TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. O presente Termo de Referência tem como objeto a contratação de empresa especializada nos serviços de renovação do licenciamento de suporte/assistência técnica da Solução Integrada de Segurança Cibernética em operação na Secretaria de Estado da Educação e da Cultura – SEDUC e o fornecimento de equipamentos de segurança de rede, visando a melhoria e futuras implantações da solução. A contratada deverá fornecer todo o hardware, software, suporte técnico, serviços e repasse de conhecimento da solução necessários para garantir a segurança da rede da SEDUC, observadas as especificações técnicas e demais condições estabelecidas neste documento e demais anexos.

1.2. Para a contratação pretendida, será adotado o Sistema de Registro de Preços (SRP) conforme justificativa:

1.2.1. A utilização do Sistema de Registro de Preços (SRP) se mostra a opção mais adequada. O SRP permite maior flexibilidade na contratação, garantindo que a SEDUC possa adquirir os itens objeto deste Termo de Referência de acordo com a demanda ao longo de um período de até 24 (vinte e quatro) meses, sem a necessidade de novas licitações. Além disso, o registro de preço possibilita obter melhores condições de negociação, promovendo uma economia para a administração pública e permitindo ajustes conforme o surgimento de novas necessidades de contratação. A adoção desse sistema também favorece o planejamento orçamentário e a otimização dos recursos, garantindo que a continuidade dos serviços críticos de TI não seja comprometida.

1.3. Os bens objeto desta contratação são caracterizados como comuns, conforme descrição constante no Estudo Técnico Preliminar e especificações detalhadas no Anexo I deste documento.

LOTE	ITEM	DESCRITIVO	UNID	QTDE
ÚNICO	01	SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW - TIPO I	UN	2
	02	SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW - TIPO II	UN	2
	03	SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW - TIPO III	UN	10
	04	SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW - TIPO IV	UN	20
	05	ATIVO DE REDE WIRED – TIPO I	UN	50
	06	ATIVO DE REDE WIRED – TIPO II	UN	50
	07	ATIVO DE REDE WIRED – TIPO III	UN	50
	08	ATIVO DE REDE WIRELESS – TIPO I	UN	100
	09	SOLUÇÃO DE GERÊNCIA DE LOGS E RELATORIA	UN	1
	10	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO I	UN	4

	11	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO II	UN	4
	12	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO III	UN	20
	13	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO IV	UN	40
	14	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO V	UN	6
	15	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO VI	UN	12
	16	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO VII	UN	447
	17	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO I	UN	100
	18	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO II	UN	163
	19	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO III	UN	100
	20	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO IV	UN	6
	21	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO V	UN	12
	22	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO VI	UN	18
	23	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO VII	UN	447
	24	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO VIII	UN	447
	25	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRELESS TIPO I	UN	200
	26	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRELESS TIPO II	UN	3072
	27	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE GERÊNCIA DE LOGS E RELATORIA	UN	2
	28	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE AUTENTICAÇÃO	UN	3
	29	SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE WAF	UN	3
	30	SERVIÇOS DE IMPLANTAÇÃO DE NGFW	UN	34
	31	SERVIÇOS DE IMPLANTAÇÃO DE REDE WIRED	UN	150
	32	SERVIÇOS DE IMPLANTAÇÃO DE REDE WIRELESS SEM INFRAESTRUTURA	UN	100
	33	SERVIÇOS DE IMPLANTAÇÃO DE REDE WIRELESS COM INFRAESTRUTURA	UN	100
	34	UST – UNIDADE DE SERVIÇOS TÉCNICOS ESPECIALIZADOS	UN	500

2. A VIGÊNCIA DA CONTRATAÇÃO

2.1. O prazo de vigência da contratação dos serviços é de 12 (doze) meses contados da assinatura do contrato, na forma do artigo 105 da Lei n° 14.133, de 2021.
2.2. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.
2.3. A vigência da Ata de Registro de Preços será de 12 (doze) meses, contados a partir da data de sua assinatura, conforme previsão do artigo 86 da Lei nº 14.133, de 2021.
2.4. Caso haja interesse da administração e observadas as condições de vantajosidade para a contratante, a vigência da ata poderá ser prorrogada por igual período, limitando-se ao prazo máximo de 24 (vinte e quatro) meses, conforme disposto no § 4º do mesmo artigo.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A Secretaria de Estado da Educação vem investindo em uma rede de comunicação para troca de informação de inteligência antimalware que integra todas Escolas e Setores Administrativos da SEDUC, permitindo que as informações sobre novos malwares, descobertos em qualquer ponto da rede sejam imediatamente disseminadas para Solução de Segurança de Redes NGFW e demais equipamentos compatíveis conectados a esta rede de proteção. Isso permite a mitigação ágil e automatizada de novas ameaças, reduzindo sobremaneira os custos e os riscos associados a ataques por artefatos maliciosos.
3.2. As demandas por serviços digitais vêm, cada vez mais, pressionando a infraestrutura de comunicação de dados e, para suportar a esta pressão, as tecnologias para este segmento vem se renovando e atuando na otimização dos serviços para atender a todos com comodidade e segurança.
3.3. Atualmente a Rede Estadual de Educação de Sergipe é composta por 318 escolas, distribuídas em 75 (setenta e cinco) municípios, com aproximadamente 165.000 (cento e sessenta e cinco mil) alunos matriculados e mais de 12.000 (doze mil) colaboradores. O presente termo prevê o fornecimento de solução de redes conectando todos os pontos de presença da SEDUC, fornecendo acesso as plataformas do Governo do Estado de Sergipe e a internet de maneira ágil e segura.
3.4. Estas aquisições/renovação buscam proporcionar maior proteção aos computadores, resguardando problemas que possam prejudicar os serviços prestados aos alunos, professores e funcionários. Portanto, é uma questão de segurança, que possibilita garantir o desempenho das estações de trabalho e, por conseguinte, disponibilizar aos funcionários condições para a realização de suas atividades e para que estas tarefas sejam executadas com êxito.
3.5. Além do avanço cada vez mais expressivo das técnicas de exploração de vulnerabilidade utilizada, entende-se a necessidade de ampliação das camadas de proteção de cyber segurança neste ambiente, visando a ampliação da maturidade das

soluções de segurança que permitam evitar possíveis ataques, sobretudo em períodos de guerra cibernética.

3.6. A essencialidade desses serviços pode ser comprovada pela hipótese de sua eventual indisponibilidade, o que causaria impactos severos e até mesmo inviabilização da realização dos trabalhos.

3.7. As Soluções de Segurança de Redes da SEDUC estão integradas permitindo notificar em tempo real a todas as estações de trabalho e servidores conectados sobre novas ameaças provenientes da Internet.

3.8. A aquisição e renovação dos itens de forma global em Lote único, garante tanto a integração das soluções como a unicidade técnica dos processos, quanto o nível de serviços prestados, assim como a otimização dos recursos necessários a gerência dos contratos e o foco na melhoria e ampliação do ambiente. O planejamento para esta contratação, de forma global, prevê também a eficiência não dos itens, mas também no âmbito em que se evita contratações conflituosas entre si, pois os equipamentos, soluções, licenciamentos e serviços especificados necessitarão de total integração, além de disponibilização de ferramental que dê visibilidade aos gestores da solução.

3.9. A licitação em lote único, visa permitir e ampliar a eficácia da Gestão de Segurança Cibernética da SEDUC, possibilitando através da compatibilidade e integração dos itens NGFW e Ativos de Rede Wired um gerenciamento unificado com uma inspeção profunda de todo o tráfego de rede. A gerência unificada e a inspeção são capazes de bloquear todo o tráfego direto de redes entre usuários da rede, garantindo que toda intermediação do tráfego interno de rede seja realizada pelo NGFW, com todas as políticas e regras de segurança aplicadas. Essas características realizam através de automações a detecção e respostas a ameaças, além de aplicar políticas de segurança específicas em cada porta dos Ativos de Rede Wired.

3.10. Assim a definição pela contratação em Lote único leva em consideração o prejuízo de ordem técnica ao conjunto dos itens, caso se decidisse pelo parcelamento (fracionamento), uma vez que os itens a serem contratados guardam estrita relação entre si, de forma que hardware, software e serviços possam ser integrados para atingir os resultados pretendidos pela administração.

3.11. Reforçamos a licitação em lote único, tendo em vista que se trata de uma aquisição e renovação de equipamentos que devem ser compatíveis entre si, onde através dos itens de Instalações o fornecedor será responsável por disponibilizar, implantar e configurar todos as soluções, integradas com a solução de segurança cibernética de redes, que necessitam estar integradas para evitar qualquer tipo de incompatibilidade.

3.12. Salientamos o objeto foi dividido em itens para facilitar o gerenciamento do lote, no entanto é necessário que o fornecedor garanta que as funcionalidades que exigem integração entre as soluções sejam plenamente funcionais e o serviço de suporte técnico seja prestado por profissionais especializados e os treinamentos nas soluções fornecidas.

4. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERANDO O CICLO DE VIDA DO

OBJETO E ESPECIFICAÇÃO DO PRODUTO

4.1. Para atendimento integral das demandas elencadas no Documento de Oficialização da Demanda, é necessário a análise da Assessoria de Tecnologia e Informática (ASTIN) que as atenda, relacionando-se com as seguintes premissas:

4.1.1. Subscrição das licenças da Solução de Segurança e Gerência Fortinet por 12 (doze) meses, com o objetivo de garantir a continuidade do ambiente de segurança.

4.1.2. Manutenção da infraestrutura adequada para a segurança da rede, assegurando proteção e disponibilidade.

4.1.3. Orientação em relação às boas práticas de gestão do ambiente, considerando, entre outros, os seguintes aspectos:

4.1.3.1. Avaliação de otimização e gerenciamento – O gerenciamento de recursos é uma prioridade crucial em todo o processo de segurança: Quando ocorrem “gargalos” de rede, isso pode levar a problemas sérios. Assim, são necessárias avaliações abrangentes para ajudar a otimizar a solução Fortinet e garantir capacidade de throughput suficiente.

4.1.3.2. Análise do monitoramento e relatórios – Os ambientes de segurança requerem supervisão constante, monitoramento de desempenho e relatórios proativos, essenciais para evitar problemas complicados e dispendiosos. Para o acompanhamento das alterações, previsíveis ou não, recomenda-se que a equipe de gestão da solução de TI seja orientada por profissionais com conhecimento técnico especializado, para auxiliá-la na avaliação e validação de ações e documentos oriundos da extração dos dados de uso da solução.

4.1.3.3. Gerenciamento de mudanças – O gerenciamento das alterações que ocorrem em um ambiente de segurança é obrigatório para o seu correto funcionamento, devido à sua arquitetura exclusiva. Alterações que podem parecer insignificantes podem ter um grande impacto no desempenho.

4.1.4. A solução deve prover suporte técnico das licenças na modalidade 24x7, com quantitativo ilimitado de chamados. O suporte técnico pode ser remoto, abrangendo toda e qualquer configuração, instalação de atualizações, patches e fixes de software e das licenças, devendo ser capaz de detectar problemas de software e emitir relatórios à SEDUC que indiquem a necessidade de abertura de chamado com o fabricante da Solução de Segurança e Gerência para solicitar o serviço de garantia, durante o período de 12 (doze) meses.

4.1.5. A disponibilização das licenças relativas aos serviços de suporte, atualizações e assistência técnica, deverá ocorrer em até 30 (trinta) dias corridos contados do recebimento, pela empresa contratada, da ordem de empenho a ser emitida e assinada pela SEDUC;

4.1.5.1. Deverão ser disponibilizados para download no site do fabricante, todos os manuais de instalação, configuração e operação do software em sua última versão;

4.1.5.2. A subscrição deverá permitir a atualização da versão do software para a versão mais atual disponível no site do fabricante;

4.1.5.3. Define-se atualização de versão como direito para atualização dos softwares, incluindo versões maiores (major releases), versões menores (minor releases), versões de manutenção (maintenance/patches releases) e atualizações (updates) que forem disponibilizadas para os softwares especificados neste item, tradicionalmente disponibilizadas através de download a partir do site na Web da Fortinet.

4.1.5.4. Devem ser fornecidas as licenças na última versão disponibilizada pelo fabricante;

4.1.6. O prazo de entrega dos equipamentos é de até 60 (sessenta) dias, contados a partir da assinatura do contrato;

4.1.7. O prazo de entrega poderá ser prorrogado mediante justificativa fundamentada por escrito da CONTRATADA, o qual deverá ser encaminhada à CONTRATANTE, antes de findar os prazos previstos nos itens 4.1.5 e 4.1.6;

4.1.8. Os produtos serão recebidos pelos responsáveis pela aquisição da solução, no qual a SEDUC emitirá o Termo de Recebimento Provisório, em até 10 (dez) dias corridos a partir da entrega das mesmas;

4.1.9. Em até 10 (dez) dias corridos contados do recebimento provisório, os responsáveis pela aquisição da solução, receberão definitivamente os produtos, emitindo o Termo de Recebimento Definitivo, verificando a conformidade do objeto quanto às exigências contidas no Edital;

4.2. **Serviços de Suporte de garantia**

4.2.1. Todas as solicitações feitas pela CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços.

4.2.2. No período de cobertura do contrato, a CONTRATADA deverá atender, **no mínimo, 95% (noventa e cinco por cento) dos chamados dentro do prazo mencionado no tempo de atendimento**, cujas informações acerca do andamento do chamado podem ser obtidas através da central de atendimento da FABRICANTE.

4.2.3. Durante o período de Garantia técnica deverá ser permitida a atualização dos firmwares para as versões mais recentes, sem ônus adicional para a SEDUC além daquele já cotado na proposta.

4.3. **Considerações gerais para execução da Garantia:**

4.3.1. A garantia de manutenção corretiva deve considerar:

4.3.1.1. **A abertura de chamados deverá ter recepção imediata**, quando aberto via telefone ou via Internet;

4.3.1.2. **Tempo de atendimento:** tempo decorrido entre o horário de abertura do chamado pelo CONTRATANTE e início do atendimento efetivo da EMPRESA CONTRATADA / FABRICANTE;

4.3.1.3. **Encerramento dos chamados:**

4.3.1.3.1. O aceite do serviço está atrelado ao retorno da normalidade da solução de virtualização afetada conforme manutenção fornecida pela EMPRESA CONTRATADA / FABRICANTE.

4.3.1.4. **Demais condições:**

4.3.1.4.1. A EMPRESA CONTRATADA / FABRICANTE poderá formalizar pedido de prorrogação para os tempos de atendimento, cujas razões expostas serão analisadas pela CONTRATANTE, que decidirá pela dilação do prazo ou aplicação das penalidades previstas no contrato.

4.3.1.4.1.1. **Justificativa:** Permitir a Contratante analisar e decidir sobre o atendimento e aplicação de multas.

4.3.1.4.2. Todas as solicitações feitas pela CONTRATANTE deverão ser registradas pela EMPRESA CONTRATADA / FABRICANTE em sistema informatizado para acompanhamento e controle da execução dos serviços.

4.3.1.4.2.1. **Justificativa**: Acompanhamento e controle dos serviços pela Contratante.

4.3.2. As especificações e características de todos os itens estão detalhadas no **Anexo I** deste Termo de Referência.

5. REQUISITOS DA CONTRATAÇÃO

Sustentabilidade:

5.1. Verificou-se que não há legislação específica e nem foi encontrado no mercado bens ou serviços viáveis com critérios de sustentabilidade para o objeto a ser contratado.

Subcontratação

5.2. Não é admitida a subcontratação do objeto contratual.

Garantia da contratação

5.3. Não haverá exigência da garantia da contratação.

Vistoria

5.4. Os componentes e subcomponentes objetos da proposta deverão possuir integração e compatibilidade com os Sistemas de Segurança, Repositório de Logs e demais equipamentos utilizados pela SEDUC – SECRETARIA DE ESTADO DA EDUCAÇÃO E DA CULTURA.

5.5. Fica facultado à LICITANTE interessada, realizar vistoria técnica na Sede da SEDUC, para tirar todas as dúvidas e tomar conhecimento pleno das condições ambientais e técnicas para a efetiva realização da entrega do solicitado. Não serão aceitas alegações posteriores de desconhecimento das condições necessárias e requerimentos de compatibilidade à execução dos serviços. Caso seja de interesse da LICITANTE, a vistoria técnica deverá ser agendada com a equipe técnica da Assessoria de Tecnologia

e Informática – ASTIN, pelo telefone (79) 3194-3300, até 72 (setenta e duas) horas antes da data do certame.

5.6. A comprovação da visitação será feita através da emissão, pela CONTRATANTE, de Declaração de Vistoria Técnica.

6. MODELO DE EXECUÇÃO DO OBJETO

6.1. *Condições de execução*

6.1.1. A CONTRATADA em até 10 (dez) dias úteis após a assinatura do contrato, deverá iniciar o planejamento para elaboração do Cronograma de instalação do equipamento e licenças, em conjunto com a CONTRATANTE;

6.1.2. Após a assinatura do instrumento contratual e até a entrega dos produtos da solução, serão realizadas reuniões preparatórias, em horário comercial e nas dependências da CONTRATANTE, com a presença dos integrantes da equipe técnica da CONTRATADA, da qual se lavrará ata para permitir o acompanhamento criterioso da execução do objeto;

6.1.3. Será apresentado pela CONTRATADA Projeto Executivo: Elaboração de projeto prévio para a implantação da solução conforme parâmetros do Termo de Referência;

6.1.4. O Plano de Instalação da solução poderá ser recusado pela CONTRATANTE, devendo a CONTRATADA realizar os ajustes definidos em reunião e reapresentá-los;

6.1.5. Sempre antes de qualquer serviço, a CONTRATADA deve efetuar vistoria técnica no local para análise dos detalhes técnicos para execução dos serviços solicitados e, ocorrendo dúvidas, a CONTRATANTE deve ser acionado para os devidos esclarecimentos;

6.1.6. Os serviços de instalação e manutenção não deverão obstruir o andamento das rotinas de trabalho dos ambientes objetos de intervenção. Quando da intervenção nestes ambientes, será de responsabilidade da CONTRATADA, a recomposição total dos mesmos, deixando os locais totalmente limpos e arrumados, inclusive com relação a algum dano a eles causado quando da execução dos serviços;

6.1.7. Quando da execução dos serviços, os locais de trabalho deverão ser mantidos desobstruídos e bem sinalizados, quando for o caso, de maneira a não comprometer a segurança daqueles que ali trafegam;

6.1.8. Após a execução dos serviços, as áreas deverão ser mantidas limpas, retirando-se toda e qualquer impureza e sobras de materiais;

6.1.9. Para facilitar os procedimentos da CONTRATANTE, a CONTRATADA deve apresentar planilhas específicas, para cada local que foi objeto de intervenção, constando relação detalhada dos produtos efetivamente instalados, dos desempenhos esperados e especificação dos procedimentos técnicos e, se couber, dos instrumentos usualmente adotados para se efetuar os testes;

6.1.10. A CONTRATADA, depois de concluído o serviço de instalação da solução, deverá realizar, com acompanhamento dos técnicos da CONTRATANTE, testes de pré-operação para validar que a solução foi instalada de acordo com o Plano de Instalação;
6.1.11. Concluído o serviço de instalação e os testes, a CONTRATADA deverá elaborar a documentação da solução, contendo todas as informações da implantação, como aspectos de arquitetura, configuração, descrição das características e recursos utilizados, testes, integrações e etc.;
6.1.12. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter nome, data e assinatura do técnico responsável da CONTRATADA;
6.1.13. A documentação deverá ser entregue em meio digital (formatos PDF e DOCx);
6.1.14. A documentação deverá ser validada pela equipe técnica da CONTRATANTE, devendo ser ajustada pela CONTRATADA caso seja solicitado.
6.1.15. No prazo de até 10 (dez) dias após a aprovação da documentação pela CONTRATANTE, caracterizando a conclusão dos serviços de instalação, configuração e operação assistida, a CONTRATANTE emitirá o Termo de Homologação;
6.1.16. Durante a etapa de homologação, caso a equipe técnica da CONTRATANTE identifique inconformidade na implantação da solução instalada, é de responsabilidade da CONTRATADA, iniciar as devidas correções num prazo de 3 (três) dias úteis após a emissão do relatório de inconformidade;
6.1.17. Não haverá custos adicionais à CONTRATANTE para a realização das correções apontadas, sendo necessária a atualização da documentação, que foi entregue na etapa de instalação para que a CONTRATANTE realize nova homologação da solução, iniciando-se um novo prazo a ser acordado entre as partes para resolução definitiva das inconformidades identificas;
6.1.18. São condições para a assinatura do Termo de Homologação do Serviço por parte da CONTRATANTE:
6.1.18.1. A CONTRATANTE receber o comunicado da CONTRATADA informando da conclusão dos serviços de instalação, conforme descrito neste Termo de Referência;
6.1.18.2. A CONTRATANTE concluir a avaliação técnica qualitativa conforme condições constantes neste Termo de Referência e constatar que não existem inconformidades na solução instalada;
6.1.19. A CONTRATANTE deve receber toda documentação atualizada que contempla:
6.1.19.1. Visão geral da arquitetura da solução implantada, com desenho da estrutura lógica e física adotada quando necessário;
6.1.19.2. Descrição das etapas do processo de instalação, detalhando as opções de configuração adotadas;

6.1.19.3. Descrição do funcionamento das soluções, incluindo manuais de utilização dos portais web para visibilidade, para procedimento de abertura de chamado junto a CONTRATADA.

6.1.20. Ativação das Licenças:

6.1.20.1. As licenças contratadas deverão ser ativadas no ambiente de TI do CONTRATANTE dentro do prazo máximo de 30 (trinta) dias contados a partir da assinatura do contrato ou do recebimento da ordem de fornecimento;

6.1.20.2. A CONTRATADA será responsável por fornecer instruções detalhadas para a ativação das licenças, garantindo que o CONTRATANTE tenha pleno acesso aos serviços de suporte e atualizações fornecidos;

6.1.21. Disponibilidade do Suporte:

6.1.21.1. O CONTRATANTE terá direito ao suporte técnico especializado, conforme as condições estabelecidas nas licenças adquirida;

6.1.21.2. O suporte deverá estar disponível durante o período de vigência da licença e será oferecido por meio de canais de atendimento (portal, telefone, e-mail) que serão indicados pela CONTRATADA;

6.1.21.3. Qualquer incidente ou problema relacionado às licenças deverá ser reportado, e a CONTRATADA deverá fornecer resposta inicial e solução conforme os níveis de serviço acordados no contrato.

6.1.22. Gestão e Monitoramento do Contrato:

6.1.22.1. A execução do contrato será monitorada pela Assessoria de Tecnologia e Informática – ASTIN do CONTRATANTE, que acompanhará o processo de ativação e o desempenho dos itens contratados;

6.1.22.2. Serão realizados relatórios periódicos de uso e atendimento ao suporte, que deverão ser revisados para garantir que os serviços estejam atendendo às necessidades operacionais do CONTRATANTE.

6.1.23. Documentação e Relatórios:

6.1.23.1. A CONTRATADA deverá entregar ao CONTRATANTE todos os documentos necessários para a gestão das licenças, incluindo manuais de uso, certificados de ativação, termos de suporte e outros documentos relevantes;

6.1.23.2. Ao final do período de licenciamento, a CONTRATADA deverá emitir um comunicado ao CONTRATANTE contendo informações sobre o uso das licenças e possíveis renovações, caso aplicável.

6.1.24. Garantias:

6.1.24.1. A CONTRATADA deverá garantir que as licenças contratadas estejam em total conformidade com as especificações técnicas estabelecidas no Anexo I deste Termo de Referência, garantindo o suporte contínuo e as atualizações de segurança durante o período de vigência do contrato.

6.1.25. Prazo de Vigência:

6.1.25.1. O prazo de vigência do contrato será de 12 (doze) meses, contados a partir da data de ativação das licenças.

6.2. ***Local da prestação dos serviços***

6.2.1. Os serviços serão prestados, na Sede da SEDUC e nas unidades atendidas com a solução de segurança de rede, conforme relação do Anexo II e de acordo com os termos previstos neste Termo de Referência e descrito no contrato com a CONTRATADA.

