS E PEAP;
- A SOLUÇÃO DEVE IMPLEMENTAR RECURSO PARA AUTENTICAÇÃO DOS USUÁRIOS ATRAVÉS DE PÁGINA WEB HTTPS, TAMBÉM CONHECIDO COMO CAPTIVE PORTAL. A SOLUÇÃO DEVE LIMITAR O ACESSO DOS USUÁRIOS ENQUANTO ESTES NÃO INFORMAREM AS CREDENCIAIS VÁLIDAS PARA ACESSO À REDE;
- A SOLUÇÃO DEVE PERMITIR A HOSPEDAGEM DO CAPTIVE PORTAL NA MEMÓRIA INTERNA DO CONTROLADOR WIRELESS;
- A SOLUÇÃO DEVE PERMITIR A CUSTOMIZAÇÃO DA PÁGINA DE AUTENTICAÇÃO, DE FORMA QUE O ADMINISTRADOR DE REDE SEJA CAPAZ DE ALTERAR O CÓDIGO HTML DA PÁGINA WEB FORMATANDO TEXTO E INSERINDO IMAGENS;

- A SOLUÇÃO DEVE PERMITIR A COLETA DE ENDEREÇO DE E-MAIL DOS USUÁRIOS COMO MÉTODO DE AUTORIZAÇÃO PARA INGRESSO À REDE;
- A SOLUÇÃO DEVE PERMITIR QUE A PÁGINA DE AUTENTICAÇÃO SEJA HOSPEDADA EM SERVIDOR EXTERNO;
- A SOLUÇÃO DEVE PERMITIR O CADASTRAMENTO DE CONTAS PARA USUÁRIOS VISITANTES NA MEMÓRIA INTERNA. A SOLUÇÃO DEVE PERMITIR AINDA QUE SEJA DEFINIDO UM PRAZO DE VALIDADE PARA A CONTA CRIADA;
- A SOLUÇÃO DEVE GARANTIR QUE USUÁRIOS SE AUTENTIQUEM EM CAPTIVE PORTAL QUE FAÇA USO DE ENDEREÇO IPV6;
- A SOLUÇÃO DEVE POSSUIR INTERFACE GRÁFICA PARA ADMINISTRAÇÃO E GERENCIAMENTO DAS CONTAS DE USUÁRIOS VISITANTES, NÃO PERMITINDO ACESSO ÀS DEMAIS FUNÇÕES DE ADMINISTRAÇÃO DA SOLUÇÃO;
- APÓS A CRIAÇÃO DE UM USUÁRIO VISITANTE, A SOLUÇÃO DEVE ENVIAR AS CREDENCIAIS POR E-MAIL PARA O USUÁRIO CADASTRADO;
- A SOLUÇÃO DEVE IMPLEMENTAR RECURSO DE DHCP SERVER (IPV4 E IPV6) PARA FACILITAR A CONFIGURAÇÃO DE REDES VISITANTES;
- A SOLUÇÃO DEVE IDENTIFICAR AUTOMATICAMENTE O TIPO DE EQUIPAMENTO E SISTEMA OPERACIONAL UTILIZADO PELO DISPOSTIVO CONECTADO À REDE WIRELESS;
- A SOLUÇÃO DEVE PERMITIR QUE OS USUÁRIOS SEJAM CAPAZES DE ACESSAR SERVIÇOS DISPONIBILIZADOS ATRAVÉS DO PROTOCOLO BONJOUR (L2) E QUE ESTEJAM HOSPEDADOS EM OUTRAS SUBREDES, TAIS COMO: AIRPLAY E CHROMECAST. DEVE SER POSSÍVEL ESPECIFICAR EM QUAIS VLANS O SERVIÇO SERÁ DISPONIBILIZADO;
- A SOLUÇÃO DEVE PERMITIR A CONFIGURAÇÃO DE REDES MESH ENTRE OS PONTOS DE ACESSO POR ELA GERENCIADOS;
- A SOLUÇÃO DEVE PERMITIR A CONFIGURAÇÃO DE REDE MESH ENTRE PONTOS DE ACESSO INDOOR E OUTDOOR;
- A SOLUÇÃO DEVE PERMITIR SER GERENCIADA ATRAVÉS DOS PROTOCOLOS HTTPS E SSH VIA IPV4 E IPV6;
- A SOLUÇÃO DEVE PERMITIR O ENVIO DOS LOGS PARA MÚLTIPLOS SERVIDORES SYSLOG EXTERNOS;
- A SOLUÇÃO DEVE PERMITIR SER GERENCIADA ATRAVÉS DO PROTOCOLO SNMP (V1, V2C E V3), ALÉM DE EMITIR NOTIFICAÇÕES ATRAVÉS DA GERAÇÃO DE TRAPS;
- A SOLUÇÃO DEVE PERMITIR QUE SOFTWARES DE GERENCIAMENTO REALIZEM CONSULTAS DIRETAMENTE NOS PONTOS DE ACESSO VIA PROTOCOLO SNMP;
- A SOLUÇÃO DEVE INCLUIR SUPORTE PARA AS RFCS 1213 (MIB II) E RFC 2665 (ETHERNET-LIKE MIB);
- A SOLUÇÃO DEVE PERMITIR A CAPTURA DE PACOTES NA REDE WIRELESS E EXPORTA-LOS EM ARQUIVOS NO FORMATO .PCAP;
- A SOLUÇÃO DEVE PERMITIR A ADIÇÃO DE PLANTA BAIXA DO PAVIMENTO PARA ILUSTRAR GRAFICAMENTE A LOCALIZAÇÃO GEOGRÁFICA E STATUS DE OPERAÇÃO DOS PONTOS DE ACESSO POR ELA GERENCIADOS. DEVE PERMITIR A ADIÇÃO DE PLANTAS BAIXAS NOS SEGUINTES FORMATOS: JPEG, PNG, GIF OU CAD;

