



ATA DE REGISTRO DE PREÇOS Nº 32/2021
PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS
IFSC

Pregão Nº 32/2021 – SRP

Processo nº 23292.010214/2021-24

O **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA**, CNPJ nº 11.402.887/0001-60, Rua 14 de Julho, 150 – Enseada dos Marinheiros – Coqueiros, Florianópolis/SC – CEP: 88.075-010, doravante denominado apenas CONTRATANTE, neste ato representado pelo seu Reitor, Sr. MAURÍCIO GARIBA JÚNIOR RG 986.743 CPF 464.505.729-49, realizou no site www.comprasnet.gov.br Pregão Eletrônico para Registro de Preços e, nos termos da Lei nº 10.520/02 e os Decretos nº 5.450/05, 7.892/13, 8.250/14, Instrução Normativa Nº 6, de 25 de julho de 2014, Lei nº 8.666/93 e das demais normas aplicáveis, em razão da classificação das propostas apresentadas no **Pregão Eletrônico de Registro de Preços nº 32/2021**, Ata de Julgamento de Preços, divulgada no Comprasnet e homologada pelo Ordenador de Despesas deste IFSC, RESOLVE registrar os preços para a aquisição dos produtos, objeto do Pregão acima citado, que passa a fazer parte desta, tendo sido os referidos preços oferecidos pelas empresas cujas propostas foram classificadas em primeiro lugar no certame acima enumerado.

CLÁUSULA PRIMEIRA – DO OBJETO

A presente Ata tem por objeto assegurar o compromisso de possível contratação entre o IFSC e as empresas vencedoras do certame licitatório referente ao **Pregão Eletrônico nº 32/2021**, cujo objeto é a contratação de pessoa jurídica para **AQUISIÇÃO DE SOLUÇÃO SOLUÇÃO UNIFICADA DE SEGURANÇA E CONECTIVIDADE SEM FIO PARA O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, IFSC**. Conforme descrito no Anexo I desta Ata e ratificado por todas as empresas vencedoras através das declarações anexas.

CLÁUSULA SEGUNDA – DA VALIDADE DA ATA

A presente Ata de registro de Preços terá a validade de 12 (Doze) meses, compreendendo o período de **19/10/2021 a 19/10/2022**.

Subcláusula Primeira – Durante o prazo de validade desta Ata de Registro de Preço, o IFSC não será obrigado a firmar as contratações que dela poderão advir, facultando-se-lhe a realização de licitação específica para a aquisição pretendida, sendo assegurado ao beneficiário do registro preferência de favorecimento em igualdade de condições.

Subcláusula Segunda - Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, observadas as disposições contidas na alínea “d” do inciso II do caput do art. 65 da Lei nº 8.666, de 1993.

Subcláusula Terceira - A Ata poderá sofrer alterações de preços de acordo com as condições estabelecidas no arts. 18 e 19 do Decreto nº 7.892, de 23 de janeiro de 2013.



CLÁUSULA TERCEIRA – DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

A presente Ata de Registro de Preços poderá ser usada por todos os órgãos da Administração Pública Federal, desde que autorizados pelo IFSC.

Subcláusula Primeira - O preço ofertado pela(s) empresa(s) signatária(s) a presente Ata de Registro de Preços é especificado conforme o Anexo I.

Subcláusula Segunda - Em cada fornecedor decorrente desta Ata, serão observadas, quanto ao preço, as cláusulas e condições constantes do Edital referente a mesma.

Subcláusula Terceira - Em cada aquisição, o preço unitário a ser pago será o constante da proposta apresentada pela(s) empresa(s) detentora(s) da presente Ata, a(s) qual(is) também a integram.

CLÁUSULA QUARTA – DA CLASSIFICAÇÃO DAS PROPOSTAS

A relação do(s) item(ns) com a(s) respectiva(s) empresa(s) ofertante(s) do menor valor por item, a(s) qual(is) terá(ão) preferência de contratação constitui o Anexo I desta Ata.

CLÁUSULA QUINTA – DO LOCAL E PRAZO DE ENTREGA.

Em cada aquisição, o prazo de entrega do objeto desta licitação será aquele definido no edital do pregão eletrônico que originou esta Ata e os quantitativos serão os informados na Autorização de Fornecimento, conforme Anexo IV do Edital.

CLÁUSULA SEXTA – DO PAGAMENTO

Em todas as aquisições, o pagamento será feito por meio de ordem bancária transmitida ao Banco do Brasil, para crédito em banco, agência e conta-corrente indicados pelo contratado até 15 (quinze) dias do aceite na respectiva Nota Fiscal pelo órgão requisitante.

Subcláusula Primeira - Para os produtos com entregas diárias e semanais, o IFSC estimará o consumo mensal e emitirá uma Autorização de Fornecimento, sendo que o pagamento se dará após as entregas das quantidades previstas na referida autorização.

CLÁUSULA SÉTIMA – DA ENTREGA

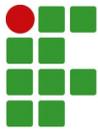
A entrega dos produtos só estará caracterizada mediante o recebimento definitivo do mesmo, ou seja, o aceite na respectiva Nota Fiscal correspondente pelo fiscal do contrato.

Subcláusula Primeira - O fornecedor ficará obrigado a atender todos os pedidos efetuados durante a vigência desta Ata, mesmo que a entrega deles decorrente estiver prevista para data posterior à do seu vencimento.

Subcláusula Segunda - Os materiais deverão ser entregues acompanhados da Nota Fiscal ou Nota Fiscal Fatura correspondente.