6.2.2. O endereço completo das unidades pode ser acessado no site da Secretaria https://www.seduc.se.gov.br/redeEstadual/escolas-rede.asp ou solicitado através do e-mail astin.seduc@seduc.se.gov.br

6.3. ***Materiais a serem disponibilizados***

6.3.1. Documentação técnica;

6.3.2. Acesso aos repositórios de software;

6.3.3. O acesso ao portal de suporte;

6.3.4. Atualizações, patches de segurança e novas versões ao longo do período da subscrição;

6.4. ***Informações relevantes para o dimensionamento da proposta***

6.4.1. As especificações e características de todos os itens estão detalhadas no **Anexo I** deste Termo de Referência.

6.4.2. As empresas interessadas em participar dessa licitação devem verificar atentamente as condições estabelecidas no edital e seus anexos, para garantir que suas propostas estão em conformidade com todos os requisitos, especificações e critérios de participação definidos;

6.4.3. A proposta deve descrever as soluções objeto deste Termo de Referência de forma detalhada, apresentando marcas, modelos, versões, serviços a serem prestados e demais informações relevantes, de modo a demonstrar o entendimento integral da contratação;

6.4.4. A proposta de preços terá validade mínima de 90 (noventa) dias a contar da data fixada da sua entrega para início da sessão pública, ainda que a licitante estipule prazo menor ou que não a consigne;

6.4.5. O proponente deverá elaborar a sua proposta escrita de preços de acordo com as exigências constantes deste Termo de Referência, expressando os valores em moeda nacional – reais e centavos, em duas casas decimais, ficando esclarecido que não serão admitidas propostas alternativas;

6.4.6. No valor da proposta deverão estar contempladas todas e quaisquer despesas necessárias ao fiel cumprimento do objeto desta licitação, inclusive todos os custos com material de consumo, salários, encargos sociais, previdenciários e trabalhistas de todo o pessoal da CONTRATADA, como também fardamento, transporte, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, tributos de qualquer natureza (exceto ICMS), impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela Contratada das obrigações;

6.4.7. A composição dos preços deve incidir todos os tributos previstos para os serviços de suporte/assistência técnica, como PIS, COFINS, FUST, FUNTTEL e outros que venham a ser obrigatórios, exceto o ICMS, considerando a isenção de que são favorecidos os órgãos da administração direta, autarquias e fundações estaduais do Estado de Sergipe;

6.4.8. Precedentemente à elaboração da proposta, a licitante deverá observar as cláusulas e disposições deste Termo de Referência, suas informações e condições para o cumprimento das obrigações objeto da licitação, não podendo alegar desconhecimento supervenientemente;

6.4.9. Recomenda-se que a apresentação da proposta e toda documentação entregue deverá estar numerada em ordem crescente e sequencial;

6.4.10. A equipe técnica da Assessoria de Tecnologia e Informática (ASTIN/SEDUC) se reserva o direito de realizar diligências, visitas técnicas e entrevistas, de modo a certificar-se da veracidade dos documentos apresentados pela empresa proponente;

6.4.11. Será desclassificada a LICITANTE que não atender à solicitação de apresentação de documentação técnica que comprove todas as características técnicas exigíveis neste Documento.

6.5. ***Especificação da garantia do serviço***

6.5.1. No momento da entrega das soluções a CONTRATADA deverá apresentar termo de garantia técnica dos produtos e suporte técnico pelo prazo mínimo da vigência contratual de 12 (doze) meses, com cobertura de atendimento a partir da data do recebimento definitivo na CONTRATANTE;

6.5.2. Os equipamentos previstos nesse documento devem possuir garantia on-site com serviço de RMA com envio de equipamentos em até 72 horas úteis e estar licenciado durante toda vigência contratual.

6.6. ***Suporte Técnico e Níveis de Serviço***

6.6.1. Os chamados de suporte técnico e garantia deverão ser abertos por meio de central de abertura de chamados da CONTRATADA, a partir de um número 0800 e ou número local no estado da Sergipe e ou por ambiente WEB, em regime de 24 (vinte e quatro) horas, durante 7 (sete) dias por semana, incluindo-se os dias úteis, feriados e finais de semana, ou por meio de portal na internet. No momento de abertura do chamado, deverá ser fornecido à CONTRATANTE um número único de identificação, data e hora de abertura do chamado. Este será considerado o início para contagem dos prazos estabelecidos. Todos os chamados, bem como as providências adotadas, deverão ser armazenados em sistema da CONTRATADA para controle de chamados. O acesso a esse sistema deverá estar disponível a CONTRATANTE;

6.6.2. Caso a central para abertura de chamados não esteja disponível, os registros dos chamados poderão ocorrer via e-mail, para tanto deverá ser disponibilizados canais necessários;

6.6.3. Os registros de chamado deverão constar as informações fidedignas ao contexto monitorado, informando horários da indisponibilidade e retorno, as intercorrências, se já houve chamado aberto e ações efetuadas para resolver o incidente;

6.6.4. A CONTRATADA deverá realizar os atendimentos através de plantão técnico de suporte on-site 24 (vinte e quatro) horas, 07 (sete) dias por semana;

6.6.5. A CONTRATADA deverá atuar de forma proativa, principalmente nos casos críticos de indisponibilidade, antecipando-se aos problemas das soluções deste termo, garantindo a qualidade do serviço estabelecida nos Níveis Mínimos de Serviço, realizando abertura, acompanhamento e fechamento de chamados técnicos relacionados com indisponibilidade e desempenho das soluções operando em regime 24 horas por dia, 7 dias por semana;

6.6.6. A CONTRATADA deve observar os procedimentos destinados a recolocar em perfeito estado de operação os serviços e equipamentos tais como:

6.6.6.1. No que tange ao hardware: desinstalação, reconfiguração ou reinstalação decorrentes de falhas no hardware, fornecimento de peças de reposição, substituição de hardware, atualização da versão de drivers, firmwares e software básico, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

6.6.6.2. No que tange a software: desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados;

6.6.7. O provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de garantia técnica especificado;

6.6.8. Todas as solicitações feitas pelo CONTRATANTE deverão ser registradas pela CONTRATADA em sistema informatizado para acompanhamento e controle da execução dos serviços e ainda:

6.6.8.1. A CONTRATADA após a realização dos serviços de manutenção deve apresentar um Relatório contendo identificação do chamado, data e hora de abertura do chamado, data e hora do início e término do atendimento, identificação do defeito, técnico responsável pela solução, as providências adotadas e outras informações pertinentes. Este relatório deve ser homologado pela CONTRATANTE, através do gestor do contrato;

6.6.8.2. Os acionamentos dos serviços serão requisitados por meio de chamados (tickets), a serem abertos pelo CONTRATANTE através de número de telefone nacional disponibilizado pela CONTRATADA. Alternativamente os chamados poderão ser abertos por e-mail ou site, desde que a utilização deste canal seja célere o suficiente para permitir o adequado atendimento ao objeto contratual;

6.6.8.3. Não haverá limitação no número de chamados que poderão ser abertos;

6.6.9. A CONTRATADA manterá registro de todos os chamados abertos, disponibilizando, para cada um, no mínimo as seguintes informações:

6.6.9.1. Número sequencial da ordem;

6.6.9.2. Data e hora de abertura;

6.6.9.3. Severidade;

6.6.9.4. Descrição do problema;

6.6.9.5. Data e hora do início do atendimento;

6.6.9.6. Data e hora de término do atendimento (solução).

6.6.10. A CONTRATADA deverá prever os seguintes Níveis de Serviços:

6.6.10.1. Atendimento técnico emergencial local para indisponibilidade total dos serviços:

6.6.10.1.1. Em até 02 (duas) horas para cidade de Aracaju e Região Metropolitana de Aracaju;

6.6.10.1.2. Em até 04 (quatro) horas para demais cidades do Estado de Sergipe;

6.6.10.2. Atendimento técnico emergencial local para indisponibilidade parcial ou degradação dos tempos de acesso e resposta dos serviços:

6.6.10.2.1. Em até 04 (quatro) horas para cidade de Aracaju e Região Metropolitana de Aracaju;

6.6.10.2.2. Em até 08 (oito) horas para demais cidades do Estado de Sergipe;

6.6.10.3. Atendimento técnico para análises, alterações de parâmetros, consulta e suporte geral em até 24 (vinte e quatro) horas.

6.6.10.4. Não serão consideradas indisponibilidades as seguintes situações:

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

6.6.10.4.2. Paradas ocasionadas nos equipamentos por erros de configuração causados pelo CONTRATANTE, sem responsabilidade da CONTRATADA;

6.6.10.4.3. Paradas ocasionadas por casos fortuitos ou de força maior, devidamente comprovados;

6.6.10.5. A ausência de dados coletados pela contratada poderá ser considerada indisponibilidade;

6.6.11. PENALIDADES POR DESCUMPRIMENTO DOS NÍVEIS DE SERVIÇO

6.6.11.1. Na hipótese de não atendimento aos níveis de serviço especificados, sem prejuízo das sanções administrativas previstas no regulamento de licitações e contratos da CONTRATANTE, serão aplicadas as penalidades:

Penalidades por cada hora completa que exceder os níveis de acordo	**Tipo Indisponibilidade**
0,10%	Indisponibilidade Total

0,05%	Indisponibilidade Parcial

6.6.11.1. As penalidades previstas na tabela acima serão calculadas tomando como base o valor da solução do contrato e serão descontadas do valor da garantia contratual, caso exigida no edital, ou dos pagamentos devidos à Contratada;

6.6.11.2. Caso a penalidade a ser aplicada seja superior ao valor da garantia contratual prestada, além da perda desta, responderá o contratado pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela CONTRATANTE ou, ainda, quando for o caso, cobrada judicialmente;

6.6.11.3. A garantia contratual deverá ser restabelecida integralmente, caso tenha incidido qualquer desconto sobre o valor desta;

6.6.11.4. O valor da penalidade no período será igual ao somatório das penalidades de cada ocorrência de não atendimento dos níveis de serviço especificados;

6.6.11.5. As penalidades aplicadas só poderão ser relevadas motivadamente e por conveniência administrativa, mediante ato da autoridade competente, devidamente justificado.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial;

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediantes simples apostila;

7.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim;

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato;

7.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros;

7.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos;

7.7. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;
7.8. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;
7.9. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção;
7.10. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;
7.11. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato;
7.12. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência;
7.13. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário;
7.14. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;
7.15. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;
7.16. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;
7.17. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico e administrativo quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações;

7.18. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 221 do Decreto Estadual nº 342/2023;

7.19. O fiscal administrativo do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual;

7.20. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração;

7.21. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

8. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

8.1. Verificação da Conformidade com a Entrega:

8.1.1. A medição será realizada com base na entrega efetiva dos itens contratados, mediante o recebimento do relatório de medição emitido pela CONTRATADA, comprovando o direito de uso do software pelo período especificado para cada lote;

8.1.2. A entrega será considerada concluída quando o CONTRATANTE confirmar, por meio de documento de aceite, que os produtos foram entregues e os serviços foram devidamente executados, conforme os termos do contrato.

8.2. Processo de Medição:

8.2.1. A medição será feita após a ativação de todas as licenças contratadas e ao final de cada produto e/ou serviço entregue, de acordo com as especificações previstas no Anexo I deste Termo de Referência;

8.2.2. Caso o fornecimento seja fracionado, poderão ser realizadas medições parciais, desde que acordado entre as partes.

8.3. Critérios de Pagamento:

8.3.1. O pagamento será efetuado em parcelas, após a conclusão da medição e a aceitação formal dos produtos pelo CONTRATANTE;

8.3.2. O prazo para pagamento será de até 30 (trinta) dias corridos após a apresentação da nota fiscal correspondente, devidamente atestada pela Assessoria de Tecnologia e Informática – ASTIN/SEDUC, e após o recebimento e aceitação dos documentos de conformidade e garantia;

8.3.3. O pagamento será realizado por meio de transferência bancária para a conta indicada pela CONTRATADA.

8.4. Penalidades e Retenções:

8.4.1. Caso sejam identificadas não conformidades durante a verificação da entrega, o pagamento poderá ser suspenso até que a CONTRATANTE realize as correções necessárias, sem prejuízo das penalidades previstas no contrato;

8.4.2. Será aplicada retenção de tributos conforme a legislação vigente, sendo descontados diretamente no momento do pagamento.

8.5. ***Do Recebimento***

8.5.1. A disponibilização das licenças dos softwares e as relativas aos serviços de suporte, atualizações e assistência técnica, deverá ocorrer em até 30 (trinta) dias corridos contados do recebimento, pela empresa contratada, da ordem de empenho a ser emitida e assinada pela SEDUC;

8.5.2. O prazo de entrega dos equipamentos é de até 60 (sessenta) dias, contados a partir da assinatura do contrato;

8.5.3. O prazo de entrega poderá ser prorrogado mediante justificativa fundamentada por escrito da CONTRATADA, o qual deverá ser encaminhada à CONTRATANTE, antes de findar os prazos previstos nos itens 8.5.1 e 8.5.2;

8.5.4. O objeto do contrato será recebido provisoriamente, no prazo de 10 (dez) dias, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo;

8.5.5. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga;

8.5.6. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico;

8.5.7. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo;

8.5.8. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato apurará o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato;

8.5.9. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório;

8.5.10. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório;

8.5.11. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis;

8.5.12. Os produtos e/ou serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Anexo I deste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

8.5.13. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo;

8.5.14. Os produtos e/ou serviços serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo aos seguintes procedimentos:

8.5.14.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico e administrativo, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento;

8.5.14.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

8.5.14.3. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas;

8.5.14.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização;

8.5.14.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

8.5.15. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento;

8.5.16. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela CONTRATADA, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança;

8.5.17. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

8.6. ***Prazo de pagamento***

8.6.1. O pagamento será efetuado após liquidação da despesa por meio de crédito em conta corrente indicada pelo licitante(s) vencedor(es), no prazo de até 30 (trinta) dias consecutivos, mediante a apresentação de Nota Fiscal/Fatura, devidamente certificada e atestada pelo setor responsável pelo acompanhamento e fiscalização do órgão contratante;

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

9.1. ***Forma de seleção e critério de julgamento da proposta***

9.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

9.1.2. Critério de Habilitação (Técnica Operacional)

9.1.2.1. Os serviços de implantação dos equipamentos e soluções de segurança deverão ser prestados pelo próprio fabricante (Professional Services) ou parceiro (revenda ou assistência técnica) autorizada pelo fabricante.

9.1.2.2. O licitante deverá comprovar prévia experiência com a execução de atividades pertinentes e compatíveis com o objeto do edital. Tal comprovação deverá ser feita através da apresentação de Atestado (s) de Capacidade Técnica (ACT), fornecido por pessoa jurídica de direito público ou privado, comprobatório da capacidade técnica para atendimento ao objeto da presente licitação, com indicação da quantidade fornecida, da qualidade do material, do atendimento, do cumprimento de prazos e demais condições de fornecimento. Para tanto, o (s) atestado (s) deverá (ão) comprovar o prévio fornecimento do objeto licitado em quantidade mínima de 50% (cinquenta por cento) do total de equipamentos solicitados no edital.

9.1.2.3. Os atestados deverão ser impressos em papel timbrado, com nome e telefone de contato dos responsáveis pela informação atestada, não sendo aceitas declarações genéricas de catálogos, manuais de Internet, devendo ainda atestar a satisfação com o serviço ofertado pela PROPONENTE.

9.1.2.4. A CONTRATANTE se reserva o direito de conferir as informações prestadas pelas empresas emitentes dos atestados, através de consultas e visitas, bem como a disponibilidade de equipamentos solicitados junto à PROPONENTE.

9.1.3. A PROPONENTE deve apresentar os seguintes documentos:

9.1.3.1. Declaração do fabricante dos equipamentos que é revenda autorizada e certificando a capacitação da licitante para participação específica no presente procedimento;

9.1.3.2. Certidão vigente de registro e quitação da empresa licitante expedido pelo órgão profissional competente (CREA);

9.1.3.3. Comprovação que possui em seu quadro permanente de profissionais pelo menos um engenheiro eletricista ou um engenheiro de telecomunicações, responsáveis técnicos devidamente registrados no CREA (Conselho Regional de Engenharia e Arquitetura) na data de abertura do Certame. A comprovação de vínculo empregatício será através da apresentação de cópia autenticada do contrato social da empresa em caso de sócio ou de cópia da carteira de trabalho do profissional em caso de empregado;

9.1.3.4. Declaração de que dispõe de mão-de-obra adequada e disponível, além de local para execução dos serviços técnicos na cidade de Aracaju – SE. Deverão ser apresentados, profissionais técnicos com certificações dos equipamentos fornecidos neste edital, devidamente treinados pelo fabricante para instalar, configurar e manter Soluções de Segurança do Fabricante das Soluções, devendo estes treinamentos técnicos serem comprovados por certificados de qualificação técnica vigentes e estes serão responsáveis pela execução dos serviços;

9.1.3.5. Prospecto com as características técnicas de todos os componentes dos equipamentos, incluindo especificação de marca, modelo e outros elementos que, de forma inequívoca, identifiquem e comprovem as configurações cotadas, possíveis expansões e upgrades, através de certificados, manuais técnicos, folders e demais literaturas técnicas editadas pelos fabricantes. Serão aceitas cópias das especificações obtidas em websites dos fabricantes na Internet, em que conste o respectivo endereço eletrônico;

9.1.3.6. Indicação exata do modelo de equipamento ofertado na Proposta de Preços, sendo os respectivos catálogos obrigatoriamente de domínio público, ou seja, deverão estar publicados no website do fabricante, comprovando todos os recursos e funcionalidades mínimas exigidas para os equipamentos que irão integrar as características técnicas solicitadas no Anexo I;

10. DO CONTRATO

10.1. Será firmado Contrato com o licitante vencedor, assinado por ambas as partes, o qual terá vigência conforme descrito no item 2 deste Termo de Referência;

10.2. A empresa deverá comparecer no prazo máximo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, por escrito, para assinatura do Contrato;

10.3. Decorrido o prazo de 05 (cinco) dias úteis, contados do recebimento do comunicado oficial para assinatura do contrato e não tendo a empresa vencedora comparecido ao chamamento, perderá o direito à contratação e estará sujeita às penalidades previstas em edital;

11. OBRIGAÇÕES DA CONTRATADA

A CONTRATADA, além das determinações contidas no instrumento convocatório, bem como daquelas decorrentes de lei, obriga-se a:

11.1. Cumprir fielmente as condições e exigências contidas neste Termo de Referência e seus anexos.

11.2. Indicar formalmente o Preposto responsável pela supervisão permanente dos serviços prestados, durante todo o período de vigência do contrato, com poderes de representante legal e um substituto para tratar de todos os assuntos relacionados ao contrato, sem ônus adicional para o CONTRATANTE.

11.3. Realizar os serviços dentro dos prazos e qualidades especificadas e, no que forem aplicáveis, com as normas do fabricante e da ABNT, além das prescrições da legislação pertinente.

11.4. Fiscalizar o cumprimento do objeto do contrato, cabendo-lhe integralmente os ônus decorrentes, fiscalização essa que se dará independentemente da que será exercida pelo CONTRATANTE.

11.5. Comunicar à equipe de fiscalização do CONTRATANTE, formalmente, a constatação de quaisquer condições inadequadas de execução dos serviços ou a iminência de fatos que possam prejudicar a perfeita execução do contrato.

11.6. Prestar todos os esclarecimentos que forem solicitados pela equipe de fiscalização do contrato.

11.7. Planejar a execução e a supervisão dos serviços.

11.8. Comunicar ao CONTRATANTE, no período mínimo de 24 (vinte e quatro) horas antes da data estabelecida para entrega de produtos e/ou realização dos serviços, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

11.9. Orientar regularmente seus empregados acerca da adequada metodologia de otimização dos serviços, dando ênfase à economia no emprego de materiais e à racionalização de energia elétrica no uso dos equipamentos.

11.10. Substituir, às suas expensas, todo e qualquer material que estiver em desacordo com as especificações e também aquele em que for constatado dano em decorrência de transporte ou acondicionamento, após a notificação formal do CONTRATANTE.

11.11. Corrigir, as suas expensas, no todo ou em parte, a execução dos serviços em que forem constatadas imperfeições, vícios, defeitos ou incorreções e que estiverem em desacordo com as especificações, após a notificação formal do CONTRATANTE.

11.12. Solicitar por escrito e devidamente fundamentado quaisquer modificações na execução dos serviços, para análise e decisão do CONTRATANTE.

11.13. Comunicar imediatamente ao Fiscal do Contrato toda e qualquer irregularidade ou dificuldade que impossibilite a execução dos serviços.

11.14. Arcar com todas as despesas diretas e indiretas, decorrentes do cumprimento das obrigações assumidas, sem qualquer ônus adicional para o CONTRATANTE.

11.15. Manter durante todo o período de execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas para sua contratação.

11.16. Responder, integralmente, por perdas e danos que vier a causar diretamente ao CONTRATANTE ou a terceiros em razão ou omissão, dolosa ou culposa, sua ou dos seus representantes ou prepostos, ficando obrigada a promover a devida restauração e/ou o ressarcimento a preços atualizados, dentro de 30 (trinta) dias contados da comprovação de sua responsabilidade. Caso não o faça no prazo estipulado, o CONTRATANTE reserva-se o direito de descontar o ressarcimento do valor da fatura do mês e/ou da garantia, sem prejuízo de poder denunciar o Contrato, de pleno direito, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

11.17. Não será aceita, sob nenhum pretexto, a transferência de responsabilidades da CONTRATADA para terceiros, sejam fabricantes, representantes ou quaisquer outros.

11.18. A CONTRATADA deverá manter em seu quadro, pessoal suficiente para atendimento dos serviços, conforme previsto nesta especificação, sem interrupção, seja por motivo de férias, descanso semanal, licença, greve, falta ao serviço e demissão de empregados, os quais não terão em hipótese alguma, qualquer relação de emprego com o CONTRATANTE.

11.19. Proibir a veiculação de publicidade ou qualquer outra informação acerca do objeto do contrato, salvo se houver prévia autorização da administração do CONTRATANTE.

11.20. Também não será permitido:

11.20.1. Reproduzir, divulgar ou utilizar em benefício próprio, ou de terceiros, quaisquer informações de que tenha tomado ciência em razão da execução dos serviços discriminados, sem o consentimento prévio e por escrito do CONTRATANTE;

11.20.2. Permitir que seus empregados pratiquem a venda de quaisquer mercadorias e produtos nas dependências do CONTRATANTE, bem como que executem atividades incompatíveis com as previstas neste Termo de Referência;

11.20.3. Utilizar o nome do CONTRATANTE, ou sua qualidade de CONTRATADA, em quaisquer atividades de divulgação empresarial, como, por exemplo, em cartões de visita, anúncios e impressos, sem o consentimento prévio e por escrito do CONTRATANTE;

11.20.4. Transferir a outrem, no todo ou em parte, o objeto do presente Termo de Referência, sem prévia e expressa anuência do CONTRATANTE.

11.21. Quanto às obrigações gerais:

11.21.1. Para efetivar a contratação, a empresa deverá comprovar regularidade perante a Receita Federal, FGTS, Justiça do Trabalho, Receita Estadual, Receita

Municipal, Tribunal de Contas da União (TCU) e INSS;

11.21.2. Disponibilizar o endereço comercial, telefone e uma conta de e-mail para fins de comunicação entre as partes, mantendo-os atualizados;

11.21.3. Deverá a CONTRATADA atender e se adequar ao disposto na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD).

11.22. Utilizar exclusivamente o Sistema de Protocolo Eletrônico do Estado de Sergipe (disponível em https://www.edocsergipe.se.gov.br/protocolo-externo/) para envio de documentação, incluindo notas fiscais/faturas.