- A SOLUÇÃO DEVE APRESENTAR GRAFICAMENTE A TOPOLOGIA LÓGICA DA REDE, REPRESENTAR OS ELEMENTOS DA REDE GERENCIADOS, ALÉM DE INFORMAÇÕES SOBRE OS USUÁRIOS CONECTADOS COM A QUANTIDADE DE DADOS TRANSMITIDOS E RECEBIDOS POR ELES;
- A SOLUÇÃO DEVE IMPLEMENTAR O GERENCIAMENTO UNIFICADO E DE FORMA GRÁFICA PARA REDES WIFI E REDES CABEADAS;
- A SOLUÇÃO DEVE PERMITIR A ATUALIZAÇÃO DE FIRMWARE DO CONTROLADOR WIRELESS MESMO QUANDO CONECTADO REMOTAMENTE;
- A SOLUÇÃO DEVE PERMITIR A IDENTIFICAÇÃO DO FIRMWARE UTILIZADO POR CADA PONTO DE ACESSO GERENCIADO E PERMITIR A ATUALIZAÇÃO INDIVIDUALIZADA ATRAVÉS DA INTERFACE GRÁFICA;
- A SOLUÇÃO DEVE POSSUIR FERRAMENTAS DE DIAGNÓSTICOS E DEBUG;
- A SOLUÇÃO DEVE SUPORTAR COMUNICAÇÃO COM ELEMENTOS EXTERNOS ATRAVÉS DE APIS;
- A SOLUÇÃO DEVERÁ SER COMPATÍVEL E GERENCIAR OS PONTOS DE ACESSO DESTE PROCESSO;