12. OBRIGAÇÕES DA CONTRATANTE

A CONTRATANTE, além das determinações contidas no instrumento convocatório, bem como daquelas decorrentes de lei, obriga-se a:

12.1. Prestar informações e esclarecimentos pertinentes e necessários que venham a ser solicitados pela CONTRATADA.

12.2. Assegurar o acesso dos empregados da CONTRATADA aos locais em que devam executar suas atividades e disponibilizar meios de identificação (crachá) a esses funcionários. Assim, por meio do setor de segurança do CONTRATANTE, manterá ficha cadastral atualizada dos representantes da empresa.

12.3. Conferir os materiais, equipamentos e/ou serviços discriminados no Estudo Técnico Preliminar e/ou no Termo de Referência e registrar as divergências quanto a quantidade e qualidade previstas.

12.4. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido.

12.5. Emitir o aceite do objeto contratado após verificação das especificações, rejeitando o que não estiver de acordo, por meio de notificação à CONTRATADA.

12.6. Efetuar os pagamentos à CONTRATADA nos prazos previstos na legislação em vigor, após o cumprimento das formalidades legais.

12.7. Fiscalizar o atendimento ao disposto no Art. 4º da Resolução CNMP nº 177/2017, de 5 de julho de 2017, quanto à vedação de atribuição de cargo de chefia a empregado que tenha praticado ato(s) tipificado(s) como causa(s) de inelegibilidade prevista na legislação eleitoral.

12.8. Exercer, quando lhe convier, fiscalização sobre os serviços contratados e, ainda, aplicar as penalidades previstas neste instrumento ou rescindir o contrato, caso a CONTRATADA descumpra quaisquer das obrigações assumidas em contrato.

12.9. Será(ão) nomeado(s) Fiscal(is) de Contrato, que ficará(ão) responsável(eis) pela

fiscalização e acompanhamento da execução do objeto contratado, o(s) qual(is) fará(ão) anotações e registros de todas as ocorrências e determinará(ão) o que for necessário à regularização das falhas ou defeitos observados para o fiel cumprimento das cláusulas e condições estabelecidas. Ademais, ficará a cargo do(s) fiscal(is) atestar a nota fiscal quando do recebimento definitivo, o que não exclui nem reduz as responsabilidades da CONTRATADA.

12.9.1. O(s) Fiscal(is) de Contrato terá(ão) poderes para:

a) Definir toda e qualquer ação de orientação, gerenciamento, controle e acompanhamento da execução do Contrato, determinando as providências cabíveis;

b) Notificar a CONTRATADA, por escrito, acerca da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

c) Suspender a execução dos serviços, total ou parcialmente, em qualquer tempo, quando estes não estiverem sendo executados dentro dos parâmetros estabelecidos no Contrato, submetendo o caso à Autoridade Competente para decisão.

12.10. O CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

ANEXO I DO TERMO DE REFERÊNCIA - ESPECIFICAÇÕES TÉCNICAS

1. ITEM 01 – SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW - TIPO I

1.1. CARACTERÍSTICAS GERAIS:

1.1.1. Solução baseada em appliance. para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

1.1.2. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.

1.1.3. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze meses), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações e contextos virtuais. Após a vigência contratual as funcionalidades que não necessitam de atualizações online continuam ativas em funcionamento sem novas atualizações e suporte do fabricante.

1.1.4. Deve possuir fonte de alimentação redundante hot swappable com chaveamento automático 110/220V. A fonte fornecida deve suportar sozinha a operação da unidade com todos os módulos de interface ativos.

1.1.5. Deve possuir firewall com capacidade mínima de processamento de 70 (setenta) Gbps.

1.1.6. Deve possuir IPS com capacidade mínima de processamento de 10 (dez) Gbps.

1.1.7. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 8,5 (oito e meio) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

1.1.8. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 7 (sete) Gbps.

1.1.9. Deve possuir VPN com capacidade de, pelo menos, 50 (cinquenta) Gbps de

tráfego IPSec.

1.1.10. Deve suportar 7.000.000 (sete milhões) conexões simultâneas.

1.1.11. Deverão ser licenciados para suportar, pelo menos, 4500 (quatro mil e quinhentos) usuários de VPN SSL.

1.1.12. Deve suportar, pelo menos, 400.000 (quatrocentos mil) novas conexões por segundo.

1.1.13. Deve suportar, pelo menos, 1.500 (mil e quinhentos) túneis de VPN Site-Site.

1.1.14. Deve suportar, pelo menos, 40.000 (quarenta mil) túneis de VPN Client-Site.

1.1.15. Deve possuir, pelo menos, 06 (seis) interfaces SFP+ 10GE.

1.1.16. Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.

1.1.17. Deve possuir, pelo menos, 14 (quatorze) interfaces RJ 45.

1.1.18. Deve incluir licença para a funcionalidade de VPN SSL.

1.1.19. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.

1.1.20. Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 70(setenta) equipamentos.

1.1.21. Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 250(duzentos e cinquenta) equipamentos.

1.1.22. Deve ser compatível com atual Solução de Gerência Centralizada de Equipamentos do fabricante Fortinet, existente na SEDUC.

1.1.23. Deve ser compatível com atual Solução Centralizada de Armazenamento de Logs e Relatórios do fabricante Fortinet, existente na SEDUC.

1.1.24. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

1.1.25. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

1.2. FUNCIONALIDADE DE FIREWALL

1.2.1. Deve possuir controle de acesso à internet por endereço IP de origem e destino;

1.2.2. Deve possuir controle de acesso à internet por sub rede;

1.2.3. Deve suportar tags de VLAN (802.1q);

1.2.4. Deve possuir ferramenta de diagnóstico do tipo tcpdump;

1.2.5. Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

1.2.6. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

1.2.7. Deve suportar single-sign-on para Active Directory, RADIUS;

1.2.8. Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

1.2.9. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

1.2.10. Deve permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

1.2.11. Deve permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

1.2.12. Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

1.2.13. Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

1.2.14. Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;

1.2.15. Deve suportar aplicações multimídia, como: H.323 e SIP;

1.2.16. Deve possuir tecnologia de firewall do tipo Statefull;

1.2.17. Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

1.2.18. Deve permitir o funcionamento em modo transparente tipo “bridge” sem

alterar o endereço MAC do tráfego;

1.2.19. Deve suportar PBR – Policy Based Routing;

1.2.20. Deve permitir a criação de VLANS no padrão IEEE 802.1q;

1.2.21. Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

1.2.22. Deve permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

1.2.23. Deve permitir forwarding de camada 2 para protocolos não IP;

1.2.24. Deve suportar forwarding multicast;

1.2.25. Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;

1.2.26. Deve permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

1.2.27. Deve permitir o agrupamento de serviços;

1.2.28. Deve permitir o filtro de pacotes sem a utilização de NAT;

1.2.29. Deve permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

1.2.30. Deve possuir mecanismo de anti-spoofing;

1.2.31. Deve permitir criação de regras definidas pelo usuário;

1.2.32. Deve permitir o serviço de autenticação para tráfego HTTP e FTP;

1.2.33. Deve permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

1.2.34. Deve possuir a funcionalidade de balanceamento e contingência de links;

1.2.35. Deve suportar sFlow;

1.2.36. O dispositivo deve ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas.

1.2.37. Deve ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

1.2.38. Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

1.2.39. Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

1.2.40. Deve suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

1.2.41. Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;

1.2.42. Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

1.2.43. Deve suportar SIP, H.323 e SCCP NAT Traversal;

1.2.44. Deve permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

1.2.45. Deve possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

1.3. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

1.3.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

1.3.2. Deve permitir modificação de valores DSCP para o DiffServ;

1.3.3. Deve permitir priorização de tráfego e suportar ToS;

1.3.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

1.3.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active

Directory, reconhecendo grupos de usuários cadastrados;

1.3.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

1.3.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

1.3.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

1.3.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

1.3.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

1.4. FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

1.4.1. Deve permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;

1.4.2. Deve possuir filtragem de e-mail por palavras chaves;

1.4.3. Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

1.4.4. Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL;

1.4.5. Deve permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

1.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

1.5.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;

1.5.2. Deve possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

1.5.3. Deve possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;

1.5.4. Deve possuir a funcionalidade de cota de tempo de utilização por categoria;

1.5.5. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

1.5.5.1. Proxy anônimo;

1.5.5.2. Webmail;

1.5.5.3. Instituições de saúde;

1.5.5.4. Notícias;

1.5.5.5. Phishing;

1.5.5.6. Hackers;

1.5.5.7. Pornografia;

1.5.5.8. Racismo;

1.5.5.9. Websites pessoais;

1.5.5.10. Compras;

1.5.6. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

1.5.7. Deve permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;

1.5.8. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

1.5.9. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado;

1.5.10. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

1.5.11. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

1.5.12. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

1.5.13. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

1.5.14. Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;

1.5.15. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

1.5.16. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

1.5.17. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

1.5.18. Deve filtrar o conteúdo baseado em categorias em tempo real;

1.5.19. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

1.5.20. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

1.5.21. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

1.5.22. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem;

1.5.23. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;

1.5.24. Deve permitir o bloqueio de redirecionamento HTTP;

1.5.25. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

1.5.26. Deve possuir Proxy Explícito e Transparente;

1.5.27. Deve implementar roteamento WCCP e ICAP;

1.6. FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

1.6.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

1.6.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

1.6.3. Deve estar orientado à proteção de redes;

1.6.4. Deve permitir funcionar em modo transparente, sniffer e router;

1.6.5. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

1.6.6. Deve permitir a criação de padrões de ataque manualmente;

1.6.7. Deve possuir integração à plataforma de segurança;

1.6.8. Deve possuir capacidade de remontagem de pacotes para identificação de ataques;

1.6.9. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;

1.6.10. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

1.6.11. Deve possuir mecanismos de detecção/proteção de ataques;

1.6.12. Deve possuir reconhecimento de padrões;

1.6.13. Deve possuir análise de protocolos;

1.6.14. Deve possuir detecção de anomalias;

1.6.15. Deve possuir detecção de ataques de RPC (Remote Procedure Call);

1.6.16. Deve possuir proteção contra-ataques de Windows ou NetBios;

1.6.17. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

1.6.18. Deve possuir proteção contra-ataques DNS (Domain Name System);

1.6.19. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;

1.6.20. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);

1.6.21. Deve possuir métodos de notificação de detecção de ataques;

1.6.22. Deve possuir alarmes na console de administração;

1.6.23. Deve possuir alertas via correio eletrônico;

1.6.24. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

1.6.25. Deve ter a capacidade de resposta/logs ativa a ataques;

1.6.26. Deve prover a terminação de sessões via TCP resets;

1.6.27. Deve armazenar os logs de sessões;

1.6.28. Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

1.6.29. Deve mitigar os efeitos dos ataques de negação de serviços;

1.6.30. Deve permitir a criação de assinaturas personalizadas;

1.6.31. Deve possuir filtros de ataques por anomalias;

1.6.32. Deve permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

1.6.33. Deve permitir filtros de anomalias de protocolos;

1.6.34. Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

1.6.35. Deve suportar verificação de ataque na camada de aplicação;

1.6.36. Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;

1.6.37. Deve possuir as seguintes estratégias de bloqueio: pass, drop e reset.

1.7. FUNCIONALIDADE DE VPN

1.7.1. Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

1.7.2. Deve possuir suporte a certificados PKI X.509 para construção de VPNs;

1.7.3. Deve possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;

1.7.4. Deve possuir suporte a VPN SSL;

1.7.5. Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

1.7.6. A VPN SSL deve possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;

1.7.7. Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

1.7.8. A VPN SSL deve suportar cliente para plataforma Windows, Linux e Mac OS X;

1.7.9. Deve permitir a arquitetura de VPN hub and spoke;

1.7.10. Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

1.8. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

1.8.1. Deve reconhecer, no mínimo, 2.000 (duas mil) aplicações;

1.8.2. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

1.8.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

1.8.3.1. P2P

1.8.3.2. Instant Messaging;

1.8.3.3. Web client;

1.8.3.4. Transferência de arquivos;

1.8.3.5. VoIP;

1.8.4. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

1.8.5. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

1.8.6. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

1.8.7. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

1.8.8. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

1.8.9. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

1.8.10. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

1.8.11. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

1.8.12. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

1.8.13. Deve permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;

1.8.14. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

1.8.15. Deve permitir criação de padrões de aplicação manualmente;

1.9. FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

1.9.1. Deve permitir a criação de endereços IPs virtuais;

1.9.2. Deve permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

1.9.3. Deve suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

1.9.4. Deve permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;

1.9.5. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;

1.9.6. Deve permitir que seja mantido o IP de origem;

1.9.7. Deve suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

1.9.8. Deve ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

1.9.9. Deve permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

1.10. FUNCIONALIDADE DE VIRTUALIZAÇÃO

1.10.1. Deve suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

1.10.2. Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais;

1.10.3. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

1.11. FUNCIONALIDADE DE CONTROLADORA WIRELESS E WI-FI

1.11.1. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante;

1.11.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

1.11.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido;

1.11.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;

1.11.5. Deverá permitir a visualização dos clientes conectados;

1.11.6. Deverá prover suporte a Fast Roaming;

1.11.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;

1.11.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

1.11.9. Deverá possuir Captive Portal por SSID;

1.11.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs;

1.11.11. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;

1.11.12. Deverá suportar os seguintes métodos de autenticação EAP:

1.11.12.1. EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA;

1.11.13. Deverá suportar 802.1x através de RADIUS;

1.11.14. Deverá suportar filtro baseado em endereço MAC por SSID;

1.11.15. Deverá permitir configurar parâmetros de rádio, como: banda e canal;

1.11.16. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

1.11.17. Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;

1.11.18. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

1.11.19. Deverá possuir WIDS com, ao menos, os seguintes perfis:

1.11.19.1. Rogue/Interfering AP Detection;

1.11.19.2. Ad-hoc Network Detection;

1.11.19.3. Wireless Bridge Detection;

1.11.19.4. Weak WEP Detection;

1.11.19.5. MAC OUI Checking;

1.11.20. Deverá permitir o uso de voz e dados sobre um mesmo SSID;

1.11.21. 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 em dBm;

1.11.22. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário;

1.11.23. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs;

1.11.24. Deverá permitir a criação de políticas de traffic shaping;

1.11.25. Deverá permitir a criação de políticas de firewall baseadas em horário;

1.11.26. Deverá permitir NAT nas políticas de firewall;

1.11.27. Deverá possibilitar definir número de clientes por SSID;

1.11.28. Deverá permitir e/ou bloquear o tráfego entre SSIDs;

1.11.29. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

1.11.30. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;

1.11.31. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;

1.11.32. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;

1.11.33. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou

1.11.34. rádios;

1.11.35. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;

1.11.36. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;

1.11.37. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;

1.11.38. 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 trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;

1.11.39. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora;

1.11.40. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;

1.11.41. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

1.11.42. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora;

1.11.43. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora;

1.11.44. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

1.11.45. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora;

1.11.46. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do

tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora;

1.11.47. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede;

1.12. FUNCIONALIDADE DE SD-WAN

1.12.1. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web;

1.12.2. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;

1.12.3. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN;

1.12.4. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações;

1.12.5. Solução deve ser capaz de prover Zero Touch provisioning;

1.12.6. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN;

1.12.7. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz;

1.12.8. A solução deve ser capaz de criar VPN "Full-Mesh" em interface gráfica ou CLI, de forma automática, e sem que o administrador precise configurar site por site;

1.12.9. A configuração VPN IPSEC deve oferecer suporte para DH Group: 14 e 15;

1.12.10. Reconhecimento em camada 7 totalmente segregado da camada 4;

1.12.11. Deve de forma alternativa, contar com um banco de Dados interno, onde

seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino;

1.12.12. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

1.12.13. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc);

1.12.14. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6;

1.12.15. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada;

1.12.16. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

1.12.17. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 a 50) do seu valor de saúde melhor que o link atual;

1.12.18. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema;

1.12.19. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

2. ITEM 02 – SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW - TIPO II

2.1. CARACTERÍSTICAS GERAIS:

2.1.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

2.1.2. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.

2.1.3. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze meses), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações e contextos virtuais. Após a vigência contratual as funcionalidades que não necessitam de atualizações online continuam ativas em funcionamento sem novas atualizações e suporte do fabricante.

2.1.4. Deve possuir fonte de alimentação com chaveamento automático 110/220V redundante. A fonte fornecida Deve suportar sozinha a operação da unidade com todos os módulos de interface ativos.

2.1.5. Deve possuir firewall com capacidade mínima de processamento de 10 (dez)Gbps.

2.1.6. Deve possuir IPS com capacidade mínima de processamento de 2 (dois) Gbps.

2.1.7. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1 (um) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

2.1.8. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 1 (um) Gbps Gbps.

2.1.9. Deve possuir VPN com capacidade de, pelo menos, 09 (nove) Gbps de tráfego IPSec.

2.1.10. Deve suportar 1.000.000 (um milhão) conexões simultâneas.

2.1.11. Deverão ser licenciados para suportar, pelo menos, 400 (quatrocentos) usuários de VPN SSL.

2.1.12. Deve suportar, pelo menos, 50.000 (cinquenta mil) novas conexões por segundo.

2.1.13. Deve suportar, pelo menos, 1.500 (mil e quinhentos) túneis de VPN Site-Site.

2.1.14. Deve suportar, pelo menos10.000 (dez mil) túneis de VPN Client-Site.

2.1.15. Deve possuir, pelo menos, 02 (duas) interfaces SFP+ 10GE.

2.1.16. Deve possuir, pelo menos, 06 (seis) interfaces SFP 1GE.

2.1.17. Deve possuir, pelo menos, 14 (quatorze) interfaces RJ 45.

2.1.18. Deve incluir licença para a funcionalidade de VPN SSL.

2.1.19. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.

2.1.20. Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 30(trinta) equipamentos.

2.1.21. Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 60(sessenta) equipamentos.

2.1.22. Deve ser compatível com atual Solução de Gerência Centralizada de Equipamentos do fabricante Fortinet, existente na SEDUC.

2.1.23. Deve ser compatível com atual Solução Centralizada de Armazenamento de Logs e Relatórios do fabricante Fortinet, existente na SEDUC.

2.1.24. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

2.1.25. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

2.2. FUNCIONALIDADE DE FIREWALL

2.2.1. Deve possuir controle de acesso à internet por endereço IP de origem e destino;

2.2.2. Deve possuir controle de acesso à internet por sub rede;

2.2.3. Deve suportar tags de VLAN (802.1q);

2.2.4. Deve possuir ferramenta de diagnóstico do tipo tcpdump;

2.2.5. Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

2.2.6. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

2.2.7. Deve suportar single-sign-on para Active Directory, RADIUS;

2.2.8. Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

2.2.9. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

2.2.10. Deve permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

2.2.11. Deve permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

2.2.12. Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

2.2.13. Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

2.2.14. Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;

2.2.15. Deve suportar aplicações multimídia, como: H.323 e SIP;

2.2.16. Deve possuir tecnologia de firewall do tipo Statefull;

2.2.17. Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

2.2.18. Deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;

2.2.19. Deve suportar PBR – Policy Based Routing;

2.2.20. Deve permitir a criação de VLANS no padrão IEEE 802.1q;

2.2.21. Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

2.2.22. Deve permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

2.2.23. Deve permitir forwarding de camada 2 para protocolos não IP;

2.2.24. Deve suportar forwarding multicast;

2.2.25. Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;

2.2.26. Deve permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

2.2.27. Deve permitir o agrupamento de serviços;

2.2.28. Deve permitir o filtro de pacotes sem a utilização de NAT;

2.2.29. Deve permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

2.2.30. Deve possuir mecanismo de anti-spoofing;

2.2.31. Deve permitir criação de regras definidas pelo usuário;

2.2.32. Deve permitir o serviço de autenticação para tráfego HTTP e FTP;

2.2.33. Deve permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

2.2.34. Deve possuir a funcionalidade de balanceamento e contingência de links;

2.2.35. Deve suportar sFlow;

2.2.36. O dispositivo deve ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas.

2.2.37. Deve ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

2.2.38. Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

2.2.39. Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

2.2.40. Deve suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

2.2.41. Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;

2.2.42. Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

2.2.43. Deve suportar SIP, H.323 e SCCP NAT Traversal;

2.2.44. Deve permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

2.2.45. Deve possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

2.3. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

2.3.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

2.3.2. Deve permitir modificação de valores DSCP para o DiffServ;

2.3.3. Deve permitir priorização de tráfego e suportar ToS;

2.3.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

2.3.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

2.3.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

2.3.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

2.3.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

2.3.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por

subrede de origem e destino;

2.3.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

2.4. FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

2.4.1. Deve permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;

2.4.2. Deve possuir filtragem de e-mail por palavras chaves;

2.4.3. Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

2.4.4. Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL;

2.4.5. Deve permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

2.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

2.5.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;

2.5.2. Deve possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

2.5.3. Deve possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;

2.5.4. Deve possuir a funcionalidade de cota de tempo de utilização por categoria;

2.5.5. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

2.5.5.1. Proxy anônimo;

2.5.5.2. Webmail;

2.5.5.3. Instituições de saúde;

2.5.5.4. Notícias;

2.5.5.5. Phishing;

2.5.5.6. Hackers;

2.5.5.7. Pornografia;

2.5.5.8. Racismo;

2.5.5.9. Websites pessoais;

2.5.5.10. Compras;

2.5.6. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

2.5.7. Deve permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;

2.5.8. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

2.5.9. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado;

2.5.10. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

2.5.11. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

2.5.12. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

2.5.13. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

2.5.14. Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;

2.5.15. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

2.5.16. Deve permitir a criação de listas personalizadas de URLs permitidas (lista

branca) e bloqueadas (lista negra);

2.5.17. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

2.5.18. Deve filtrar o conteúdo baseado em categorias em tempo real;

2.5.19. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

2.5.20. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

2.5.21. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

2.5.22. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem;

2.5.23. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;

2.5.24. Deve permitir o bloqueio de redirecionamento HTTP;

2.5.25. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

2.5.26. Deve possuir Proxy Explícito e Transparente;

2.5.27. Deve implementar roteamento WCCP e ICAP;

2.6. FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

2.6.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

2.6.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

2.6.3. Deve estar orientado à proteção de redes;

2.6.4. Deve permitir funcionar em modo transparente, sniffer e router;

2.6.5. Deve possuir tecnologia de detecção baseada em assinaturas que sejam

atualizadas automaticamente;

2.6.6. Deve permitir a criação de padrões de ataque manualmente;

2.6.7. Deve possuir integração à plataforma de segurança;

2.6.8. Deve possuir capacidade de remontagem de pacotes para identificação de ataques;

2.6.9. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;

2.6.10. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

2.6.11. Deve possuir mecanismos de detecção/proteção de ataques;

2.6.12. Deve possuir reconhecimento de padrões;

2.6.13. Deve possuir análise de protocolos;

2.6.14. Deve possuir detecção de anomalias;

2.6.15. Deve possuir detecção de ataques de RPC (Remote Procedure Call);

2.6.16. Deve possuir proteção contra-ataques de Windows ou NetBios;

2.6.17. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

2.6.18. Deve possuir proteção contra-ataques DNS (Domain Name System);

2.6.19. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;

2.6.20. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);

2.6.21. Deve possuir métodos de notificação de detecção de ataques;

2.6.22. Deve possuir alarmes na console de administração;

2.6.23. Deve possuir alertas via correio eletrônico;

2.6.24. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

2.6.25. Deve ter a capacidade de resposta/logs ativa a ataques;

2.6.26. Deve prover a terminação de sessões via TCP resets;

2.6.27. Deve armazenar os logs de sessões;

2.6.28. Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

2.6.29. Deve mitigar os efeitos dos ataques de negação de serviços;

2.6.30. Deve permitir a criação de assinaturas personalizadas;

2.6.31. Deve possuir filtros de ataques por anomalias;

2.6.32. Deve permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

2.6.33. Deve permitir filtros de anomalias de protocolos;

2.6.34. Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

2.6.35. Deve suportar verificação de ataque na camada de aplicação;

2.6.36. Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;