➢ **SD-WAN**

- DEVE IMPLEMENTAR BALANCEAMENTO DE LINK POR HASH DO IP DE ORIGEM;
- DEVE IMPLEMENTAR BALANCEAMENTO DE LINK POR HASH DO IP DE ORIGEM E DESTINO;
- DEVE IMPLEMENTAR BALANCEAMENTO DE LINK POR PESO. NESTA OPÇÃO DEVE SER POSSÍVEL DEFINIR O PERCENTUAL DE TRÁFEGO QUE SERÁ ESCOADO POR CADA UM DOS LINKS.
- DEVE IMPLEMENTAR BALANCEAMENTO DE LINK POR CUSTO CONFIGURADO DO LINK.
- DEVE SUPORTAR O BALANCEAMENTO DE, NO MÍNIMO, 256 LINKS;
- DEVE SUPORTAR O BALANCEAMENTO DE LINKS DE INTERFACES FÍSICAS, SUB-INTERFACES LÓGICAS DE VLAN E TÚNEIS IPSEC
- DEVE IMPLEMENTAR BALANCEAMENTO DE LINKS SEM A NECESSIDADE DE CRIAÇÃO DE ZONAS OU USO DE INSTÂNCIAS VIRTUAIS;
- DEVE GERAR LOG DE EVENTOS QUE REGISTREM ALTERAÇÕES NO ESTADO DOS LINKS DO SDWAN, MONITORADOS PELA CHECAGEM DE SAÚDE
- DEVE SUPORTAR ZERO-TOUCH PROVISIONING
- POSSUIR CHECAGEM DO ESTADO DE SAÚDE DO LINK BASEANDO-SE EM CRITÉRIOS MÍNIMOS DE: LATÊNCIA, JITTER E PERDA DE PACOTES
- DEVE SER POSSÍVEL CONFIGURAR A PORCENTAGEM DE PERDA DE PACOTES E O TEMPO DE LATÊNCIA E JITTER, NA MEDIÇÃO DE ESTADO DE LINK. ESTES VALORES SERÃO UTILIZADOS PELA SOLUÇÃO PARA DECIDIR QUAL LINK SERÁ UTILIZADO
- A SOLUÇÃO DEVE PERMITIR MODIFICAR O INTERVALO DE TEMPO DE CHECAGEM, EM SEGUNDOS, PARA CADA UM DOS LINKS.
- A CHECAGEM DE ESTADO DE SAÚDE DEVE SUPORTAR TESTE COM PING, HTTP E DNS
- SUPORTAR UDP HOLE PUNCHING EM ARQUITETURA ADVPN

- A CHECAGEM DE ESTADO DE SAÚDE DEVE SUPORTAR A MARCAÇÃO DE PACOTES COM DSCP, PARA AVALIAÇÃO MAIS PRECISA DE LINKS QUE POSSUEM QOE CONFIGURADO
- AS REGRAS DE ESCOLHA DO LINK SD-WAN DEVEM SUPORTAR O RECONHECIMENTO DE APLICAÇÕES, GRUPOS DE USUÁRIOS, ENDEREÇO IP DE DESTINO E PROTOCOLO.
- DEVE SUPORTAR A CONFIGURAÇÃO DE NÍVEL MÍNIMO DE QUALIDADE (LATÊNCIA, JITTER E PERDA DE PACOTES) PARA QUE DETERMINADO LINK SEJA ESCOLHIDO PELO SD-WAN
- DEVE SUPORTAR ENVIO DE BGP ROUTE-MAP PARA BGP NEIGHBORS, CASO A QUALIDADE MÍNIMA DE UM LINK NÃO SEJA DETECTADA PELA CHECAGEM DE SAÚDE DO LINK

- **GARANTIA**
  - A GARANTIA EXIGIDA PARA TODA A SOLUÇÃO SERÁ DE NO MÍNIMO 36 MESES (3 ANOS).