2.6.37. Deve possuir as seguintes estratégias de bloqueio: pass, drop e reset.

2.7. FUNCIONALIDADE DE VPN

2.7.1. Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

2.7.2. Deve possuir suporte a certificados PKI X.509 para construção de VPNs;

2.7.3. Deve possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;

2.7.4. Deve possuir suporte a VPN SSL;

2.7.5. Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

2.7.6. A VPN SSL deve possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;

2.7.7. Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

2.7.8. A VPN SSL deve suportar cliente para plataforma Windows, Linux e Mac OS X;

2.7.9. Deve permitir a arquitetura de VPN hub and spoke;

2.7.10. Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

2.8. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

2.8.1. Deve reconhecer, no mínimo, 2.000 (duas mil) aplicações;

2.8.2. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

2.8.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

2.8.3.1. P2P

2.8.3.2. Instant Messaging;

2.8.3.3. Web client;

2.8.3.4. Transferência de arquivos;

2.8.3.5. VoIP;

2.8.4. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

2.8.5. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

2.8.6. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

2.8.7. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

2.8.8. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

2.8.9. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

2.8.10. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

2.8.11. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

2.8.12. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

2.8.13. Deve permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;

2.8.14. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

2.8.15. Deve permitir criação de padrões de aplicação manualmente;

2.9. FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

2.9.1. Deve permitir a criação de endereços IPs virtuais;

2.9.2. Deve permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

2.9.3. Deve suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

2.9.4. Deve permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;

2.9.5. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;

2.9.6. Deve permitir que seja mantido o IP de origem;

2.9.7. Deve suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

2.9.8. Deve ter a capacidade de identificar, através de health checks, quais os

servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

2.9.9. Deve permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

2.10. FUNCIONALIDADE DE VIRTUALIZAÇÃO

2.10.1. Deve suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

2.10.2. Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais;

2.10.3. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

2.11. FUNCIONALIDADE DE CONTROLADORA WIRELESS E WI-FI

2.11.1. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante;

2.11.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

2.11.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido;

2.11.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;

2.11.5. Deverá permitir a visualização dos clientes conectados;

2.11.6. Deverá prover suporte a Fast Roaming;

2.11.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;

2.11.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

2.11.9. Deverá possuir Captive Portal por SSID;

2.11.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs;

2.11.11. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;

2.11.12. Deverá suportar os seguintes métodos de autenticação EAP:

2.11.12.1. EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA;

2.11.13. Deverá suportar 802.1x através de RADIUS;

2.11.14. Deverá suportar filtro baseado em endereço MAC por SSID;

2.11.15. Deverá permitir configurar parâmetros de rádio, como: banda e canal;

2.11.16. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

2.11.17. Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;

2.11.18. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

2.11.19. Deverá possuir WIDS com, ao menos, os seguintes perfis:

2.11.19.1. Rogue/Interfering AP Detection;

2.11.19.2. Ad-hoc Network Detection;

2.11.19.3. Wireless Bridge Detection;

2.11.19.4. Weak WEP Detection;

2.11.19.5. MAC OUI Checking;

2.11.20. Deverá permitir o uso de voz e dados sobre um mesmo SSID;

2.11.21. 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 em dBm;

2.11.22. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário;

2.11.23. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs;

2.11.24. Deverá permitir a criação de políticas de traffic shaping;

2.11.25. Deverá permitir a criação de políticas de firewall baseadas em horário;

2.11.26. Deverá permitir NAT nas políticas de firewall;

2.11.27. Deverá possibilitar definir número de clientes por SSID;

2.11.28. Deverá permitir e/ou bloquear o tráfego entre SSIDs;

2.11.29. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

2.11.30. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;

2.11.31. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;

2.11.32. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;

2.11.33. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou

2.11.34. rádios;

2.11.35. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;

2.11.36. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;

2.11.37. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;

2.11.38. 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 trafegados em

um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;

2.11.39. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora;

2.11.40. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;

2.11.41. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

2.11.42. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora;

2.11.43. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora;

2.11.44. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

2.11.45. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora;

2.11.46. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora;

2.11.47. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede;

2.12. FUNCIONALIDADE DE SD-WAN

2.12.1. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

2.12.2. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

2.12.3. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

2.12.4. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

2.12.5. Solução deve ser capaz de prover Zero Touch provisioning.

2.12.6. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

2.12.7. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

2.12.8. A solução deve ser capaz de criar VPN "Full-Mesh" em interface gráfica ou CLI, de forma automática, e sem que o administrador precise configurar site por site.

2.12.9. A configuração VPN IPSEC deve oferecer suporte para DH Group: 14 e 15.

2.12.10. Reconhecimento em camada 7 totalmente segregado da camada 4.

2.12.11. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.

2.12.12. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

2.12.13. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc).

2.12.14. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com

suporte a IPv6.

2.12.15. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada.

2.12.16. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

2.12.17. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 a 50) do seu valor de saúde melhor que o link atual.

2.12.18. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

2.12.19. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

3. ITEM 03 – SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW - TIPO III

3.1. CARACTERÍSTICAS GERAIS:

3.1.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

3.1.2. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.

3.1.3. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze meses), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações e contextos virtuais. Após a vigência contratual as funcionalidades que não necessitam de atualizações online continuam ativas em funcionamento sem novas atualizações e suporte do fabricante.

3.1.4. Deve possuir fonte de alimentação com chaveamento automático 110/220V.

3.1.5. Deve possuir firewall com capacidade mínima de processamento de 27 (vinte e sete) Gbps.

3.1.6. Deve possuir IPS com capacidade mínima de processamento de 4 (quatro) Gbps.

3.1.7. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 2 (dois) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

3.1.8. Deve possuir Inspeção SSL Throughput com capacidade mínima de processamento de 2 (dois) Gbps.

3.1.9. Deve possuir VPN com capacidade de, pelo menos, 22 (vinte e dois) Gbps de tráfego IPSec.

3.1.10. Deve suportar 3.000.000 (três milhões) conexões simultâneas.

3.1.11. Deverão ser licenciados para suportar, pelo menos, 200 (duzentos) usuários de VPN SSL.

3.1.12. Deve suportar, pelo menos, 120.000 (cento e vinte mil) novas conexões por segundo.

3.1.13. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.

3.1.14. Deve suportar, pelo menos 2000 (dois mil) túneis de VPN Client-Site.

3.1.15. Deve possuir, pelo menos, 02 (duas) interfaces SFP+ 10GE.

3.1.16. Deve possuir, pelo menos, 02 (duas) interfaces 10/5/2.5 RJ45.

3.1.17. Deve possuir, pelo menos, 8 (oito) interfaces RJ 45.

3.1.18. Deve incluir licença para a funcionalidade de VPN SSL.

3.1.19. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.

3.1.20. Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 20(vinte) equipamentos.

3.1.21. Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 40(quarenta) equipamentos.

3.1.22. Deve ser compatível com atual Solução de Gerência Centralizada de Equipamentos do fabricante Fortinet, existente na SEDUC.

3.1.23. Deve ser compatível com atual Solução Centralizada de Armazenamento de Logs e Relatórios do fabricante Fortinet, existente na SEDUC.

3.1.24. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

3.1.25. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

3.2. FUNCIONALIDADE DE FIREWALL

3.2.1. Deve possuir controle de acesso à internet por endereço IP de origem e destino;

3.2.2. Deve possuir controle de acesso à internet por sub rede;

3.2.3. Deve suportar tags de VLAN (802.1q);

3.2.4. Deve possuir ferramenta de diagnóstico do tipo tcpdump;

3.2.5. Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

3.2.6. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

3.2.7. Deve suportar single-sign-on para Active Directory, RADIUS;

3.2.8. Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

3.2.9. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

3.2.10. Deve permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

3.2.11. Deve permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

3.2.12. Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

3.2.13. Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

3.2.14. Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;

3.2.15. Deve suportar aplicações multimídia, como: H.323 e SIP;

3.2.16. Deve possuir tecnologia de firewall do tipo Statefull;

3.2.17. Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

3.2.18. Deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;

3.2.19. Deve suportar PBR – Policy Based Routing;

3.2.20. Deve permitir a criação de VLANS no padrão IEEE 802.1q;

3.2.21. Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

3.2.22. Deve permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

3.2.23. Deve permitir forwarding de camada 2 para protocolos não IP;

3.2.24. Deve suportar forwarding multicast;

3.2.25. Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;

3.2.26. Deve permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

3.2.27. Deve permitir o agrupamento de serviços;

3.2.28. Deve permitir o filtro de pacotes sem a utilização de NAT;

3.2.29. Deve permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

3.2.30. Deve possuir mecanismo de anti-spoofing;

3.2.31. Deve permitir criação de regras definidas pelo usuário;

3.2.32. Deve permitir o serviço de autenticação para tráfego HTTP e FTP;

3.2.33. Deve permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

3.2.34. Deve possuir a funcionalidade de balanceamento e contingência de links;

3.2.35. Deve suportar sFlow;

3.2.36. O dispositivo deve ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas.

3.2.37. Deve ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

3.2.38. Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

3.2.39. Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

3.2.40. Deve suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

3.2.41. Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;

3.2.42. Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

3.2.43. Deve suportar SIP, H.323 e SCCP NAT Traversal;

3.2.44. Deve permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

3.2.45. Deve possuir porta de comunicação serial ou USB para testes e

configuração do equipamento, com acesso protegido por usuário e senha.

3.3. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

3.3.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

3.3.2. Deve permitir modificação de valores DSCP para o DiffServ;

3.3.3. Deve permitir priorização de tráfego e suportar ToS;

3.3.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

3.3.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

3.3.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

3.3.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

3.3.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

3.3.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

3.3.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

3.4. FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

3.4.1. Deve permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;

3.4.2. Deve possuir filtragem de e-mail por palavras chaves;

3.4.3. Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

3.4.4. Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL;

3.4.5. Deve permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

3.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

3.5.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;

3.5.2. Deve possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

3.5.3. Deve possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;

3.5.4. Deve possuir a funcionalidade de cota de tempo de utilização por categoria;

3.5.5. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

3.5.5.1. Proxy anônimo;

3.5.5.2. Webmail;

3.5.5.3. Instituições de saúde;

3.5.5.4. Notícias;

3.5.5.5. Phishing;

3.5.5.6. Hackers;

3.5.5.7. Pornografia;

3.5.5.8. Racismo;

3.5.5.9. Websites pessoais;

3.5.5.10. Compras;

3.5.6. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

3.5.7. Deve permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;

3.5.8. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço

IP;

3.5.9. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado;

3.5.10. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

3.5.11. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

3.5.12. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

3.5.13. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

3.5.14. Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;

3.5.15. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

3.5.16. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

3.5.17. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

3.5.18. Deve filtrar o conteúdo baseado em categorias em tempo real;

3.5.19. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

3.5.20. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

3.5.21. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

3.5.22. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem;

3.5.23. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;

3.5.24. Deve permitir o bloqueio de redirecionamento HTTP;

3.5.25. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

3.5.26. Deve possuir Proxy Explícito e Transparente;

3.5.27. Deve implementar roteamento WCCP e ICAP;

3.6. FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

3.6.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

3.6.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

3.6.3. Deve estar orientado à proteção de redes;

3.6.4. Deve permitir funcionar em modo transparente, sniffer e router;

3.6.5. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

3.6.6. Deve permitir a criação de padrões de ataque manualmente;

3.6.7. Deve possuir integração à plataforma de segurança;

3.6.8. Deve possuir capacidade de remontagem de pacotes para identificação de ataques;

3.6.9. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;

3.6.10. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

3.6.11. Deve possuir mecanismos de detecção/proteção de ataques;

3.6.12. Deve possuir reconhecimento de padrões;

3.6.13. Deve possuir análise de protocolos;

3.6.14. Deve possuir detecção de anomalias;

3.6.15. Deve possuir detecção de ataques de RPC (Remote Procedure Call);

3.6.16. Deve possuir proteção contra-ataques de Windows ou NetBios;

3.6.17. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

3.6.18. Deve possuir proteção contra-ataques DNS (Domain Name System);

3.6.19. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;

3.6.20. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);

3.6.21. Deve possuir métodos de notificação de detecção de ataques;

3.6.22. Deve possuir alarmes na console de administração;

3.6.23. Deve possuir alertas via correio eletrônico;

3.6.24. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

3.6.25. Deve ter a capacidade de resposta/logs ativa a ataques;

3.6.26. Deve prover a terminação de sessões via TCP resets;

3.6.27. Deve armazenar os logs de sessões;

3.6.28. Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

3.6.29. Deve mitigar os efeitos dos ataques de negação de serviços;

3.6.30. Deve permitir a criação de assinaturas personalizadas;

3.6.31. Deve possuir filtros de ataques por anomalias;

3.6.32. Deve permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

3.6.33. Deve permitir filtros de anomalias de protocolos;

3.6.34. Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

3.6.35. Deve suportar verificação de ataque na camada de aplicação;

3.6.36. Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;

3.6.37. Deve possuir as seguintes estratégias de bloqueio: pass, drop e reset.

3.7. FUNCIONALIDADE DE VPN

3.7.1. Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

3.7.2. Deve possuir suporte a certificados PKI X.509 para construção de VPNs;

3.7.3. Deve possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;

3.7.4. Deve possuir suporte a VPN SSL;

3.7.5. Deve possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

3.7.6. A VPN SSL deve possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;

3.7.7. Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

3.7.8. A VPN SSL deve suportar cliente para plataforma Windows, Linux e Mac OS X;

3.7.9. Deve permitir a arquitetura de VPN hub and spoke;

3.7.10. Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

3.8. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

3.8.1. Deve reconhecer, no mínimo, 2.000 (duas mil) aplicações;

3.8.2. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

3.8.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

3.8.3.1. P2P

3.8.3.2. Instant Messaging;

3.8.3.3. Web client;

3.8.3.4. Transferência de arquivos;

3.8.3.5. VoIP;

3.8.4. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

3.8.5. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

3.8.6. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

3.8.7. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

3.8.8. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

3.8.9. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

3.8.10. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

3.8.11. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

3.8.12. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

3.8.13. Deve permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo,

as seguintes categorias: Instant Messaging e transferência de arquivos;

3.8.14. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

3.8.15. Deve permitir criação de padrões de aplicação manualmente;

3.9. FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

3.9.1. Deve permitir a criação de endereços IPs virtuais;

3.9.2. Deve permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

3.9.3. Deve suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

3.9.4. Deve permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;

3.9.5. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;

3.9.6. Deve permitir que seja mantido o IP de origem;

3.9.7. Deve suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

3.9.8. Deve ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

3.9.9. Deve permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

3.10. FUNCIONALIDADE DE VIRTUALIZAÇÃO

3.10.1. Deve suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

3.10.2. Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais;

3.10.3. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

3.11. FUNCIONALIDADE DE CONTROLADORA WIRELESS E WI-FI

3.11.1. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante;

3.11.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

3.11.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido;

3.11.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;

3.11.5. Deverá permitir a visualização dos clientes conectados;

3.11.6. Deverá prover suporte a Fast Roaming;

3.11.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;

3.11.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

3.11.9. Deverá possuir Captive Portal por SSID;

3.11.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs;

3.11.11. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;

3.11.12. Deverá suportar os seguintes métodos de autenticação EAP:

3.11.12.1. EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA;

3.11.13. Deverá suportar 802.1x através de RADIUS;

3.11.14. Deverá suportar filtro baseado em endereço MAC por SSID;

3.11.15. Deverá permitir configurar parâmetros de rádio, como: banda e canal;

3.11.16. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

3.11.17. Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;

3.11.18. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

3.11.19. Deverá possuir WIDS com, ao menos, os seguintes perfis:

3.11.19.1. Rogue/Interfering AP Detection;

3.11.19.2. Ad-hoc Network Detection;

3.11.19.3. Wireless Bridge Detection;

3.11.19.4. Weak WEP Detection;

3.11.19.5. MAC OUI Checking;

3.11.20. Deverá permitir o uso de voz e dados sobre um mesmo SSID;

3.11.21. 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 em dBm;

3.11.22. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário;

3.11.23. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs;

3.11.24. Deverá permitir a criação de políticas de traffic shaping;

3.11.25. Deverá permitir a criação de políticas de firewall baseadas em horário;

3.11.26. Deverá permitir NAT nas políticas de firewall;

3.11.27. Deverá possibilitar definir número de clientes por SSID;

3.11.28. Deverá permitir e/ou bloquear o tráfego entre SSIDs;

3.11.29. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

3.11.30. A comunicação entre o Access Point e a Controladora Wireless deverá

poder ser efetuada de forma criptografada;

3.11.31. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;

3.11.32. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;

3.11.33. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou

3.11.34. rádios;

3.11.35. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;

3.11.36. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;

3.11.37. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;

3.11.38. 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 trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;

3.11.39. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora;

3.11.40. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;

3.11.41. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

3.11.42. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja

baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora;

3.11.43. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora;

3.11.44. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

3.11.45. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora;

3.11.46. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora;

3.11.47. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede;

3.12. FUNCIONALIDADE DE SD-WAN

3.12.1. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

3.12.2. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

3.12.3. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

3.12.4. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

3.12.5. Solução deve ser capaz de prover Zero Touch provisioning.

3.12.6. A solução de Zero Touch provisioning deve ser capaz de suportar

endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

3.12.7. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

3.12.8. A solução deve ser capaz de criar VPN "Full-Mesh" em interface gráfica ou CLI, de forma automática, e sem que o administrador precise configurar site por site.

3.12.9. A configuração VPN IPSEC deve oferecer suporte para DH Group: 14 e 15.

3.12.10. Reconhecimento em camada 7 totalmente segregado da camada 4.

3.12.11. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação a um determinado IP/ range de IPs de destino.

3.12.12. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados.

3.12.13. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc).

3.12.14. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6.

3.12.15. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada.

3.12.16. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

3.12.17. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 a 50) do seu valor de saúde melhor que o link atual.

3.12.18. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

3.12.19. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

4. ITEM 04 – SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW - TIPO IV

4.1. CARACTERÍSTICAS GERAIS:

4.1.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

4.1.2. A solução poderá ser composta por mais de um equipamento para atender as funcionalidades exigidas, desde que todos os itens sejam do mesmo fabricante garantindo total compatibilidade e integração, desde que ocupem até 2U, no máximo.

4.1.3. Deve possuir e estar licenciado durante a vigência contratual de 12 (doze meses), minimamente com as seguintes funcionalidades: Firewall, Traffic Shapping, QoS, recursos de SD-WAN, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações e contextos virtuais. Após a vigência contratual as funcionalidades que não necessitam de atualizações online continuam ativas em funcionamento sem novas atualizações e suporte do fabricante.

4.1.4. Deve possuir fonte de alimentação com chaveamento automático 110/220V.

4.1.5. Deve possuir firewall com capacidade mínima de processamento de 4 (quatro) Gbps.

4.1.6. Deve possuir IPS com capacidade mínima de processamento de 2 (dois) Gbps.

4.1.7. Proteção contra ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 1 (um) Gbps, contemplando as funções de Firewall, IPS, controle de aplicação e proteção contra Malware/Antivírus ativadas de maneira simultâneas.

4.1.8. Deve possuir VPN com capacidade de, pelo menos, 4 (quatro) Gbps de tráfego IPSec.

4.1.9. Deve suportar 700.000 (setecentos mil) conexões simultâneas.

4.1.10. Deve suportar, pelo menos, 80.000 (oitenta mil) novas conexões por segundo.

4.1.11. Deve suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.

4.1.12. Deve suportar, pelo menos 250 (duzentos e cinquenta) túneis de VPN Client-Site.

4.1.13. Deve possuir, pelo menos, 01 (um) interfaces SFP GE.

4.1.14. Deve possuir, pelo menos, 05 (cinco) interfaces RJ 45.

4.1.15. Todos os equipamentos que acompanharem a solução devem suportar o modo de alta disponibilidade e estar licenciados para operar desta forma.

4.1.16. Deve ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 8(oito) equipamentos.

4.1.17. Deve ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 8(oito) equipamentos.

4.1.18. Deve ser compatível com atual Solução de Gerência Centralizada de Equipamentos do fabricante Fortinet, existente na SEDUC.

4.1.19. Deve ser compatível com atual Solução Centralizada de Armazenamento de Logs e Relatórios do fabricante Fortinet, existente na SEDUC.

4.1.20. Deve possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de segurança durante a vigência contratual.

4.1.21. Deve ser fornecida toda documentação técnica em formato digital, através de acesso a URL oficial do fabricante, em português do Brasil ou em inglês.