ITEM 2: SERVIÇOS DE INSTAÇÃO, CONFIGURAÇÃO E REPASSE DE CONHECIMENTO PARA SOLUÇÃO DE SEGURANÇA DE REDE E ACESSO REMOTO
QUANTIDADE: 01 UNIDADE

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

- **REUNIÃO DE KICK-OFF**
  - A EMPRESA CONTRATADA, DEVERÁ REALIZAR REUNIÃO COM EQUIPE TÉCNICA DA PREFEITURA E ELABORAR O LEVANTAMENTO DE ITENS NECESSÁRIOS PARA A CRIAÇÃO DO PROJETO PROVISÓRIO DE IMPLANTAÇÃO – PPI. NESTE DOCUMENTO FICARÃO DESCRITAS TODAS AS PARTICULARIDADES DA IMPLANTAÇÃO. A PARTIR DESTE DOCUMENTO A CONTRATADA APRESENTARÁ UM CRONOGRAMA COM DEFINIÇÃO DE DATAS DE ENTREGA DO PROJETO E CADA UMA DE SUAS ETAPAS; TAL REUNIÃO PODE SER PRESENCIAL OU REMOTA;
  - TODAS AS FASES DO PROJETO DEVERÃO SER GUIADAS E GERIDAS POR UM GERENTE DE PROJETOS OU TECNICO CERTIFICADO DA CONTRATADA;
  - O GERENTE DE PROJETOS OU TECNICO CERTIFICADO DA CONTRATADA SERÁ RESPONSÁVEL PELO ACOMPANHAMENTO DIÁRIO DOS TRABALHOS DE IMPLANTAÇÃO E DEVERÁ GERAR O RELATÓRIO DE ATIVIDADES PARA OS RESPONSÁVEIS DA PREFEITURA DE SORRISO – MT. ESTE TRABALHO DEVERÁ INCLUIR ATIVIDADES COMO INÍCIO DO PROJETO, REUNIÕES DE ACOMPANHAMENTO, REUNIÕES DE INÍCIO, CONCLUSÃO DE FASES E CONCLUSÃO DO PROJETO;

- **IMPLANTAÇÃO DE FIREWALL**
  - A IMPLANTAÇÃO PODE SER REALIZADA DE FORMA PRESENCIAL OU REMOTA;
  - ATUALIZAÇÃO DE FIRMWARE DOS EQUIPAMENTOS;
  - CONFIGURAÇÕES DE IDS E IPS;
  - INTEGRAR A BASE DE USUÁRIOS DO AD DA PREFEITURA AO APPLIANCE PARA EFETUAR CONFIGURAÇÕES DE PERMISSÕES DE ACESSO;
  - CRIAR TODA E QUALQUER REGRA DE NAT NECESSÁRIA;
  - CONFIGURAR FILTRO DE CONTEÚDO DE ACORDO COM DEFINIÇÕES DA PREFEITURA;

- **TESTES OPERACIONAIS E OPERAÇÃO ASSISTIDA**
  - APÓS A CONFIGURAÇÃO, CUSTOMIZAÇÃO E OPERACIONALIZAÇÃO DE TODA SOLUÇÃO, A CONTRATADA DEVE SE COMPROMETER A REALIZAR TODOS OS TESTES OPERACIONAIS PARA GARANTIR O PERFEITO FUNCIONAMENTO DA SOLUÇÃO OFERTADA.
  - A CONTRATADA TERÁ A RESPONSABILIDADE DE AUXILIAR A EQUIPE DA PREFEITURA DE SORRISO A OPERAR O NOVO AMBIENTE. ALÉM DE GUIAR A EQUIPE TÉCNICA DA PREFEITURA DURANTE O TEMPO VIGENTE DA OPERAÇÃO ASSISTIDA
  - OS PROFISSIONAIS DA CONTRATADA DEVERÃO ESTAR À DISPOSIÇÃO PARA QUAISQUER ESCLARECIMENTOS SOBRE A TECNOLOGIA UTILIZADA;
  - TODOS OS TESTES TERÃO O ACOMPANHAMENTO E A APROVAÇÃO DO RESPONSÁVEL DA PREFEITURA.