4.2. FUNCIONALIDADE DE FIREWALL

4.2.1. Deve possuir controle de acesso à internet por endereço IP de origem e destino;

4.2.2. Deve possuir controle de acesso à internet por sub rede;

4.2.3. Deve suportar tags de VLAN (802.1q);

4.2.4. Deve possuir ferramenta de diagnóstico do tipo tcpdump;

4.2.5. Deve possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

4.2.6. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

4.2.7. Deve suportar single-sign-on para Active Directory, RADIUS;

4.2.8. Deve possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

4.2.9. Deve possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

4.2.10. Deve permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

4.2.11. Deve permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

4.2.12. Deve possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

4.2.13. Deve suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

4.2.14. Deve possuir funcionalidades de DHCP Cliente, Servidor e Relay;

4.2.15. Deve suportar aplicações multimídia, como: H.323 e SIP;

4.2.16. Deve possuir tecnologia de firewall do tipo Statefull;

4.2.17. Deve suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

4.2.18. Deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego;

4.2.19. Deve suportar PBR – Policy Based Routing;

4.2.20. Deve permitir a criação de VLANS no padrão IEEE 802.1q;

4.2.21. Deve possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

4.2.22. Deve permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

4.2.23. Deve permitir forwarding de camada 2 para protocolos não IP;

4.2.24. Deve suportar forwarding multicast;

4.2.25. Deve suportar roteamento multicast PIM Sparse Mode e Dense Mode;

4.2.26. Deve permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

4.2.27. Deve permitir o agrupamento de serviços;

4.2.28. Deve permitir o filtro de pacotes sem a utilização de NAT;

4.2.29. Deve permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

4.2.30. Deve possuir mecanismo de anti-spoofing;

4.2.31. Deve permitir criação de regras definidas pelo usuário;

4.2.32. Deve permitir o serviço de autenticação para tráfego HTTP e FTP;

4.2.33. Deve permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

4.2.34. Deve possuir a funcionalidade de balanceamento e contingência de links;

4.2.35. Deve suportar sFlow;

4.2.36. O dispositivo deve ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas.

4.2.37. Deve ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

4.2.38. Deve permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

4.2.39. Deve permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

4.2.40. Deve suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

4.2.41. Deve permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;

4.2.42. Deve possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

4.2.43. Deve suportar SIP, H.323 e SCCP NAT Traversal;

4.2.44. Deve permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

4.2.45. Deve possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

4.3. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

4.3.1. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

4.3.2. Deve permitir modificação de valores DSCP para o DiffServ;

4.3.3. Deve permitir priorização de tráfego e suportar ToS;

4.3.4. Deve limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

4.3.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.3.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

4.3.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

4.3.8. Deve permitir definir banda máxima e banda garantida para um usuário, IP, grupo

de IPs, protocolo e aplicação;

4.3.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

4.3.10. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

4.4. FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

4.4.1. Deve permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;

4.4.2. Deve possuir filtragem de e-mail por palavras chaves;

4.4.3. Deve permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

4.4.4. Deve possuir, para a funcionalidade de anti-spam, o recurso de RBL;

4.4.5. Deve permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

4.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

4.5.1. Deve possuir solução de filtro de conteúdo Web integrado à solução de segurança;

4.5.2. Deve possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

4.5.3. Deve possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;

4.5.4. Deve possuir a funcionalidade de cota de tempo de utilização por categoria;

4.5.5. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

4.5.5.1. Proxy anônimo;

4.5.5.2. Webmail;

4.5.5.3. Instituições de saúde;

4.5.5.4. Notícias;

4.5.5.5. Phishing;

4.5.5.6. Hackers;

4.5.5.7. Pornografia;

4.5.5.8. Racismo;

4.5.5.9. Websites pessoais;

4.5.5.10. Compras;

4.5.6. Deve permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

4.5.7. Deve permitir a criação de, pelo menos, 07 (sete) categorias personalizadas;

4.5.8. Deve permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

4.5.9. Deve prover Termo de Responsabilidade on-line, podendo ser customizável, aceitando idioma português, para aceite pelo usuário, a ser apresentado toda vez que quando houver tentativa de acesso a determinado serviço permitido ou bloqueado;

4.5.10. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

4.5.11. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

4.5.12. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

4.5.13. Deve exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

4.5.14. Deve permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;

4.5.15. Deve permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

4.5.16. Deve permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

4.5.17. Deve permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

4.5.18. Deve filtrar o conteúdo baseado em categorias em tempo real;

4.5.19. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

4.5.20. Deve permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

4.5.21. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.5.22. Deve permitir a criação de regras para acesso/bloqueio por sub rede de origem;

4.5.23. Deve ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;

4.5.24. Deve permitir o bloqueio de redirecionamento HTTP;

4.5.25. Deve permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

4.5.26. Deve possuir Proxy Explícito e Transparente;

4.5.27. Deve implementar roteamento WCCP e ICAP;

4.6. FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

4.6.1. Deve permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

4.6.2. Deve possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

4.6.3. Deve estar orientado à proteção de redes;

4.6.4. Deve permitir funcionar em modo transparente, sniffer e router;

4.6.5. Deve possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

4.6.6. Deve permitir a criação de padrões de ataque manualmente;

4.6.7. Deve possuir integração à plataforma de segurança;

4.6.8. Deve possuir capacidade de remontagem de pacotes para identificação de ataques;

4.6.9. Deve possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;

4.6.10. Deve possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

4.6.11. Deve possuir mecanismos de detecção/proteção de ataques;

4.6.12. Deve possuir reconhecimento de padrões;

4.6.13. Deve possuir análise de protocolos;

4.6.14. Deve possuir detecção de anomalias;

4.6.15. Deve possuir detecção de ataques de RPC (Remote Procedure Call);

4.6.16. Deve possuir proteção contra-ataques de Windows ou NetBios;

4.6.17. Deve possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

4.6.18. Deve possuir proteção contra-ataques DNS (Domain Name System);

4.6.19. Deve possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;

4.6.20. Deve possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);

4.6.21. Deve possuir métodos de notificação de detecção de ataques;

4.6.22. Deve possuir alarmes na console de administração;

4.6.23. Deve possuir alertas via correio eletrônico;

4.6.24. Deve possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deve ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

4.6.25. Deve ter a capacidade de resposta/logs ativa a ataques;

4.6.26. Deve prover a terminação de sessões via TCP resets;

4.6.27. Deve armazenar os logs de sessões;

4.6.28. Deve atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

4.6.29. Deve mitigar os efeitos dos ataques de negação de serviços;

4.6.30. Deve permitir a criação de assinaturas personalizadas;

4.6.31. Deve possuir filtros de ataques por anomalias;

4.6.32. Deve permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

4.6.33. Deve permitir filtros de anomalias de protocolos;

4.6.34. Deve suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

4.6.35. Deve suportar verificação de ataque na camada de aplicação;

4.6.36. Deve suportar verificação de tráfego em tempo real, via aceleração de hardware;

4.6.37. Deve possuir as seguintes estratégias de bloqueio: pass, drop e reset.

4.7. FUNCIONALIDADE DE VPN

4.7.1. Deve possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

4.7.2. Deve possuir suporte a certificados PKI X.509 para construção de VPNs;

4.7.3. Deve possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;

4.7.4. Deve possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

4.7.5. Deve permitir a arquitetura de VPN hub and spoke;

4.7.6. Deve possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

4.8. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

4.8.1. Deve reconhecer, no mínimo, 2.000 (duas mil) aplicações;

4.8.2. Deve possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

4.8.3. Deve possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

4.8.3.1. P2P

4.8.3.2. Instant Messaging;

4.8.3.3. Web client;

4.8.3.4. Transferência de arquivos;

4.8.3.5. VoIP;

4.8.4. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

4.8.5. Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

4.8.6. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.8.7. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

4.8.8. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

4.8.9. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

4.8.10. Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.8.11. Deve possuir integração com tokens para autenticação de 02 (dois) fatores;

4.8.12. Deve permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

4.8.13. Deve permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;

4.8.14. Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

4.8.15. Deve permitir criação de padrões de aplicação manualmente;

4.9. FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

4.9.1. Deve permitir a criação de endereços IPs virtuais;

4.9.2. Deve permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

4.9.3. Deve suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

4.9.4. Deve permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Static, Round Robin, Weighted, First Alive e HTTP host, Least Session, Least RTT;

4.9.5. Deve permitir persistência de sessão por cookie HTTP ou SSL session ID;

4.9.6. Deve permitir que seja mantido o IP de origem;

4.9.7. Deve suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

4.9.8. Deve ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

4.9.9. Deve permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

4.10. FUNCIONALIDADE DE VIRTUALIZAÇÃO

4.10.1. Deve suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

4.10.2. Deve permitir a criação de administradores independentes para cada uma das instâncias virtuais;

4.10.3. Deve permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

4.11. FUNCIONALIDADE DE CONTROLADORA WIRELESS E WI-FI

4.11.1. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante;

4.11.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

4.11.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido;

4.11.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;

4.11.5. Deverá permitir a visualização dos clientes conectados;

4.11.6. Deverá prover suporte a Fast Roaming;

4.11.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;

4.11.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

4.11.9. Deverá possuir Captive Portal por SSID;

4.11.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs;

4.11.11. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;

4.11.12. Deverá suportar os seguintes métodos de autenticação EAP:

4.11.12.1. EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA;

4.11.13. Deverá suportar 802.1x através de RADIUS;

4.11.14. Deverá suportar filtro baseado em endereço MAC por SSID;

4.11.15. Deverá permitir configurar parâmetros de rádio, como: banda e canal;

4.11.16. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

4.11.17. Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;

4.11.18. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

4.11.19. Deverá possuir WIDS com, ao menos, os seguintes perfis:

4.11.19.1. Rogue/Interfering AP Detection;

4.11.19.2. Ad-hoc Network Detection;

4.11.19.3. Wireless Bridge Detection;

4.11.19.4. Weak WEP Detection;

4.11.19.5. MAC OUI Checking;

4.11.20. Deverá permitir o uso de voz e dados sobre um mesmo SSID;

4.11.21. 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 em dBm;

4.11.22. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário;

4.11.23. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs;

4.11.24. Deverá permitir a criação de políticas de traffic shaping;

4.11.25. Deverá permitir a criação de políticas de firewall baseadas em horário;

4.11.26. Deverá permitir NAT nas políticas de firewall;

4.11.27. Deverá possibilitar definir número de clientes por SSID;

4.11.28. Deverá permitir e/ou bloquear o tráfego entre SSIDs;

4.11.29. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

4.11.30. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;

4.11.31. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;

4.11.32. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;

4.11.33. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou

4.11.34. rádios;

4.11.35. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;

4.11.36. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;

4.11.37. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;

4.11.38. 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 trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;

4.11.39. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.11.40. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;

4.11.41. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.11.42. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora;

4.11.43. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.11.44. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.11.45. Deverá permitir aplicar políticas de controle AntiSpam para todas as redes cujo tráfego seja tunelado até a Controladora;

4.11.46. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.11.47. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede;

4.12. FUNCIONALIDADE DE SD-WAN

4.12.1. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

4.12.2. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

4.12.3. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

4.12.4. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

4.12.5. Solução deve ser capaz de prover Zero Touch provisioning.

4.12.6. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

4.12.7. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

4.12.8. A solução deve ser capaz de criar VPN "Full-Mesh" em interface gráfica ou CLI, de forma automática, e sem que o administrador precise configurar site por site.

4.12.9. A configuração VPN IPSEC deve oferecer suporte para DH Group: 14 e 15.

4.12.10. Reconhecimento em camada 7 totalmente segregado da camada 4.

4.12.11. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.

4.12.12. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados.

4.12.13. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc).

4.12.14. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6.

4.12.15. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições em que a largura de banda é modificada.

4.12.16. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

4.12.17. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 a 50) do seu valor de saúde melhor que o link atual.

4.12.18. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

4.12.19. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

5. ITEM 05 – ATIVO DE REDE WIRED – TIPO I

5.1. Deve possuir garantia e suporte do fabricante pelo período de 12 (doze) meses;

5.2. A CONTRATADA deve realizar a instalação inicial do equipamento que está restrita a entrega do equipamento, conferência de itens e teste inicial de funcionamento.

5.3. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 2 do modelo OSI;

5.4. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

5.5. Adicionalmente, deve possuir 04 (quatro) slots SFP+ para conexão de fibras ópticas operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

5.6. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial;

5.7. Deve possuir capacidade de comutação de pelo menos 125 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);

5.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

5.9. Deve possuir tabela MAC com suporte a 30.000 endereços;

5.10. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

5.11. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

5.12. Deve suportar a comutação de Jumbo Frames;

5.13. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

5.14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

5.15. Deve implementar serviço de DHCP Relay;

5.16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentos) entradas na tabela;

5.17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring);

5.18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).

5.19. Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

5.20. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

5.21. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;

5.22. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

5.23. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

5.24. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

5.25. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

5.26. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, campo CoS e VLAN ID;

5.27. Deve suportar a definição de dias e horários que a ACL deverá ser aplicada na rede;

5.28. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

5.29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

5.30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

5.31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

5.32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

5.33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

5.34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

5.35. Deve suportar MAC Authentication Bypass (MAB);

5.36. Deve implementar RADIUS CoA (Change of Authorization);

5.37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

5.38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

5.39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

5.40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

5.41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

5.42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

5.43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

5.44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

5.45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

5.46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

5.47. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

5.48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

5.49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

5.50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

5.51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

5.52. Deve permitir ser gerenciado através de IPv6;

5.53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

5.54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso

administrativo ao equipamento;

5.55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

5.56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

5.57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch;

5.58. Deverá suportar ser configurado e monitorado através de REST API;

5.59. Deve em conjunto com a controladora ser capaz de implementar e orquestrar políticas de segurança de micro segmentação nos switches controlando como os usuários/endpoints se comunicam lateralmente entre si.

5.60. Deve em conjunto com a controladora permitir a criação de automações que executem ações baseado em eventos de rede detectados no ambiente, como quarentenar um dispositivo, isolar um endpoint, implementar e/ou ajustar políticas de segurança dependendo do evento detectado, de forma automatizada.

5.61. Deve suportar temperatura de operação de até 40º Celsius;

5.62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

5.63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

5.64. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03 e 04 “SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW TIPO I, II, III e IV” deste termo ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

5.64.1. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo disrupção do serviço mediante a falha de um elemento;

5.64.2. Deve operar como ponto central para automação e gerenciamento dos switches;

5.64.3. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

5.64.4. Deve possuir interface gráfica para configuração, administração e

monitoração dos switches;

5.64.5. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

5.64.6. Deve montar a topologia da rede de maneira automática;

5.64.7. Deve através da interface gráfica ser capaz de configurar as VLANs da rede e distribuí-las automaticamente em todos os switches gerenciados;

5.64.8. Deve ser capaz de configurar os switches da rede;

5.64.9. Deve através da interface gráfica ser capaz de configurar as VLANs da rede e distribuí-las automaticamente em todos os switches gerenciados;

5.64.10. Deve através da interface gráfica ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

5.64.11. Deve através da interface gráfica ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

5.64.12. Deve através da interface gráfica ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

5.64.13. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

5.64.14. Deve através da interface gráfica ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

5.64.15. Deve através da interface gráfica ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

5.64.16. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

5.64.17. Deve ser capaz de configurar parâmetros SNMP dos switches;

5.64.18. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

5.64.19. A solução de gerência centralizada deve permitir o envio automático de e-

mails de notificação para os administradores da rede em caso de eventos de falhas;

5.64.20. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches;

5.64.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

5.64.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;

5.64.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

5.64.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

5.64.25. Deve possuir API no formato REST.

6. ITEM 06 – ATIVO DE REDE WIRED – TIPO II

6.1. Deve possuir garantia e suporte do fabricante pelo período de 12 (doze) meses;

6.2. A CONTRATADA deve realizar a instalação inicial do equipamento que está restrita a entrega do equipamento, conferência de itens e teste inicial de funcionamento.

6.3. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 2 do modelo OSI;

6.4. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

6.5. Adicionalmente, deve possuir 04 (quatro) slots SFP+ para conexão de fibras ópticas operando em 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

6.6. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial;

6.7. Deve possuir capacidade de comutação de pelo menos 170 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);

6.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

6.9. Deve possuir tabela MAC com suporte a 30.000 endereços;

6.10. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

6.11. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

6.12. Deve suportar a comutação de Jumbo Frames;

6.13. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

6.14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

6.15. Deve implementar serviço de DHCP Relay;

6.16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentos) entradas na tabela;

6.17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring);

6.18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree).

6.19. Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

6.20. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

6.21. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;

6.22. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

6.23. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

6.24. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch

deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

6.25. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

6.26. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, campo CoS e VLAN ID;

6.27. Deve suportar a definição de dias e horários que a ACL deverá ser aplicada na rede;

6.28. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

6.29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

6.30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

6.31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

6.32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

6.33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

6.34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

6.35. Deve suportar MAC Authentication Bypass (MAB);

6.36. Deve implementar RADIUS CoA (Change of Authorization);

6.37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

6.38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

6.39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

6.40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

6.41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

6.42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

6.43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

6.44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

6.45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

6.46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

6.47. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

6.48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

6.49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

6.50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

6.51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

6.52. Deve permitir ser gerenciado através de IPv6;

6.53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de

permissões para administração e configuração do switch;

6.54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

6.55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

6.56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

6.57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch;

6.58. Deverá suportar ser configurado e monitorado através de REST API;

6.59. Deve em conjunto com a controladora ser capaz de implementar e orquestrar políticas de segurança de micro segmentação nos switches controlando como os usuários/endpoints se comunicam lateralmente entre si.

6.60. Deve em conjunto com a controladora permitir a criação de automações que executem ações baseado em eventos de rede detectados no ambiente, como quarentenar um dispositivo, isolar um endpoint, implementar e/ou ajustar políticas de segurança dependendo do evento detectado, de forma automatizada.

6.61. Deve suportar temperatura de operação de até 40º Celsius;

6.62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

6.63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

6.64. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03 e 04 “SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW TIPO I, II, III e IV”deste termo ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

6.64.1. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo disrupção do serviço mediante a falha de um elemento;

6.64.2. Deve operar como ponto central para automação e gerenciamento dos switches;

6.64.3. Deve realizar o gerenciamento de inventário de hardware, software e

configuração dos Switches;

6.64.4. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

6.64.5. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

6.64.6. Deve montar a topologia da rede de maneira automática;

6.64.7. Deve através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

6.64.8. Deve ser capaz de configurar os switches da rede;

6.64.9. Deve através da interface gráfica ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

6.64.10. Deve através da interface gráfica ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

6.64.11. Deve através da interface gráfica ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

6.64.12. Deve através da interface gráfica ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

6.64.13. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

6.64.14. Deve através da interface gráfica ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

6.64.15. Deve através da interface gráfica ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

6.64.16. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

6.64.17. Deve ser capaz de configurar parâmetros SNMP dos switches;

6.64.18. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software

para cada switch, além de permitir a atualização dos switches individualmente;

6.64.19. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

6.64.20. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches;

6.64.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

6.64.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;

6.64.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

6.64.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

6.64.25. Deve possuir API no formato REST;

7. ITEM 07 – ATIVO DE REDE WIRED – TIPO III

7.1. Deve possuir garantia e suporte do fabricante pelo período de 12 (doze) meses.

7.2. A CONTRATADA deve realizar a instalação inicial do equipamento que está restrita a entrega do equipamento, conferência de itens e teste inicial de funcionamento.

7.3. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 2 do modelo OSI;

7.4. Deve possuir 8 (oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

7.5. Adicionalmente, deve possuir 02 (dois) slots SFP para conexão de fibras ópticas operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

7.6. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE

802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 130W;

7.7. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial;

7.8. Deve possuir capacidade de comutação de pelo menos 20 Gbps e ser capaz de encaminhar até 30 Mpps (milhões de pacotes por segundo);

7.9. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

7.10. Deve possuir tabela MAC com suporte a 8.000 endereços;

7.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

7.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

7.13. Deve suportar a comutação de Jumbo Frames;

7.14. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

7.15. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

7.16. Deve implementar serviço de DHCP Relay;

7.17. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentos) entradas na tabela;

7.18. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring);

7.19. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree);

7.20. Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

7.21. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

7.22. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;

7.23. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

7.24. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

7.25. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

7.26. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

7.27. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, campo CoS e VLAN ID;

7.28. Deve suportar a definição de dias e horários que a ACL deverá ser aplicada na rede;

7.29. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

7.30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

7.31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

7.32. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

7.33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

7.34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

7.35. Deve suportar MAC Authentication Bypass (MAB);

7.36. Deve implementar RADIUS CoA (Change of Authorization);

7.37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

7.38. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

7.39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

7.40. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

7.41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

7.42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

7.43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

7.44. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

7.45. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

7.46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

7.47. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

7.48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

7.49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

7.50. Deve suportar o protocolo HTTPS para configuração e administração remota através

de interface web;

7.51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

7.52. Deve permitir ser gerenciado através de IPv6;

7.53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

7.54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

7.55. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

7.56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

7.57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch;

7.58. Deverá suportar ser configurado e monitorado através de REST API;

7.59. Deve em conjunto com a controladora ser capaz de implementar e orquestrar políticas de segurança de micro segmentação nos switches controlando como os usuários/endpoints se comunicam lateralmente entre si.

7.60. Deve em conjunto com a controladora permitir a criação de automações que executem ações baseado em eventos de rede detectados no ambiente, como quarentenar um dispositivo, isolar um endpoint, implementar e/ou ajustar políticas de segurança dependendo do evento detectado, de forma automatizada.

7.61. Deve suportar temperatura de operação de até 40º Celsius;

7.62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

7.63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

7.64. Deve ser compatível e gerenciado pelos ITENS 01, 02, 03 e 04 “SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDE NGFW TIPO I, II, III e IV” deste termo ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

7.64.1. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo disrupção do serviço mediante a falha de um elemento;

7.64.2. Deve operar como ponto central para automação e gerenciamento dos switches;

7.64.3. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

7.64.4. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

7.64.5. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

7.64.6. Deve montar a topologia da rede de maneira automática;

7.64.7. Deve através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

7.64.8. Deve ser capaz de configurar os switches da rede;

7.64.9. Deve através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

7.64.10. Deve através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

7.64.11. Deve através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

7.64.12. Deve através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

7.64.13. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

7.64.14. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

7.64.15. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

7.64.16. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

7.64.17. Deve ser capaz de configurar parâmetros SNMP dos switches;

7.64.18. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

7.64.19. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

7.64.20. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches;

7.64.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

7.64.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;

7.64.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

7.64.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

7.64.25. Deve possuir API no formato REST;

8. ITEM 08 – ATIVO DE REDE WIRELESS – TIPO I

8.1. Deve possuir garantia e suporte do fabricante pelo período de 12 (doze) meses.

8.2. Deve possuir, ao menos, 02 (duas) interfaces de rede 10/100/1000/2500 Base-T RJ-45.

8.3. Deve possuir, ao menos, 01 (uma) interface de console RS-232 RJ-45.

8.4. Deve possuir, ao menos 01 rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento.

8.5. Deve suportar, ao menos, 16 (dezesseis) SSIDs simultâneos por Ponto de Acesso, sendo, pelo menos, 08 (oito) por rádio.

8.6. Deve possuir potência de transmissão de, ao menos, 21 dBm.

8.7. Deve possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.1x, IEEE 802.1q e IEEE 802.11ax com ganhos de, no mínimo, 5 dBi para 6GHz.

8.8. Deve suportar operação na temperatura de 0 a 40 °C.

8.9. Deve ser fornecido com todos os acessórios necessários para que seja feita sua fixação em teto ou parede.

8.10. Deve suportar os padrões 802.11a/b/g/n/ac/ax/q/x.

8.11. Deve possuir capacidade tri-band com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

8.12. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação.

8.13. Deve possuir a tecnologia MU-MIMO com operação 2x2.

8.14. Deve suportar taxas de conexão (data rate) de até 2.4 Gbps.

8.15. Deve atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac Wave1/Wave2, IEEE 802.11ax e IEEE 802.11x, com operação nas frequências de 2.4 GHz, 5 GHz e 6 GHz de forma simultânea.

8.16. Deve possuir PoE (Power over Ethernet), padrão 802.3at, possibilitando seu uso sem a necessidade de fontes de energia externas em qualquer porta Ethernet.

8.17. Deve ser incluso injetor PoE capaz de suportar completa operação do equipamento.

8.18. Deve suportar a criação de redes mesh.

8.19. 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 trafegados em um determinado SSID devem ser encaminhados via túnel seguro (com criptografia) até o controlador wireless.

8.20. Deve suportar a criação de enlaces de bridge entre 02 (dois) Access Points.

8.21. Deve suportar associação dinâmica de usuários a VLANs de acordo com parâmetros de autenticação.

8.22. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz, 5GHz e 6GHz.

8.23. Deve possuir funcionalidade de ajuste de potência automática, de forma a reduzir interferência entre canais.

8.24. Deve implementar UL (uplink) MU-MIMO 802.11ax mode.

8.25. Deve implementar Spectrum Analyzer.

8.26. Deve implementar Spatial Reuse (BSS Coloring).

8.27. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;

8.28. Deve possuir certificação WiFi Alliance.

8.29. Deve possuir homologação da ANATEL, de acordo com a Resolução número 242.

8.30. Deve ser fornecida Controladora Wireless que atenda aos requisitos abaixo, caso compatível poderá ser utilizada atual solução existente na SEDUC:

8.30.1. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante;

8.30.2. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

8.30.3. Deverá suportar monitoração e supressão de Ponto de Acesso indevido;

8.30.4. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;

8.30.5. Deverá permitir a visualização dos clientes conectados;

8.30.6. Deverá prover suporte a Fast Roaming;

8.30.7. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;

8.30.8. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

8.30.9. Deverá possuir Captive Portal por SSID;

8.30.10. Deverá permitir configurar o bloqueio de tráfego entre SSIDs;

8.30.11. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

8.30.12. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

8.30.13. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;

8.30.14. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

8.30.15. Deverá permitir a criação de políticas de firewall baseadas em horário;

8.30.16. Deverá permitir NAT nas políticas de firewall;

8.30.17. Deverá possibilitar definir número de clientes por SSID;

8.30.18. Deverá permitir e/ou bloquear o tráfego entre SSIDs;

8.30.19. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas autogeradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

8.30.20. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;

8.30.21. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;

8.30.22. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;

8.30.23. Deve possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios;

8.30.24. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;

8.30.25. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;

8.30.26. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;

8.30.27. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

8.30.28. Deve suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;

8.30.29. Deve suportar os seguintes métodos de autenticação EAP:

8.30.30. EAP-TLS , EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA;

8.30.31. Deve suportar 802.1x através de RADIUS;

8.30.32. Deve suportar filtro baseado em endereço MAC por SSID;

8.30.33. Deve permitir configurar parâmetros de rádio, como: banda e canal;

8.30.34. Deve possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

8.30.35. Deve possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;

8.30.36. Deve possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

8.30.37. Deve possuir WIDS com, ao menos, os seguintes perfis:

8.30.38. Rogue/Interfering AP Detection;

8.30.39. Ad-hoc Network Detection;

8.30.40. Wireless Bridge Detection;

8.30.41. Weak WEP Detection;

8.30.42. MAC OUI Checking;

8.30.43. A solução Deve detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

8.30.44. 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 trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;

9. ITEM 09 – SOLUÇÃO DE GERÊNCIA DE LOGS E RELATORIA

9.1. Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização: VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer.

9.2. Deverá possuir a capacidade de receber pelo menos 50 GB de logs dias, e garantia de pelo menos 250 GB de logs diários, além de atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 12 (doze) meses.

9.3. Deverá possuir o licenciamento do serviço de Indicadores de Comprometimento (IoC) do mesmo fabricante com capacidade de receber pelo menos 250 GB de logs diários.

9.4. Deverá suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções.

9.5. Deverá possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento.

9.6. Deverá permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento.

9.7. Deverá suportar SNMP versão 2 e 3

9.8. Deverá permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.

9.9. Deverá permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.

9.10. Deverá permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH

9.11. Deverá possuir autenticação de usuários para acesso à plataforma via LDAP

9.12. Deverá possuir autenticação de usuários para acesso à plataforma via Radius

9.13. Deverá possuir autenticação de usuários para acesso à plataforma via TACACS +

9.14. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico

9.15. Deverá possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas.

9.16. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de gráfico

9.17. Deverá possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.

9.18. Deverá possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.

9.19. Deverá possuir visualização da quantidade de logs enviados de cada dispositivo monitorado

9.20. Deverá possuir mecanismos de apagamento automático para logs antigos.

9.21. Deverá permitir importação e exportação de relatórios;

9.22. Deverá ter a capacidade de criar relatórios no formato HTML;

9.23. Deverá ter a capacidade de criar relatórios em formato PDF;

9.24. Deverá ter a capacidade de criar relatórios no formato XML;

9.25. Deverá ter a capacidade de criar relatórios no formato CSV;

9.26. Deverá permitir exportar os logs no formato CSV;

9.27. Deverá gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.

9.28. Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.

9.29. Deverá ter relatórios predefinidos.

9.30. Deverá poder enviar automaticamente os logs para um servidor FTP externo para a solução

9.31. Deverá permitir a duplicação de relatórios existentes, deve ser possível para edição posterior.

9.32. Deverá ter a capacidade de personalizar a capa dos relatórios obtidos.

9.33. Deverá permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.

9.34. Deverá ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas

9.35. Deverá ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real.

9.36. Deverá permitir que os arquivos de log sejam baixados da plataforma para uso externo.

9.37. Deverá ter a capacidade de gerar e enviar relatórios periódicos automaticamente.

9.38. Deverá permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.

9.39. Deverá permitir o envio por e-mail relatórios automaticamente.

9.40. Deverá permitir que o relatório seja enviado por email ao destinatário específico.

9.41. Deverá permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.

9.42. Deverá exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.

9.43. Deverá permitir o uso de filtros nos relatórios.

9.44. Deverá permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.

9.45. Deverá permitir especificar o idioma dos relatórios criados

9.46. Deverá gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.

9.47. Deverá permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.

9.48. Deverá ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.

9.49. Deverá possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros.

9.50. Deverá ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.

9.51. Deverá importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.

9.52. Deverá ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.

9.53. Deverá fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.

9.54. Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.

9.55. Deverá permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos

9.56. Deverá permitir visualizar em tempo real os logs recebidos.

9.57. Deverá permitir o encaminhamento de log no formato syslog.

9.58. Deverá permitir o encaminhamento de log no formato CEF (Common Event Format).

9.59. Deverá gerar alertas de eventos a partir de logs recebidos

9.60. Deverá permitir a criação de incidentes a partir de alertas de eventos para o terminal

9.61. Deverá permitir a integração ao sistema de tickets do ServiceNow

9.62. Deverá permitir o suporte a logs na nuvem pública do Amazon S3

9.63. Deverá permitir o suporte a logs na nuvem pública do Microsoft Azure

9.64. Permitir o suporte aos registros de nuvem pública do Gooogle Cloud

9.65. Suportar o padrão SAML para autenticação do usuário administrador

9.66. Deverá possuir relatório de conformidade com o PCI DSS;

9.67. Deverá possuir um relatório de uso do aplicativo SaaS

9.68. Deverá possuir um relatório de prevenção de perda de dados (DLP)

9.69. Deverá possuir um relatório de VPN

9.70. Deverá possuir um relatório IPS (Intruder Prevention System)

9.71. Deverá possuir um relatório de reputação do cliente

9.72. Deverá possuir um relatório de análise de segurança do usuário

9.73. Deverá possuir um relatório de análise de ameaças cibernéticas

9.74. Deverá possuir um breve relatório resumido diário de eventos e incidentes de segurança

9.75. Deverá possuir um relatório de tráfego DNS

9.76. Deverá possuir um relatório de tráfego de e-mail

9.77. Deverá possuir um relatório dos 10 principais aplicativos usados na rede

9.78. Deverá possuir um relatório dos 10 principais sites usados na rede

9.79. Deverá possuir um relatório de uso de mídia social

10. ITEM 10 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO I

10.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FG-400F, SKU FC-10-0400F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.

11. ITEM 11 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO II

11.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FG-100F, SKU FC-10-F100F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.

12. ITEM 12 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO III

12.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FG-90G, SKU FC-10-0090G-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.

13. ITEM 13 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO IV

13.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FG-50G-SFP, SKU FC-10-F50GS-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic

Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.

14. ITEM 14 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO V

14.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FG-1100E, SKU FC-10-F11HE-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.

15. ITEM 15 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO VI

15.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FG-601E, SKU FC-10-F6H1E-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.

16. ITEM 16 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DO SISTEMA NGFW TIPO VII

16.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FG-60F, SKU FC-10-0060F-950-02-12, pelo período de 12 (doze) meses das funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec, Controle de Aplicações, Otimização WAN.

17. ITEM 17 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO I

17.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FS-124F, SKU FC-10-S124N-247-02-12, pelo período de 12 (doze) meses das funcionalidades: atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone), bem como uma opção de devolução de hardware.

18. ITEM 18 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO II

18.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FS-148F, SKU FC-10-148FN-247-02-12, pelo período de 12 (doze) meses das funcionalidades: atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone), bem como uma opção de devolução de hardware.

19. ITEM 19 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO III

19.1. CARACTERISTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FS-108F-FPOE, SKU FC-10-F108F-247-02-12, pelo período de 12 (doze) meses das funcionalidades: atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone), bem como uma opção de devolução de hardware.

20. ITEM 20 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO IV

20.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FS-1024D, SKU FC-10-W1024-247-02-12, pelo período de 12 (doze) meses das funcionalidades: atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone), bem como uma opção de devolução de hardware.

21. ITEM 21 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO V

21.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FS-548D, SKU FC-10-W0548-247-02-12, pelo período de 12 (doze) meses das funcionalidades: atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone), bem como uma opção de devolução de hardware.

22. ITEM 22 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO VI

22.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os

equipamentos do Fabricante Fortinet Modelo FS-248E-FPOE, SKU FC-10-W248E-247-02-12, pelo período de 12 (doze) meses das funcionalidades: atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone), bem como uma opção de devolução de hardware.

23. ITEM 23 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO VII

23.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FS-124E, SKU FC-10-WP12E-247-02-12, pelo período de 12 (doze) meses das funcionalidades: atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone), bem como uma opção de devolução de hardware.

24. ITEM 24 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRED TIPO VIII

24.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FS-124E-POE, SKU FC-10-S248P-247-02-12, pelo período de 12 (doze) meses das funcionalidades: atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone), bem como uma opção de devolução de hardware.

25. ITEM 25 –SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRELESS TIPO I

25.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FAP-231G-N, SKU FC-10-PG231-247-02-12, pelo período de 12 (doze) meses das funcionalidades: atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone), bem como uma opção de devolução de hardware.

26. ITEM 26 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DOS ATIVOS WIRELESS TIPO II

26.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FAP-221E-N, SKU FC-10-PE221-247-02-12, pelo período de 12 (doze) meses das funcionalidades: atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone), bem como uma opção de devolução de hardware.

27. ITEM 27 – SERVIÇO DE UPGRADE E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE GERÊNCIA DE LOGS E RELATORIA

27.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FORTIANALYZER-VM, SKU FortiCare Premium Support FC6-10-LV0VM-248-02-12 e SKU FortiGuard IOC and Outbreak Detection Service FC6-10-LV0VM-661-02-12 pelo período de 12 (doze) meses contemplando todas funcionalidades e suporte.

28. ITEM 28 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE AUTENTICAÇÃO

28.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FAC-VM com 100.000 usuários, SKU FC6-10-0ACVM-248-02-12, pelo período de 12 (doze) meses das funcionalidades: atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone).

29. ITEM 29 – SERVIÇO DE LICENCIAMENTO E ATUALIZAÇÃO DAS FUNCIONALIDADES DA SOLUÇÃO DE WAF

29.1. CARACTERÍSTICAS GERAIS: Licenciamento e Suporte Técnico para os equipamentos do Fabricante Fortinet Modelo FWB-VM08, SKU FC-10-VVM08-581-02-12, pelo período de 12 (doze) meses das funcionalidades: Av, FortiWeb Security Service, IP Reputation, Threat Analytics Service, atualizações de firmware, acesso ao portal de suporte e recursos técnicos associados, relatórios sobre incidentes técnicos (via web, bate-papo e telefone).

30. ITEM 30 - SERVIÇOS DE IMPLANTAÇÃO DE NGFW

30.1. Os serviços envolvendo a execução de atividade de rotinas de implantação deverão ser prestados de maneira a apoiar os processos de trabalho e atividades pontuais para atender a necessidades específicas apresentadas pela CONTRATANTE.

30.2. Os serviços envolverão todas as atividades de implantação, configurações, programações e atendimento às demandas apresentadas pela CONTRATANTE, referente aos Itens 01, 02, 03 e 04.

30.3. A execução do Contrato deverá seguir metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada. À CONTRATANTE caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços. A CONTRATADA deverá disponibilizar um Gerente do Projeto, o qual deverá supervisionar todas as atividades dos profissionais vinculados à dedicação exclusiva.

Ao Gerente do Projeto será atribuída a responsabilidades de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela CONTRATANTE.

30.4. Os serviços deverão ser realizados nas dependências do CONTRATANTE, utilizando-se de equipamentos e infraestrutura com capacidade operacional.

30.5. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.

30.6. Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE.

30.7. Deve ser realizado o desenvolvimento de plano de implementação; planejamento; análise; configuração; integração; migração; testes de verificação; ajustes; otimização; troubleshooting; updates; upgrades; ensaios de contingência; criação de regras de segurança;

30.8. Deve ser realizado definição da arquitetura lógica e física do projeto, garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais;

30.9. Deve ser realizado gerenciamento de projetos: gerenciamento do projeto propriamente dito, considerando controle de prazos, esforço, elaboração de relatórios de posicionamento executivo, indicadores do projeto e qualquer outra métrica prevista no PMBOOK. O objetivo de todas estas atividades é a garantia de qualidade do projeto no que tange prazos e esforço.

30.10. Devem estar contemplados nos serviços de instalação minimamente as atividades:

30.10.1. Power-On / Inst. Padrão

30.10.2. Enviar Licença do NGFW

30.10.3. Registrar equipamento no portal de suporte do Fabricante

30.10.4. Capturar tela do dashboard inicial do NGFW

30.10.5. Configurações iniciais do sistema

30.10.6. Atualização Firmware

30.10.7. Portas de acessos;

30.10.8. Configurações de horário (NTP / Time Zone);

30.10.9. Credenciais de acesso administrativo;

30.10.10. Configuração de funcionalidades (Features).

30.10.11. Configuração de usuários administrativos

30.10.12. Configurações de interface

30.10.13. Criação de interfaces;

30.10.14. Criação e configuração de zonas;

30.10.15. Configuração de túneis tipo IPSec;

30.10.16. Configurações de interfaces e membros de SD-WAN;

30.10.17. Configurações de regras e monitores de performance para SD-WAN (Rules / SLA);

30.10.18. Configurações de roteamento (roteamento estático / roteamento dinâmico);

30.10.19. Configurações de políticas e objetos (Policy's)

30.10.20. Criação de objetos e grupos de rede (Address / Groups)

30.10.21. Criação de serviços e protocolos (Service / Groups);

30.10.22. Criação de políticas de segurança (Policy's);

30.10.23. Ajustes de precedência de políticas de segurança;

30.10.24. Ajustes de serviços e protocolos a serem liberados nas policys.

30.10.25. Integração com Soluções de Gerência, Autenticação e LOGs

30.10.26. Configuração envio de logs para atual solução

30.10.27. Configuração da solução de Gerência Centralizada

30.10.28. Configuração de Autenticação via Solução de Autenticação

30.10.29. Hands-on da Solução

31. ITEM 31 - SERVIÇOS DE IMPLANTAÇÃO DE ATIVOS DE REDE WIRED

31.1. Os serviços envolvendo a execução de atividade de rotinas de implantação deverão ser prestados de maneira a apoiar os processos de trabalho e atividades pontuais para atender a necessidades específicas apresentadas pela CONTRATANTE

31.2. Os serviços envolverão todas as atividades de configurações, programações e atendimento às demandas apresentadas pela CONTRATANTE, referente aos Itens 05 06 e 07.

31.3. A execução do Contrato deverá seguir metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada. À CONTRATANTE caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços. A CONTRATADA deverá disponibilizar um Gerente do Projeto, o qual deverá supervisionar todas as atividades dos profissionais vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidades de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela CONTRATANTE.

31.4. Os serviços poderão ser realizados nas dependências da CONTRATANTE ou realizados de forma remota e assistida pela equipe de TI da CONTRATANTE.

31.5. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.

31.6. Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE.

31.7. Devem estar contempladas nos serviços de instalação minimamente as atividades:

31.7.1. Power-On / Inst. Padrão

31.7.2. Registro portal do Fabricante

31.7.3. Inserção de Contrato de Suporte

31.7.4. Configurações iniciais do Switch

31.7.5. Atualização de Firmware

31.7.6. Configurações gerais

31.7.7. Configurações de Rede e Gerência na Controladora

31.7.8. Configurações de rede

31.7.9. Configurações de VLAN's

31.7.10. Associação do Ativo de Rede Wired a Controladora

31.7.11. Hands-on da Solução

32. ITEM 32 - SERVIÇOS DE IMPLANTAÇÃO DE ATIVOS DE REDE WIRELESS SEM INFRAESTRUTURA

32.1. Os serviços envolvendo a execução de atividade de rotinas de implantação deverão ser prestados de maneira a apoiar os processos de trabalho e atividades pontuais para atender a necessidades específicas apresentadas pela CONTRATANTE

32.2. Os serviços envolverão todas as atividades de configurações, programações e atendimento às demandas apresentadas pela CONTRATANTE, referente ao item 07.

32.3. A execução do Contrato deverá seguir metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada. À CONTRATANTE caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços. A CONTRATADA deverá disponibilizar um Gerente do Projeto, o qual deverá supervisionar todas as atividades dos profissionais vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidades de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela CONTRATANTE.

32.4. Os serviços poderão ser realizados nas dependências da CONTRATANTE ou realizados de forma remota e assistida pela equipe de TI da CONTRATANTE.

32.5. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.

32.6. Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE.

32.7. A CONTRATADA será responsável pela realização de mapa de calor de cobertura de sinal, mediante a apresentação de planta baixa em formato PDF ou DWG pela CONTRATANTE.

32.8. Devem estar contemplados nos serviços de instalação minimamente as atividades:

32.8.1. Power-On / Inst. Padrão

32.8.2. Registro portal do Fabricante

32.8.3. Inserção de Contrato de Suporte

32.8.4. Fixação do Access Point em local definido pela Contratante

32.8.5. Configurações iniciais do Access Point

32.8.6. Atualização de Firmware

32.8.7. Configurações gerais

32.8.8. Configurações de Rede e Gerência na Controladora

32.8.9. Configurações de rede

32.8.10. Configurações de VLAN's

32.8.11. Associação do Ativo de Rede Wireless a Controladora

32.8.12. Hands-on da Solução

32.9. A instalação deve ocorrer com uso de ferramental apropriada com escadas ou andaimes.

32.10. Todos os trabalhos devem atender as normas regulamentadoras vigentes NR-2 (Inspeção Prévia), NR-03 (Embargo ou Interdição), NR-5 (Comissão Interna de Prevenção de Acidentes), NR-6 (Equipamentos de Proteção Individual - EPI), NR-10 (Segurança em Instalações e Serviços em Eletricidade), NR-11 (Transporte, Movimentação, Armazenagem e Manuseio de Materiais), NR-12 (Máquinas e equipamentos), NR-21 (Trabalhos a Céu Aberto), NR-23 (Proteção Contra Incêndios), NR-26 (Sinalização de Segurança), NR-28 (Fiscalização e Penalidades), NR-35 (Trabalho em Altura).

32.11. A CONTRATADA deve fazer a configuração do Access Point e a conexão lógica com a Controladora Wireless existente.

32.12. A instalação deve ser previamente agendada pela CONTRATADA e o CONTRATANTE.

33. ITEM 33 - SERVIÇOS DE IMPLANTAÇÃO DE ATIVOS DE REDE WIRELESS COM INFRAESTRUTURA

33.1. Os serviços envolvendo a execução de atividade de rotinas de implantação deverão ser prestados de maneira a apoiar os processos de trabalho e atividades pontuais para

atender a necessidades específicas apresentadas pela CONTRATANTE.

33.2. Os serviços envolverão todas as atividades de configurações, programações e atendimento às demandas apresentadas pela CONTRATANTE, referente item 07.

33.3. A execução do Contrato deverá seguir metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada. À CONTRATANTE caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços. A CONTRATADA deverá disponibilizar um Gerente do Projeto, o qual deverá supervisionar todas as atividades dos profissionais vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidades de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela CONTRATANTE.

33.4. Os serviços poderão ser realizados nas dependências da CONTRATANTE ou realizados de forma remota e assistida pela equipe de TI da CONTRATANTE.

33.5. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.

33.6. Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE.

33.7. A CONTRATADA será responsável pela realização de mapa de calor de cobertura de sinal, mediante a apresentação de planta baixa em formato PDF ou DWG pela CONTRATANTE.

33.8. Devem estar contempladas nos serviços de instalação minimamente as atividades:

33.8.1. Power-On / Inst. Padrão

33.8.2. Registro portal do Fabricante

33.8.3. Inserção de Contrato de Suporte

33.8.4. Fixação do Access Point em local definido pela Contratante

33.8.5. Configurações iniciais do Access Point

33.8.6. Atualização de Firmware

33.8.7. Configurações gerais

33.8.8. Configurações de Rede e Gerência na Controladora

33.8.9. Configurações de rede

33.8.10. Configurações de VLAN's

33.8.11. Associação do Ativo de Rede Wireless a Controladora

33.8.12. Hands-on da Solução

33.9. A CONTRATADA deverá fornecer ponto de rede, que deve ser instalado no local que será indicado no site survey;

33.10. Deve incluir materiais (cabeamento lógico, kits de sustentação e ancoragem em posteamento, acessórios e kits montagem).

33.11. A instalação deve ocorrer com uso de ferramental apropriada com escadas ou andaimes.

33.12. O ponto de rede deve passar por tubulações subterrânea ou aérea, ou por ambos os encaminhamentos se necessário, (conforme definido no site survey e aprovado pela CONTRATANTE)

33.13. Deverá ser fornecido quando necessário cabeamento categoria 5e, com infraestrutura, patch cord, line cord, canaleta, guia de cabo, conector RJ-45 fêmea, cabeamento UTP e certificação do ponto lógico para até 90 metros de distância do rack.

33.14. Distância máxima de 90 (noventa) metros entre o access point e o rack de rede.

33.15. Os pontos deverão ser identificados com etiquetas.

33.16. Os pontos de rede devem incluir conectores fêmeas e machos.

33.17. Todos os trabalhos devem atender as normas regulamentadoras NR-2 (Inspeção Prévia), NR-03 (Embargo ou Interdição), NR-5 (Comissão Interna de Prevenção de Acidentes), NR-6 (Equipamentos de Proteção Individual - EPI), NR-10 (Segurança em Instalações e Serviços em Eletricidade), NR-11 (Transporte, Movimentação, Armazenagem e Manuseio de Materiais), NR-12 (Máquinas e equipamentos), NR-21 (Trabalhos a Céu Aberto), NR-23 (Proteção Contra Incêndios), NR-26 (Sinalização de Segurança), NR-28 (Fiscalização e Penalidades), NR-35 (Trabalho em Altura).

33.18. A CONTRATADA deve fazer a configuração do Access Point e a conexão lógica com a Controladora Wireless existente.

33.19. A instalação deve ser previamente agendada pela CONTRATADA e o CONTRATANTE.

34. ITEM 34 – UNIDADE DE SERVIÇOS TÉCNICO ESPECIALIZADOS (UST)

34.1. A UST consiste na “moeda” usada para dimensionar todas as atividades que serão demandadas pela CONTRATANTE, no escopo de cada Ordem de Serviço. A contratação será em volume de UST por atividade e a licitação resultará na oferta do valor de uma UST que irá representar o esforço combinado de profissionais envolvidos, variando a complexidade e prioridade da atividade.

34.2. Cada Unidade de Serviço Técnico (UST) corresponderá à 2h (duas horas) locais de profissional especializado nas plataformas ofertadas. O serviço deve ser prestado pelo próprio fabricante (Professional Services) ou pela empresa contratada.

34.3. Atividades: assessement; desenvolvimento de plano de implementação; planejamento; análise; configuração; integração; migração; testes de verificação; ajustes; tunning; hardening; otimização; troubleshooting; updates; upgrades; provas de conceito; ensaios de contingência; customização de consultas de relatórios; treinamentos “hands on”; análise de vulnerabilidades; criação e manutenção de regras de segurança e redes; participação em comitês de segurança para esclarecimentos; documentação “as built”; documentação para rollout;

34.4. Os perfis dos profissionais/atividades definidas seguirão o padrão de perfis indicados por metodologias de projetos, como PMBOK. Abaixo, um detalhamento sobre os perfis de profissionais e o escopo de cada um de seus papeis:

34.5. Arquitetura: definição da arquitetura lógica e física do projeto, garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais; propor melhorias; definir controles e monitoramento do ambiente, sugerindo métricas, thresholds e indicadores de acompanhamento; apoio no planejamento, execução e avaliação de mudanças;

34.6. Implementação: Levantamento de dados, execução das implantações incluindo configuração customizada, integração, migrações e testes, adaptações código, criação de infraestrutura, orientação, documentação, etc;

34.7. Gerenciamento de projetos: gerenciamento do projeto propriamente dito, considerando controle de prazos, esforço, elaboração de relatórios de posicionamento executivo, indicadores do projeto e qualquer outra métrica prevista no PMBOOK. O objetivo de todas estas atividades é a garantia de qualidade do projeto no que tange prazos e esforço

34.8. Suporte: Atendimento a incidentes de suporte realizando análises, troubleshooting, diagnósticos; realizando ajustes e otimização configurações; analisando e aplicando patches, fixes e updates, aplicando testes e realizando ensaios; monitorando o ambiente;

34.9. Dinâmica de contratação

34.9.1. Será contratada a quantidade de Unidades de Serviços Técnicos estimadas para consumo pelo período desejado durante a vigência do contrato. A CONTRATANTE emitirá nota(s) de empenho para adquirir vouchers para quantidade de Unidades de Serviços Técnicos estimados para o período correspondente.