- **DOCUMENTAÇÃO FINAL**
  - APRESENTAÇÃO PARA A EQUIPE DA PREFEITURA DE SORRISO COM A PASSAGEM DE CONHECIMENTO DO PROJETO FINALIZADO, ONDE IRÁ ABRANGER A CONFIGURAÇÃO FÍSICA E LÓGICA E TODAS AS INFORMAÇÕES DAS CONFIGURAÇÕES REALIZADAS NO PROJETO, PERMITINDO QUE A PREFEITURA DE SORRISO TIRE DÚVIDAS A RESPEITO DA SOLUÇÃO IMPLEMENTADA;
  - ENTREGA DA DOCUMENTAÇÃO DO PROJETO INSTALADO E SUAS RESPECTIVAS CONFIGURAÇÕES EM MÍDIA ELETRÔNICA EM CD, DVD OU PREFERENCIALMENTE PDF.

- **REPASSE DE TECNOLOGIA**
  - A TRANSFERÊNCIA DE CONHECIMENTO COMPREENDERÁ NECESSARIAMENTE OS SEGUINTES TÓPICOS:
    - INSTALAÇÃO, CONFIGURAÇÃO E OPERAÇÃO DO EQUIPAMENTO;
    - APRESENTAÇÃO DO PROJETO;
    - DESCRIÇÃO DA ARQUITETURA DO EQUIPAMENTO;
    - DESCRIÇÃO DO HARDWARE E SOFTWARE DISPONÍVEL;
    - ESTRATÉGIAS DE IMPLEMENTAÇÃO DOS EQUIPAMENTOS;
    - CONFIGURAÇÃO E ADMINISTRAÇÃO DOS EQUIPAMENTOS;
  - A CONTRATADA PODERÁ UTILIZAR OS EQUIPAMENTOS IMPLANTADOS PARA MINISTRAR O TREINAMENTO;
  - O REPASSE DE CONHECIMENTO DEVERÁ SER REALIZADO PARA UMA ÚNICA TURMA DE ATÉ 04 (QUATRO);
  - A TRANSFERÊNCIA DE CONHECIMENTO ESTARÁ CENTRADA NA SOLUÇÃO FORNECIDA, PRIVILEGIANDO ATIVIDADES PRÁTICAS QUE PERMITAM UMA MELHOR FIXAÇÃO DO APRENDIZADO, BEM COMO POSSIBILITE A EQUIPE TÉCNICA GERENCIAR A SOLUÇÃO IMPLANTADA;
  - A CONTRATADA DEVERÁ FORNECER, NO INÍCIO DE CADA TÓPICO, APOSTILAS (DIGITAL OU IMPRESSA) QUE ABORDEM TODO O CONTEÚDO PROGRAMÁTICO, AS QUAIS PODERÃO ESTAR NO TODO OU EM PARTE, EM PORTUGUÊS;
  - O INÍCIO DESTA ATIVIDADE, BEM COMO O PERÍODO E HORÁRIO DE REALIZAÇÃO, SERÁ DEFINIDO PELA PREFEITURA EM COMUM ACORDO COM A CONTRATADA;

- **PERFIL DOS PROFISSIONAIS DA CONTRATADA**

- A CONTRATADA DEVERÁ DISPONIBILIZAR PROFISSIONAIS COM CERTIFICADO DO FABRICANTE DO EQUIPAMENTO OFERTADO OU DEVERÁ APRESENTAR UM ATESTADO DE CAPACIDADE TÉCNICA DE SERVIÇO DE INSTALAÇÃO DE FIREWALL, COMPROVANDO QUE ESTÁ APTA A INSTALAÇÃO DOS EQUIPAMENTOS.

ANEXO II - DOTAÇÕES:

A despesa decorrente do objeto desta licitação ocorrerá à conta de recursos específicos consignados no Orçamento:

ÓRGÃO	DOTAÇÃO	PROJ/ATIVIDADE	ELEMENTO DESPESA	COD RED
SEC. MUNICIPAL DE ADMINISTRAÇÃO	**10.001.04.122.0002.2010**	**MANUT. DAS ATIV. DA SEMAD**	**33.90.40.00.00**	**480**
SEC. MUNICIPAL DE ADMINISTRAÇÃO	**10.001.04.122.0002.2010**	**MANUT. DAS ATIV. DA SEMAD**	**44.90.52.00.00**	**482**