34.9.2. A Contratada deve entregar os vouchers relativos à quantidade de Unidades de Serviços contratadas, que poderão ser consumidos pela CONTRANTE ao longo do período do contrato, de acordo com a necessidade;

34.9.3. A CONTRATANTE consultará a CONTRATADA para calcular a quantidade de Unidades de Serviços Técnicos necessárias para realizar a atividade pretendida e emitirá Ordem de Serviço para a Contratada prestar os serviços. Ao final dos serviços, contabilizará o consumo das Unidades de Serviços Técnico utilizadas;

34.10. O prazo máximo para início das atividades pela empresa contratada será de 20 (vinte) dias;

34.11. As contabilizações de UST serão feitas individualmente para cada profissional alocado;

34.12. As USTs executadas fora do expediente comercial por solicitação deste órgão, serão contabilizadas em dobro;

34.13. A empresa Contratada deve nomear funcionário capacitado que será responsável por fornecer aconselhamento técnico e operacional sobre os serviços; assistência sobre as condições do contrato; gerenciamento de escalação junto ao Fabricante; Gerenciamento de recursos e cronograma de entrega dos serviços;

34.14. Neste modelo de execução dos serviços não se caracteriza a subordinação direta e nem a pessoalidade, visto que não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da empresa contratada e este Órgão. As empresas proponentes deverão considerar em seus custos todos os recursos necessários ao completo atendimento aos objetos, tais como despesas com pessoal (salários, férias, encargos, benefícios, seleção, outras) de modo a garantir os serviços definidos.

ANEXO II – RELAÇÃO DAS UNIDADES ATENDIDAS

#	DRE	MUNICIPO	ESCOLA	INEP
1	DEA	ARACAJU	CENTRO DE ATENDIMENTO EDUCACIONAL ESPECIALIZADO JOAO CARDOSO NASCIMENTO JUNIOR	28017285
2	DEA	ARACAJU	CENTRO DE EXCELENCIA ATHENEU SERGIPENSE	28017838
3	DEA	ARACAJU	CENTRO DE EXCELÊNCIA BARÃO DE MAUÁ	28018435
4	DEA	ARACAJU	CENTRO DE EXCELÊNCIA DOM LUCIANO CABRAL DUARTE	28018451
5	DEA	ARACAJU	CENTRO DE EXCELÊNCIA GOVERNADOR AUGUSTO FRANCO	28018419
6	DEA	ARACAJU	CENTRO DE EXCELÊNCIA GOVERNADOR DJENAL TAVARES QUEIROZ	28028783
7	DEA	ARACAJU	CENTRO DE EXCELÊNCIA JOHN KENNEDY	28019164
8	DEA	ARACAJU	CENTRO DE EXCELÊNCIA JOSÉ ROLLEMBERG LEITE	28018397
9	DEA	ARACAJU	CENTRO DE EXCELÊNCIA LEANDRO MACIEL	28018460
10	DEA	ARACAJU	CENTRO DE EXCELÊNCIA NELSON MANDELA	28018494
11	DEA	ARACAJU	CENTRO DE EXCELÊNCIA PROFESSORA MARIA IVANDA DE CARVALHO NASCIMENTO	28018486
12	DEA	ARACAJU	CENTRO DE EXCELÊNCIA PROFESSORA OFENÍSIA SOARES FREIRE	28018915
13	DEA	ARACAJU	CENTRO DE EXCELÊNCIA PROFESSOR GONÇALO ROLLEMBERG LEITE	28018400
14	DEA	ARACAJU	CENTRO DE EXCELÊNCIA PROFESSOR JOÃO COSTA	28017862
15	DEA	ARACAJU	CENTRO DE EXCELÊNCIA PROFESSOR JOSÉ CARLOS DE SOUZA	28018478
16	DEA	ARACAJU	CENTRO DE EXCELÊNCIA PROFESSOR PAULO FREIRE	28017854
17	DEA	ARACAJU	CENTRO DE EXCELÊNCIA SANTOS DUMONT	28018940
18	DEA	ARACAJU	CENTRO DE EXCELÊNCIA SECRETÁRIO DE ESTADO FRANCISCO ROSA SANTOS	28018389
19	DEA	ARACAJU	CENTRO DE EXCELÊNCIA VITÓRIA DE SANTA MARIA	28033477
20	DEA	ARACAJU	CENTRO DE REFERENCIA DE E.J.A PROFESSOR SEVERINO UCHOA	28017315
21	DEA	ARACAJU	CENTRO DE EXCELÊNCIA DE EDUCAÇÃO PROFISSIOINAL JOSÉ FIGUEIREDO BARRETO	28026730
22	DEA	ARACAJU	CE PROF BENEDITO OLIVEIRA	28018117
23	DEA	ARACAJU	COLÉGIO ESTADUAL 17 DE MARÇO	28018567
24	DEA	ARACAJU	COLÉGIO ESTADUAL 24 DE OUTUBRO	28018575
25	DEA	ARACAJU	COLÉGIO ESTADUAL ALCEU AMOROSO LIMA	28018591
26	DEA	ARACAJU	COLÉGIO ESTADUAL GENERAL SIQUEIRA	28019725
27	DEA	ARACAJU	COLÉGIO ESTADUAL IVO DO PRADO	28018125
28	DEA	ARACAJU	COLEGIO ESTADUAL JACKSON DE FIGUEIREDO	28017846
29	DEA	ARACAJU	COLÉGIO ESTADUAL JORNALISTA PAULO COSTA	28018702
30	DEA	ARACAJU	COLÉGIO ESTADUAL JOSÉ AUGUSTO FERRAZ	28018729
31	DEA	ARACAJU	COLÉGIO ESTADUAL JUGURTA BARRETO DE LIMA	28031911
32	DEA	ARACAJU	COLÉGIO ESTADUAL LEONOR TELES DE MENEZES	28018761
33	DEA	ARACAJU	COLEGIO ESTADUAL MINISTRO PETRONIO PORTELA	28019067
34	DEA	ARACAJU	COLÉGIO ESTADUAL MONSENHOR CARLOS CAMÉLIO COSTA	28018796
35	DEA	ARACAJU	COLÉGIO ESTADUAL OLAVO BILAC	28018818
36	DEA	ARACAJU	COLÉGIO ESTADUAL PAULINO NASCIMENTO	28019180
37	DEA	ARACAJU	COLÉGIO ESTADUAL PROFESSORA ÁUREA MELO	28018931
38	DEA	ARACAJU	COLÉGIO ESTADUAL PROFESSOR ACRÍSIO CRUZ	28018869

39	DEA	ARACAJU	COLÉGIO ESTADUAL PROFESSORA MARIA DAS GRAÇAS AZEVEDO MELO	28032578
40	DEA	ARACAJU	COLEGIO ESTADUAL PROFESSOR ARICIO FORTES	28018508
41	DEA	ARACAJU	COLÉGIO ESTADUAL PROFESSOR FRANCISCO PORTUGAL	28018885
42	DEA	ARACAJU	COLÉGIO ESTADUAL PROFESSOR JOAQUIM VIEIRA SOBRAL	28018320
43	DEA	ARACAJU	COLEGIO ESTADUAL TOBIAS BARRETO	28018516
44	DEA	ARACAJU	CONSERVATORIO DE MUSICA DE SERGIPE	28032705
45	DEA	ARACAJU	INST. EDUC. STA TEREZINHA DO MENINO JESUS	28031407
46	DEA	ARACAJU	ESCOLA ESTADUAL MARIA MARCIA DE OLIVEIRA MORAES	28019350
47	DEA	ARACAJU	ESCOLA ESTADUAL 08 DE MAIO	28019520
48	DEA	ARACAJU	ESCOLA ESTADUAL 11 DE AGOSTO	28018540
49	DEA	ARACAJU	ESCOLA ESTADUAL 8 DE JULHO	28018583
50	DEA	ARACAJU	ESCOLA ESTADUAL AUGUSTO MAYNARD	28019911
51	DEA	ARACAJU	ESCOLA ESTADUAL CLODOALDO DE ALENCAR	28019040
52	DEA	ARACAJU	ESCOLA ESTADUAL DES. JOAO BOSCO DE ANDRADE LIMA	28019024
53	DEA	ARACAJU	ESCOLA ESTADUAL DR. MANOEL LUIZ	28018648
54	DEA	ARACAJU	ESCOLA ESTADUAL EMBAIXADOR BILAC PINTO	28018656
55	DEA	ARACAJU	ESCOLA ESTADUAL JACINTHO DE FIGUEIREDO MARTINS	28018290
56	DEA	ARACAJU	ESCOLA ESTADUAL JOAO PAULO II	28018680
57	DEA	ARACAJU	ESCOLA ESTADUAL JOSE DA SILVA RIBEIRO FILHO	28019741
58	DEA	ARACAJU	ESCOLA ESTADUAL JOSE DE ALENCAR CARDOSO	28018737
59	DEA	ARACAJU	ESCOLA ESTADUAL MANOEL DIONÍZIO DE SANTANA	28019172
60	DEA	ARACAJU	ESCOLA ESTADUAL MINISTRO GERALDO BARRETO SOBRAL CAIC	28026845
61	DEA	ARACAJU	ESCOLA ESTADUAL MONTEIRO LOBATO	28018800
62	DEA	ARACAJU	ESCOLA ESTADUAL OLIMPIA BITTENCOURT	28018826
63	DEA	ARACAJU	ESCOLA ESTADUAL POETA GARCIA ROSA	28018842
64	DEA	ARACAJU	ESCOLA ESTADUAL PROFª MYRIAM DE OLIVEIRA SANTOS MELO	28020111
65	DEA	ARACAJU	ESCOLA ESTADUAL PROFESSORA JUDITE OLIVEIRA	28018745
66	DEA	ARACAJU	ESCOLA ESTADUAL PROFESSOR ARTHUR FORTES	28003551
67	DEA	ARACAJU	ESCOLA ESTADUAL PROFESSOR MANOEL FRANCO FREIRE	28018893
68	DEA	ARACAJU	ESCOLA ESTADUAL PROFESSOR RUY ELOY	28018923
69	DEA	ARACAJU	ESCOLA ESTADUAL PROFESSOR VALNIR CHAGAS	28019059
70	DEA	ARACAJU	ESCOLA ESTADUAL RODRIGUES DOREA	28019784
71	DEA	ARACAJU	ESCOLA ESTADUAL SAO CRISTOVAO	28018958
72	DEA	ARACAJU	ESCOLA ESTADUAL CORONEL FRANCISCO DE SOUZA PORTO	28020235
73	DEA	ARACAJU	ESCOLA ESTADUAL SENADOR LEITE NETO	28018974
74	DEA	ARACAJU	ESCOLA ESTADUAL WOLNEY LEAL DE MELO	28021096
75	DEA	ARACAJU	ESCOLA ESTADUAL SÃO JOSÉ	28020235
76	DEA	ARACAJU	INSTITUTO DE EDUCAÇÃO RUY BARBOSA	28019806
77	DEA	ARACAJU	JARDIM DE INFANCIA EUVALDO D. GONCALVES C. DOMESTICA	28019938
78	DRE01	ARAUA	COLÉGIO ESTADUAL MANUEL BOMFIM	28021797
79	DRE01	BOQUIM	CENTRO DE EXCELÊNCIA CLEONICE SOARES DA FONSECA	28022033
80	DRE01	BOQUIM	COLEGIO ESTADUAL SEVERIANO CARDOSO	28022025
81	DRE01	BOQUIM	CEEP MARIA FONTES DE FARIA (DONA MARIETA)	28035100
82	DRE01	BOQUIM	ESCOLA ESTADUAL PE. JOSE GUMERCINDO DOS SANTOS	28022378
83	DRE01	CRISTINAPOLIS	COLÉGIO ESTADUAL LEONARDO GOMES DE CARVALHO LEITE	28022394
84	DRE01	CRISTINAPOLIS	COLÉGIO ESTADUAL OTÁVIO DE SOUZA LEITE	28022440
85	DRE01	ESTANCIA	CENTRO DE EXCELÊNCIA SENADOR WALTER FRANCO	28024524
86	DRE01	ESTANCIA	CENTRO DE REFERENCIA DE EDUCACAO DE JOVENS E ADULTOS JORGE AMADO	28024419
87	DRE01	ESTANCIA	COLEGIO ESTADUAL ARABELA RIBEIRO	28024532
88	DRE01	ESTANCIA	COLEGIO ESTADUAL GUMERCINDO BESSA	28024559
89	DRE01	ESTANCIA	COLÉGIO ESTADUAL PROF. GILSON AMADO	28024540

90	DRE01	ESTANCIA	ESCOLA ESTADUAL CONSTANCIO VIEIRA	28024990
91	DRE01	ESTANCIA	ESCOLA ESTADUAL GILBERTO AMADO	28025032
92	DRE01	INDIAROBA	CENTRO DE EXCELÊNCIA ARQUIBALDO MENDONÇA	28025326
93	DRE01	INDIAROBA	COLÉGIO ESTADUAL DIONÍZIO MACHADO	28025180
94	DRE01	ITABAIANINHA	CENTRO DE EXCELÊNCIA PREFEITO JOALDO LIMA DE CARVALHO	28029577
95	DRE01	ITABAIANINHA	COLÉGIO ESTADUAL MONSENHOR OLÍMPIO CAMPOS	28022645
96	DRE01	PEDRINHAS	COLÉGIO ESTADUAL DOUTOR JESSÉ FONTES	28023277
97	DRE01	PEDRINHAS	COLÉGIO ESTADUAL PROFESSORA JOSEFINA LEITE CAMPOS	28023153
98	DRE01	SALGADO	COLÉGIO ESTADUAL ALENCAR CARDOSO	28023315
99	DRE01	SALGADO	COLEGIO ESTADUAL DEPUTADO JOALDO VIEIRA BARBOSA	28040201
100	DRE01	SALGADO	COLÉGIO ESTADUAL FRANCISCO BARBOSA SANTOS	28023331
101	DRE01	SALGADO	E E JOSE CONRADO DE ARAÚJO	28023323
102	DRE01	SANTA LUZIA DO ITANHY	COLÉGIO ESTADUAL COMENDADOR CALAZANS	28025903
103	DRE01	TOMAR DO GERU	CENTRO DE EXCELÊNCIA DOM JOSÉ VICENTE TÁVORA	28023730
104	DRE01	TOMAR DO GERU	C. E. PREF. PEDRO DE BALBINO	28032080
105	DRE01	UMBAUBA	CENTRO ESTADUAL DE EDUCACAO PROFISSIONAL ULISSES GUIMARAES	28036204
106	DRE01	UMBAUBA	COLÉGIO ESTADUAL DOUTOR ANTÔNIO GARCIA FILHO	28024150
107	DRE01	UMBAUBA	COLÉGIO ESTADUAL PREFEITO ANFILÓFIO FERNANDES VIANA	28028562
108	DRE02	LAGARTO	CEN EXC PROF. ABELARDO ROMERO DANTAS	28011104
109	DRE02	LAGARTO	COLÉGIO ESTADUAL DOM MÁRIO RINO SIVIERI	28026667
110	DRE02	LAGARTO	COLÉGIO ESTADUAL DOUTOR EVANDRO MENDES	28012054
111	DRE02	LAGARTO	COLEGIO ESTADUAL LUIZ ALVES DE OLIVEIRA	28011058
112	DRE02	LAGARTO	COLÉGIO ESTADUAL MONSENHOR JUAREZ SANTOS PRATA	28011074
113	DRE02	LAGARTO	COLÉGIO ESTADUAL SILVIO ROMERO	28011082
114	DRE02	LAGARTO	DRE02 / LAGARTO / CE PROF JOSÉ CLÁUDIO MONTEIRO	28032225
115	DRE02	LAGARTO	ESCOLA ESTADUAL MONSENHOR MARINHO	28012100
116	DRE02	LAGARTO	ESCOLA ESTADUAL NOSSA SENHORA DA PIEDADE	28012062
117	DRE02	LAGARTO	ESCOLA ESTADUAL SENADOR LEITE NETO	28012119
118	DRE02	LAGARTO	ESCOLA ROTARY CLUBE	28011945
119	DRE02	POCO VERDE	CENTRO DE EXCELÊNCIA "EPIFÂNIO DÓRIA"	28008782
120	DRE02	POCO VERDE	COLEGIO ESTADUAL PROFESSOR JOAO DE OLIVEIRA	28008677
121	DRE02	POCO VERDE	COLEGIO ESTADUAL SAO JOSE	28009134
122	DRE02	POCO VERDE	COLÉGIO ESTADUAL SEBASTIÃO DA FONSECA	28009223
123	DRE02	POCO VERDE	ESCOLA ESTADUAL ANTONIO MUNIZ DE SOUZA	28008731
124	DRE02	RIACHAO DO DANTAS	COLÉGIO ESTADUAL DOUTOR OSMAN HORA FONTES	28012542
125	DRE02	RIACHAO DO DANTAS	COLÉGIO ESTADUAL LOURIVAL FONTES	28012143
126	DRE02	RIACHAO DO DANTAS	COLÉGIO ESTADUAL NAPOLEÃO DE MENEZES ALVES	28012151
127	DRE02	SIMAO DIAS	CENTRO DE EDUCAÇÃO PROFISSIONAL PROFESSOR UDILSON SOARES RIBEIRO	
128	DRE02	SIMAO DIAS	CENTRO DE EXCELÊNCIA DR MILTON DORTAS	28009398
129	DRE02	SIMAO DIAS	CENTRO DE REFERENCIA DE ED. DE J. E A. PROFESSOR MARCOS FERREIRA	28009266
130	DRE02	SIMAO DIAS	COLÉGIO ESTADUAL FAUSTO CARDOSO	28009851
131	DRE02	SIMAO DIAS	COLEGIO ESTADUAL SENADOR LOURIVAL BAPTISTA	28009487
132	DRE02	SIMAO DIAS	ESCOLA ESTADUAL ARISTEU CARLOS VALADARES	28009401
133	DRE02	SIMAO DIAS	ESCOLA ESTADUAL CARMEM DO PRADO DANTAS AMARAL	28031644
134	DRE02	SIMAO DIAS	ESCOLA ESTADUAL JOAO FERREIRA DE MATOS	28010060
135	DRE02	SIMAO DIAS	ESCOLA ESTADUAL JOAO MATTOS DE CARVALHO	28009894

136	DRE02	SIMAO DIAS	ESCOLA ESTADUAL JOSE DE CARVALHO DEDA	28009533
137	DRE02	SIMAO DIAS	ESCOLA ESTADUAL MARIA DE LOURDES S. LEITE	28009380
138	DRE02	SIMAO DIAS	ESCOLA ESTADUAL PEDRO VALADARES	28009363
139	DRE02	SIMAO DIAS	ESCOLA ESTADUAL VEREADOR MANOEL SOBRINHO	28009576
140	DRE02	TOBIAS BARRETO	CENTRO DE EXCELÊNCIA MARIA ROSA DE OLIVEIRA	28010450
141	DRE02	TOBIAS BARRETO	COLEGIO ESTADUAL ABELARDO BARRETO DO ROSARIO	28010132
142	DRE02	TOBIAS BARRETO	COLÉGIO ESTADUAL PROFESSORA MARIA LUCILENE DE ALMEIDA SANTOS	28010817
143	DRE02	TOBIAS BARRETO	COLEGIO ESTADUAL TOBIAS BARRETO	28010825
144	DRE02	TOBIAS BARRETO	ESCOLA ESTADUAL JOAO ANTONIO CESAR	28010728
145	DRE02	TOBIAS BARRETO	ESCOLA ESTADUAL ROSINHA FELIPE	28010868
146	DRE02	TOBIAS BARRETO	ESCOLA ESTADUAL RURAL ENGENHEIRO JOSE CARVALHO	28031814
147	DRE02	TOBIAS BARRETO	COLÉGIO ESTADUAL PROFESSORA JOSEFA ALVES DE ALMEIDA	28037456
148	DRE03	AREIA BRANCA	COLEGIO ESTADUAL DEPUTADO GUIDO AZEVEDO	28006542
149	DRE03	AREIA BRANCA	COLEGIO ESTADUAL PEDRO DINIZ GONCALVES	28006569
150	DRE03	CAMPO DO BRITO	CENTRO DE EXCELÊNCIA ROQUE JOSÉ DE SOUZA	28006739
151	DRE03	CAMPO DO BRITO	COLEGIO ESTADUAL GUILHERME CAMPOS	28006720
152	DRE03	CAMPO DO BRITO	ESCOLA ESTADUAL DEP. FRANCISCO DA PAIXAO	28030753
153	DRE03	CARIRA	COLEGIO ESTADUAL PROFESSOR ARTUR FORTES	28003551
154	DRE03	FREI PAULO	COLEGIO ESTADUAL PROFESSOR GENTIL TAVARES DA MOTA	28004060
155	DRE03	FREI PAULO	ESCOLA ESTADUAL MARTINHO GARCEZ	28004256
156	DRE03	ITABAIANA	COLEGIO ESTADUAL DR. AIRTON TELES	28007158
157	DRE03	ITABAIANA	COLEGIO ESTADUAL DR. AUGUSTO CESAR LEITE	28007166
158	DRE03	ITABAIANA	COLEGIO ESTADUAL EDUARDO SILVEIRA	28007816
159	DRE03	ITABAIANA	COLEGIO ESTADUAL MURILO BRAGA	28007000
160	DRE03	ITABAIANA	COLEGIO ESTADUAL PADRE MENDONCA	28007140
161	DRE03	ITABAIANA	COLEGIO ESTADUAL PROFESSOR NESTOR CARVALHO LIMA	28007190
162	DRE03	ITABAIANA	ESCOLA ESTADUAL DEP. MANOEL TELES	28007840
163	DRE03	ITABAIANA	ESCOLA ESTADUAL ELIEZER PORTO	28007832
164	DRE03	ITABAIANA	ESCOLA ESTADUAL VICENTE MACHADO MENEZES	28006950
165	DRE03	ITABAIANA	ESCOLA ROTARY DR. CARLOS MELO	28007425
166	DRE03	MACAMBIRA	COLEGIO ESTADUAL MARCOLINO CRUZ SANTOS	28007867
167	DRE03	MALHADOR	COLEGIO ESTADUAL JOSE JOAQUIM CARDOSO	28008227
168	DRE03	MALHADOR	COLEGIO ESTADUAL SAO JOSE	28008057
169	DRE03	MOITA BONITA	COLEGIO ESTADUAL DJENAL TAVARES DE QUEIROZ	28008235
170	DRE03	MOITA BONITA	COLEGIO ESTADUAL PROFª MARIA DA GLORIA COSTA	28008243
171	DRE03	NOSSA SENHORA APARECIDA	ESCOLA ESTADUAL JOAO SALONIO	28004264
172	DRE03	PEDRA MOLE	COLEGIO ESTADUAL AUGUSTO FRANCO	28004582
173	DRE03	PINHAO	COLÉGIO ESTADUAL PROFESSORA ANITA PASSOS DE OLIVEIRA	28004701
174	DRE03	RIBEIROPOLIS	CENTRO DE EXCELÊNCIA ABDIAS BEZERRA	28004809
175	DRE03	RIBEIROPOLIS	COLEGIO ESTADUAL JOAO XXIII	28030095
176	DRE03	RIBEIROPOLIS	COLEGIO ESTADUAL JOSUE PASSOS	28005155
177	DRE03	SAO DOMINGOS	COLEGIO ESTADUAL EMELIANO RIBEIRO	28008421
178	DRE03	SAO MIGUEL DO ALEIXO	CENTRO DE EXCELÊNCIA MIGUEL DAS GRAÇAS	28006356
179	DRE04	CAPELA	C. E. COELHO E CAMPOS	28014553
180	DRE04	CAPELA	CENTRO DE EXCELÊNCIA EDELZIO VIEIRA DE MELO	28014146
181	DRE04	CAPELA	COLÉGIO ESTADUAL IRMÃ MARIA CLEMÊNCIA	28014138
182	DRE04	CAPELA	ESCOLA ESTADUAL MARIA DA GLORIA MOTA CABRAL	28014219
183	DRE04	CAPELA	ESCOLA ESTADUAL MONSENHOR ERALDO BARBOSA DE ALMEIDA	28014081
184	DRE04	CAPELA	ESCOLA ESTADUAL PROFª MARIA BERENICE B. ALVES	28014170
185	DRE04	CARMOPOLIS	CENTRO ESTADUAL DE EDUCAÇÃO PROFISSIONAL	28035585

			GOVERNADOR MARCELO DÉDA CHAGAS	
186	DRE04	CARMOPOLIS	COLÉGIO ESTADUAL POETA JOSÉ SAMPAIO	28016165
187	DRE04	DIVINA PASTORA	CENTRO DE EXCELÊNCIA DOUTOR JOÃO DE MELO PRADO	28014693
188	DRE04	GENERAL MAYNARD	COLÉGIO ESTADUAL PROFESSORA MARIA CONCEIÇÃO DE SANTANA	28016300
189	DRE04	JAPARATUBA	CENTRO DE EXCELÊNCIA SENADOR GONÇALO ROLLEMBERG	28015002
190	DRE04	JAPARATUBA	COLÉGIO ESTADUAL JOSÉ DE MATOS TELES	28029569
191	DRE04	PIRAMBU	COLÉGIO ESTADUAL JOSÉ AMARAL LEMOS	28015983
192	DRE04	ROSARIO DO CATETE	CENTRO DE EXCELÊNCIA LEANDRO MACIEL	28016890
193	DRE04	SANTA ROSA DE LIMA	CENTRO DE EXCELÊNCIA "DR. EDELZIO VIEIRA DE MELO"	28014812
194	DRE04	SIRIRI	CENTRO DE EXCELÊNCIA CORONEL JOSÉ JOAQUIM BARBOSA	28014839
195	DRE05	AQUIDABA	COLÉGIO ESTADUAL FRANCISCO FIGUEIREDO	28005163
196	DRE05	AQUIDABA	ESCOLA DE 1° GRAU NAÇÕES UNIDAS	28005201
197	DRE05	AQUIDABA	ESCOLA ESTADUAL MILTON AZEVEDO	28005198
198	DRE05	CUMBE	COLÉGIO ESTADUAL ALCEBÍADES PAES	28005651
199	DRE05	FEIRA NOVA	COLÉGIO ESTADUAL MARIA MONTESSORI	28000315
200	DRE05	GRACCHO CARDOSO	COLÉGIO ESTADUAL MANOEL ALCINO DO NASCIMENTO	28000951
201	DRE05	ITABI	CENTRO DE EXCELÊNCIA MARIA DAS GRAÇAS MENEZES MOURA	28001150
202	DRE05	NOSSA SENHORA DAS DORES	CENTRO DE EXCELÊNCIA EDUCAÇÃO PROFISSIONALIZANTE BERILA ALVES DE ALMEIDA	28035690
203	DRE05	NOSSA SENHORA DAS DORES	COLÉGIO ESTADUAL GENERAL CALAZANS	28006330
204	DRE05	NOSSA SENHORA DAS DORES	COLÉGIO ESTADUAL PROFESSOR FERNANDO AZEVEDO	28006046
205	DRE06	AMPARO DE SAO FRANCISCO	COLEGIO ESTADUAL MANOEL JOAQUIM DE OLIVEIRA CAMPOS	28012631
206	DRE06	BREJO GRANDE	CENTRO DE EXCELÊNCIA DR. LUIZ GARCIA	28012720
207	DRE06	BREJO GRANDE	C E QUILOMBOLA 03 DE MAIO	28012739
208	DRE06	CANHOBA	COLEGIO ESTADUAL SAO FRANCISCO DE ASSIS	28012836
209	DRE06	CEDRO DE SAO JOAO	CENTRO DE EXCELÊNCIA MANUEL DANTAS	28013018
210	DRE06	ILHA DAS FLORES	COLEGIO ESTADUAL DRº JESSE TRINDADE	28013093
211	DRE06	ILHA DAS FLORES	COLÉGIO ESTADUAL PROFESSOR ANTONIO CALIXTO DE FIGUEIREDO CRUZ	28013158
212	DRE06	ILHA DAS FLORES	ESCOLA ESTADUAL MANOEL ANTONIO PEREIRA	28013212
213	DRE06	JAPOATA	ASSOC. MANTEN. DA ESC. FAMILIA AGRICOLA DE LADEIRINHAS	28026268
214	DRE06	JAPOATA	CENTRO DE EXCELÊNCIA JOSINO MENEZES	28015355
215	DRE06	JAPOATA	COLÉGIO ESTADUAL OTÁVIO BEZERRA	28015444
216	DRE06	JAPOATA	COLEGIO ESTADUAL PROFª. ROBERTA RAMALHO DE SOUZA	28015479
217	DRE06	JAPOATA	COLEGIO ESTADUAL PROFESSORA MARIA VIEIRA DA SILVA SANTOS	28032195
218	DRE06	MALHADA DOS BOIS	COLEGIO ESTADUAL EMILIANO GUIMARAES	28005759
219	DRE06	MURIBECA	COLÉGIO ESTADUAL ALMIRANTE BARROSO	28005848
220	DRE06	NEOPOLIS	CENTRO DE EXCELENCIA MARECHAL PEREIRA LOBO	28013298
221	DRE06	NEOPOLIS	CENTRO ESTADUAL DE EDUCACAO PROFISSIONAL AGONALTO PACHECO DA SILVA	28041801
222	DRE06	NEOPOLIS	COLEGIO ESTADUAL CALDAS JUNIOR	28013247
223	DRE06	NEOPOLIS	COLÉGIO ESTADUAL GOVERNADOR GERAL MANOEL DE MIRANDA	28013310
224	DRE06	NEOPOLIS	ESCOLA DE ENSINO FUNDAMENTAL SAGRADA FAMILIA	28013476

225	DRE06	NEOPOLIS	ESCOLA ESTADUAL MONSENHOR JOSÉ MORENO DE SANT'ANA	28013379
226	DRE06	NEOPOLIS	ESCOLA ESTADUAL ZECA PEREIRA	28013301
227	DRE06	PACATUBA	CENTRO DE EXCELÊNCIA DR. LEANDRO MACIEL	28015622
228	DRE06	PACATUBA	ESCOLA ESTADUAL NOSSA SENHORA SANTANA	28015762
229	DRE06	PROPRIA	CENTRO DE EXCELENCIA JOANA DE F BARBOSA	28013719
230	DRE06	PROPRIA	COLEGIO ESTADUAL CEL JOAO FERNANDES DE BRITO	28013700
231	DRE06	PROPRIA	COLÉGIO ESTADUAL PROFESSOR CEZÁRIO SIQUEIRA	28013875
232	DRE06	PROPRIA	ESCOLA ESTADUAL D. ANTONIO DOS S. CABRAL	28013840
233	DRE06	PROPRIA	ESCOLA ESTADUAL GRACCHO CARDOSO	28013867
234	DRE06	PROPRIA	ESCOLA ESTADUAL PROFESSOR IRMÃO SALATIEL FRANCISCANO DO AMARAL	28013913
235	DRE06	SANTANA DO SAO FRANCISCO	COLEGIO ESTADUAL ANTONIO MATHIAS BARROSO	28013921
236	DRE06	SANTANA DO SAO FRANCISCO	COLÉGIO ESTADUAL PROFESSOR GOMES NETO	28013972
237	DRE06	SAO FRANCISCO	COLEGIO ESTADUAL JOAO DIAS GUIMARAES	28016106
238	DRE06	TELHA	COLEGIO ESTADUAL JOSE GUIMARAES LIMA	28013980
239	DRE07	GARARU	CENTRO DE EXCELÊNCIA NELSON REZENDE DE ALBUQUERQUE	28000897
240	DRE07	GARARU	COLEGIO ESTADUAL PROFESSOR JOSE AUGUSTO DA ROCHA LIMA	28027736
241	DRE07	GARARU	ESCOLA ESTADUAL MONSENHOR RANGEL	28000749
242	DRE07	NOSSA SENHORA DE LOURDES	COLEGIO ESTADUAL ALMIRANTE TAMANDARE	28013620
243	DRE07	NOSSA SENHORA DE LOURDES	COLÉGIO ESTADUAL MONSENHOR FERNANDO GRAÇA LEITE	28013514
244	DRE07	NOSSA SENHORA DE LOURDES	ESCOLA ESTADUAL PROFESSORA EULINA BATISTA DE MELO	28039408
245	DRE07	PORTO DA FOLHA	CENTRO DE EXCELÊNCIA GOVERNADOR LOURIVAL BAPTISTA	28026705
246	DRE07	PORTO DA FOLHA	COLÉGIO ESTADUAL. CEL. MAYNARD GOMES	28003071
247	DRE07	PORTO DA FOLHA	COLÉGIO ESTADUAL PEDRO ALVES DE SOUZA	28003047
248	DRE07	PORTO DA FOLHA	COLEGIO ESTADUAL PROFESSORA CLEMENCIA ALVES DA SILVA	28033884
249	DRE07	PORTO DA FOLHA	COLÉGIO ESTADUAL PROFESSORA MARIA ZENITE DOS SANTOS	28026543
250	DRE07	PORTO DA FOLHA	COLÉGIO ESTADUAL QUILOMBOLA 27 DE MAIO	28003055
251	DRE07	PORTO DA FOLHA	COLÉGIO INDÍGENA ESTADUAL DOM JOSÉ BRANDÃO DE CASTRO	28003535
252	DRE08	BARRA DOS COQUEIROS	COLEGIO ESTADUAL DR. CARLOS FIRPO	28020308
253	DRE08	BARRA DOS COQUEIROS	COLEGIO ESTADUAL PROF. JOSE FRANKLIN	28020340
254	DRE08	BARRA DOS COQUEIROS	ESCOLA REUNIDAS COELHO NETO	28020367
255	DRE08	ITAPORANGA D AJUDA	CENTRO DE EXCELÊNCIA FELISBELLO FREIRE	28025423
256	DRE08	ITAPORANGA D AJUDA	COLEGIO ESTADUAL HELIO WANDERLEY SOBRAL CARVALHO	28028317
257	DRE08	ITAPORANGA D AJUDA	COLÉGIO ESTADUAL PEDRO ALMEIDA VALADARES	28025733
258	DRE08	ITAPORANGA D AJUDA	ESCOLA ESTADUAL FRANCISCO SALES SOBRAL	28025849
259	DRE08	ITAPORANGA D AJUDA	ESCOLA ESTADUAL JOSE SOBRAL GARCEZ	28025873
260	DRE08	LARANJEIRAS	COLEGIO ESTADUAL PROFª ZIZINHA GUIMARAES	28016319

261	DRE08	LARANJEIRAS	ESCOLA ESTADUAL CONEGO FILADELFO OLIVEIRA	28016360
262	DRE08	LARANJEIRAS	ESCOLA ESTADUAL JOAO RIBEIRO	28016335
263	DRE08	MARUIM	CENTRO DE EXCELÊNCIA DR. ALCIDES PEREIRA	28016637
264	DRE08	MARUIM	COLEGIO ESTADUAL FELIPE TIAGO GOMES	28029275
265	DRE08	NOSSA SENHORA DO SOCORRO	CENTRO DE EXCELÊNCIA DE EDUCAÇÃO PROFISSIONAL GOVERNADOR SEIXAS DÓRIA	28035631
266	DRE08	NOSSA SENHORA DO SOCORRO	CENTRO DE EXCELENCIA DEP. JONAS AMARAL	28032306
267	DRE08	NOSSA SENHORA DO SOCORRO	CENTRO DE EXCELÊNCIA GILBERTO FREIRE	28026853
268	DRE08	NOSSA SENHORA DO SOCORRO	CENTRO DE EXCELÊNCIA PROFISSIONALIZANTE PROF. NEUZICE BARRETO	28036069
269	DRE08	NOSSA SENHORA DO SOCORRO	COLEGIO ESTADUAL ALFREDO MONTES	28020464
270	DRE08	NOSSA SENHORA DO SOCORRO	COLEGIO ESTADUAL FREI INOCENCIO	28020502
271	DRE08	NOSSA SENHORA DO SOCORRO	COLEGIO ESTADUAL JOAO BATISTA NASCIMENTO	28020766
272	DRE08	NOSSA SENHORA DO SOCORRO	COLEGIO ESTADUAL POETA JOSE SAMPAIO	28020529
273	DRE08	NOSSA SENHORA DO SOCORRO	COLÉGIO ESTADUAL PROF. ANTONIO FONTES FREITAS	28020456
274	DRE08	NOSSA SENHORA DO SOCORRO	COLEGIO ESTADUAL PROF JOSE BARRETO FONTES	28020421
275	DRE08	NOSSA SENHORA DO SOCORRO	COLEGIO ESTADUAL PROF LEAO MAGNO BRASIL	28020448
276	DRE08	NOSSA SENHORA DO SOCORRO	COLÉGIO ESTADUAL PRES. JUSCELINO KUBITSCHEK	28020480
277	DRE08	NOSSA SENHORA DO SOCORRO	E E POETA JOAO FREIRE RIBEIRO	28020499
278	DRE08	NOSSA SENHORA DO SOCORRO	E E PROF. CECINHA MELO COSTA	28021002
279	DRE08	NOSSA SENHORA DO SOCORRO	ESCOLA ESTADUAL JOAO ARLINDO DE JESUS	28020510
280	DRE08	NOSSA SENHORA DO SOCORRO	ESCOLA ESTADUAL JORGE AMADO	28020472
281	DRE08	NOSSA SENHORA DO SOCORRO	ESCOLA ESTADUAL JORNALISTA CELIO NUNES	28020995
282	DRE08	NOSSA SENHORA DO SOCORRO	ESCOLA ESTADUAL JOSE FREIRE DA COSTA PINTO	28020871
283	DRE08	NOSSA SENHORA DO SOCORRO	ESCOLA ESTADUAL MARIA JOSÉ SANTOS SOUZA	28020804
284	DRE08	NOSSA SENHORA DO SOCORRO	ESCOLA ESTADUAL MARINALVA ALVES	28020774
285	DRE08	NOSSA SENHORA DO SOCORRO	ESCOLA ESTADUAL PROFª JULIA TELES	28020537
286	DRE08	NOSSA SENHORA DO SOCORRO	ESCOLA ESTADUAL PROFESSORA AGDA FONTES FERREIRA	28020987
287	DRE08	NOSSA SENHORA DO SOCORRO	ESCOLA ESTADUAL PROFESSOR DIOMEDES S. DA SILVA	28020979
288	DRE08	NOSSA SENHORA DO SOCORRO	ESCOLA ESTADUAL ZUMBI DOS PALMARES	28029003

289	DRE08	NOSSA SENHORA DO SOCORRO	ESCOLA RURAL PAULO FREIRE	28020715
290	DRE08	RIACHUELO	COLEGIO ESTADUAL PROFª MARIA DE LOURDES GOIS	28028384
291	DRE08	SANTO AMARO DAS BROTAS	COLEGIO ESTADUAL ESPERIDIAO MONTEIRO	28016980
292	DRE08	SANTO AMARO DAS BROTAS	COLEGIO ESTADUAL PROFESSOR. ROGACIANO M LEAO BRASIL	28016971
293	DRE08	SANTO AMARO DAS BROTAS	ESCOLA MENINO JESUS DE SION	28017129
294	DRE08	SAO CRISTOVAO	C E DEPUTADO ELISIO CARMELO	28021045
295	DRE08	SAO CRISTOVAO	CENTRO DE EXCELÊNCIA PROF HAMILTON ALVES ROCHA	28032640
296	DRE08	SAO CRISTOVAO	COLEGIO ESTADUAL ARMINDO GUARANA	28021177
297	DRE08	SAO CRISTOVAO	COLEGIO ESTADUAL PE GASPAR LOURENCO	28021223
298	DRE08	SAO CRISTOVAO	COLÉGIO ESTADUAL PROFª GLORITA PORTUGAL	28021142
299	DRE08	SAO CRISTOVAO	C E PROFª CLARICE DA SILVA	28021231
300	DRE08	SAO CRISTOVAO	ESCOLA ESTADUAL LUIZ GUIMARAES	28021754
301	DRE08	SAO CRISTOVAO	ESCOLA ESTADUAL PROFª NEYDE MESQUITA	28021568
302	DRE08	SAO CRISTOVAO	ESCOLA ESTADUAL PROFª NORMELIA ARAUJO MELO	28021770
303	DRE08	SAO CRISTOVAO	ESCOLA ESTADUAL PROFESSOR MANOEL DOS PASSOS DE OLIVEIRA TELES	28021100
304	DRE08	SAO CRISTOVAO	ESCOLA ESTADUAL SEN. PAULO SARASATE	28021215
305	DRE09	CANINDE DE SAO FRANCISCO	CENTRO DE EXCELÊNCIA DOM JUVÊNCIO DE BRITTO	28000013
306	DRE09	CANINDE DE SAO FRANCISCO	COLEGIO ESTADUAL DELMIRO DE M. BRITTO	28027434
307	DRE09	MONTE ALEGRE DE SERGIPE	CENTRO DE EXCELENCIA 28 DE JANEIRO	28001400
308	DRE09	MONTE ALEGRE DE SERGIPE	COLÉGIO ESTADUAL JOSÉ INÁCIO DE FARIAS	28001630
309	DRE09	NOSSA SENHORA DA GLORIA	CENTRO DE EXCELENCIA MANOEL MESSIAS FEITOSA	28001699
310	DRE09	NOSSA SENHORA DA GLORIA	COLÉGIO ESTADUAL CÍCERO BEZERRA	28001680
311	DRE09	NOSSA SENHORA DA GLORIA	ESCOLA ESTADUAL PADRE LEON GREGORIO	28002199
312	DRE09	NOSSA SENHORA DA GLORIA	ESCOLA ESTADUAL PROFESSORA EVANGELINA AZEVEDO	28002229
313	DRE09	POCO REDONDO	CENTRO DE EXCELÊNCIA "PROFESSORA NOÊMIA DE SOUZA"	28032730
314	DRE09	POCO REDONDO	CENTRO ESTADUAL DE EDUCAÇÃO PROF. DOM JOSE BRANDAO DE CASTRO	28033086
315	DRE09	POCO REDONDO	COLÉGIO ESTADUAL PROFESSOR JOSÉ ARIBALDO DE CAMPOS LIMA	28002261
316	DRE09	POCO REDONDO	COLÉGIO ESTADUAL PROFESSOR JUSTINIANO DE MELO E SILVA	28002245
317	DRE09	POCO REDONDO	ESCOLA ESTADUAL DURVAL RODRIGUES ROSA	28029364
318	DRE09	POCO REDONDO	ESCOLA ESTADUAL TEOTÔNIO ALVES CHINA	28002865
319	SEDUC	ARACAJU	COMPLEXO ADMINISTRATIVO DA SECRETARIA DE ESTADO DA EDUCAÇÃO E DA CULTURA	
320	SEDUC	ARACAJU	BIBLIOTECA PÚBLICA	
321	SEDUC	ARACAJU	ARQUIVO PÚBLICO	
322	SEDUC	ARACAJU	CONSELHO ESTADUAL DE EDUCAÇÃO	
323	SEDUC	ARACAJU	CENTRO DE REFERÊNCIA EM EDUCAÇÃO ESPECIAL	
324	SEDUC	ARACAJU	COORDENADORIA DE EDUCAÇÃO A DISTÂNCIA, FORMAÇÃO E	

			TECNOLOGIAS EDUCACIONAIS	
325	SEDUC	ARACAJU	DIVISÃO DE ALMOXARIFADO	
326	SEDUC	ARACAJU	DIVISÃO DE SEGURANÇA	
327	SEDUC	ARACAJU	SERVIÇO DE MANUTENÇÃO PREDIAL	
328	SEDUC	ARACAJU	DIRETORIA REGIONAL DE EDUCAÇÃO - DEA	
329	DRE01	ESTANCIA	DIRETORIA REGIONAL DE EDUCAÇÃO - DR-01	
330	DRE02	LAGARTO	DIRETORIA REGIONAL DE EDUCAÇÃO - DR-02	
331	DRE03	ITABAIANA	DIRETORIA REGIONAL DE EDUCAÇÃO - DR-03	
332	DRE04	JAPARATUBA	DIRETORIA REGIONAL DE EDUCAÇÃO - DR-04	
333	DRE05	NOSSA SENHORA DAS DORES	DIRETORIA REGIONAL DE EDUCAÇÃO - DR-05	
334	DRE06	PROPRIA	DIRETORIA REGIONAL DE EDUCAÇÃO - DR-06	
335	DRE07	GARARU	DIRETORIA REGIONAL DE EDUCAÇÃO - DR-07	
336	DRE08	NOSSA SENHORA DO SOCORRO	DIRETORIA REGIONAL DE EDUCAÇÃO - DR-08	
337	DRE09	NOSSA SENHORA DA GLORIA	DIRETORIA REGIONAL DE EDUCAÇÃO - DR-09	

ANEXO III - MODELO DE APRESENTAÇÃO DA PROPOSTA

A
SECRETARIA DE ESTADO DA EDUCAÇÃO E DA CULTURA
Ref. PREGÃO N. ____/____.
Empresa: _____
CNPJ: _____
Endereço/Telefone: _____

Em atendimento ao Edital do Pregão à epígrafe, apresentamos a seguinte proposta de preços:

Item	Descrição	Qtde	Unidade de medida	Valor unitário	Valor Total
				R$	R$

Aracaju, _____ de ____ de _____.

Assinaturas

ANEXO IV - MODELO DE ATESTADO DE VISTORIA

ATESTADO DE VISTORIA (VISITA) TÉCNICA

Atestamos que, o Responsável Técnico e/ou Representante Legal da empresa _____, CNPJ nº _____, realizou na data de ____ de _____ de 2024, a vistoria referente ao Certame denominado Pregão Eletrônico nº _____ / 2024, cujo objeto é a contratação de empresa especializada nos serviços de renovação do licenciamento de suporte/assistência técnica da Solução Integrada de Segurança Cibernética em operação na Secretaria de Estado da Educação e da Cultura – SEDUC e o fornecimento de equipamentos de segurança de rede, visando a melhoria e futuras implantações da solução, englobando o fornecimento do projeto executivo, hardware, software, subscrições, instalações, configurações, suporte técnico local, treinamento e demais insumos necessários para o pleno funcionamento das soluções, conforme termos e condições constantes no presente Edital e em seus anexos, declarando o mesmo, para os fins que se façam necessários que em nome da empresa, tomou pleno conhecimento dos detalhes dos serviços a serem contratados e das condições locais, abdicando assim a empresa a qual representa, do direito de alegar desconhecimento acerca de qualquer dificuldade que porventura venha a surgir no transcorrer da execução dos serviços objeto do presente certame.

Aracaju, XX de XXXX de 2024.

_____

Nome, cargo e Assinatura do representante legal da empresa (ou preposto que realizou a visita)

_____

Nome, cargo e Assinatura do representante legal da SEDUC

Aracaju, 19 de novembro de 2024

e-doc SERGIPE **ASSINADO ELETRONICAMENTE**
Verificar autenticidade conforme mensagem apresentada no rodapé do documento

ADILSON OLIVEIRA ANDRADE
Gerente

e-doc SERGIPE **ASSINADO ELETRONICAMENTE**
Verificar autenticidade conforme mensagem apresentada no rodapé do documento

BRENO CARMO DO NASCIMENTO SANTOS
Diretor(a)

Protocolo de Assinatura(s)

O documento acima foi proposto para assinatura digital. Para verificar as assinaturas acesse o endereço http://edocsergipe.se.gov.br/consultacodigo e utilize o código abaixo para verificar se este documento é válido.

Código de verificação: ZQ26-MMAF-GR8L-MM5I

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 12/02/2025 é(são) :

Legenda: Aprovada Indeterminada Pendente

- ADILSON OLIVEIRA ANDRADE - 18/11/2024 07:07:42 (Docflow)
- BRENO CARMO DO NASCIMENTO SANTOS - 19/11/2024 09:43:08 (Docflow)