CLÁUSULA OITAVA – DAS PENALIDADES

A licitante que ensejar o retardamento da execução do certame, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantido o direito de ampla defesa, ficará impedida de licitar e contratar com a União, e será descredenciada do SICAF, pelo prazo de até 05 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade



sem prejuízo das multas previstas em edital e no contrato, e das demais cominações legais.

Subcláusula Única - A contratada ficará sujeita, ainda, as penalidades previstas no edital do Pregão que originou esta Ata.

CLÁUSULA NONA – DO REAJUSTE DE PREÇOS

Considerando o prazo de validade estabelecido na Cláusula Segunda da presente Ata, e em atendimento ao §1º, art.28, da Lei Federal 9.069 de 29.6.1995 e demais legislação, é vedado qualquer reajuste de preços.

Subcláusula Única - Fica ressalvada a possibilidade de Alteração das condições para a 03/12 concessão de reajuste em face da superveniência de normas federais aplicáveis à espécie.

CLÁUSULA DÉCIMA – DAS CONDIÇÕES DE RECEBIMENTO

Os materiais objetos desta Ata de Registro de preços serão recebidos pelo requisitante consoante o disposto no art. 73 da Lei 8.666/93 e demais normas pertinentes.

CLÁUSULA DÉCIMA PRIMEIRA – DO CANCELAMENTO DA ATA DE REGISTRO DE PREÇOS

Esta Ata de Registro de Preços poderá ser cancelada, de pleno direito:

I – Pela Administração, quando:

- a-** a detentora não cumprir as obrigações constantes desta Ata de Registro de Preços;
- b-** a detentora não assinar a Ata no prazo estabelecido e a Administração não aceitar a sua justificativa;
- c-** a detentora der causa a rescisão administrativa de contrato decorrente de registro de preços;
- d-** em qualquer das hipóteses de inexecução total ou parcial de contrato decorrente de registro de preços;
- e-** os preços registrados se apresentarem superiores aos praticados no mercado;
- f-** por razões de interesse público devidamente demonstradas e justificadas pela Administração;
- g-** a comunicação do cancelamento do preço registrado, nos casos previstos neste Edital, será feita pessoalmente ou por correspondência com aviso de recebimento, juntando-se o comprovante aos autos que deram origem ao registro de preços;
- h-** no caso de ser ignorado, incerto ou inacessível o endereço da detentora, a comunicação será feita por publicação no Diário Oficial da União, considerando-se cancelado o preço registrado após a publicação.

II- Pelas detentoras, quando:

- a-** mediante solicitação por escrito, comprovarem estar impossibilitadas de cumprir as exigências desta Ata de Registro de Preços;
- b-** o fornecedor poderá solicitar o cancelamento do seu registro de preços na ocorrência de



fato superveniente que venha comprometer a perfeita execução contratual, decorrente de caso fortuito ou de força maior, devidamente comprovados;

c- à solicitação das detentoras para cancelamento dos preços registrados deverá ser formulada com a antecedência de 30 (trinta) dias, facultada à Administração a aplicação das penalidades previstas na Lei, caso não aceitas as razões do pedido.

CLÁUSULA DÉCIMA SEGUNDA – DA AUTORIZAÇÃO PARA AQUISIÇÃO E EMISSÃO DAS AUTORIZAÇÕES DE FORNECIMENTO

As aquisições do objeto da presente Ata de Registro de Preço serão autorizadas, caso a caso, pelo Ordenador de Despesas do IFSC.

Subcláusula Primeira - A emissão das autorizações de fornecimento, sua retificação ou cancelamento, total ou parcial serão igualmente autorizados pelo órgão requisitante.

Subcláusula Segunda - Durante o prazo de validade do Registro de Preços, o IFSC poderá ou não contratar o objeto deste pregão.

CLÁUSULA DÉCIMA TERCEIRA – DAS DISPOSIÇÕES FINAIS E DO FORO

Integram esta Ata, o Anexo I (preços registrados) e as declarações de concordância das empresas vencedoras.

Esta Ata está vinculada ao Edital do **Pregão Eletrônico para Registro de Preços nº 32/2021** e às propostas aceitas durante a sessão do referido certame pelas empresas relacionadas no Anexo I desta Ata.

Fica eleito o Foro da Justiça Federal, Seção Judiciária Florianópolis para dirimir quaisquer questões decorrentes da utilização da presente ata.

Os casos omissos serão resolvidos de acordo com a Lei 10.520/2002 e Decreto 5.450/2005, Lei 8.666/93 e demais normas aplicáveis.

Florianópolis, 19 de Outubro de 2021.

MAURÍCIO GARIBA JÚNIOR
REITOR DO IFSC

(Autorizado conforme despacho no Documento nº em 23292.030824/2021-43 19/10/2021).

OBS: A adesão das empresas vencedoras a esta Ata se dá pelas Declarações de Concordância anexas



ANEXO I - DA ATA DE REGISTRO DE PREÇOS

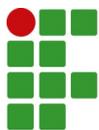
EMPRESAS E PREÇOS REGISTRADOS

Pregão Nº 32 /2021 – SRP

Processo nº 23292.010214/2021-24

Relação de empresas vencedoras, contendo a descrição dos itens e preços negociados na sessão do Pregão.

EMPRESA (1)			RTA REDE DE TECNOLOGIA AVANÇADA LTDA.		
ENDEREÇO			RUA DOM AGUIRRE, Nº 515, VILA SOFIA.. Bairro: VILA SOFIA, SÃO PAULO / SP CEP: 04671-24		
CNPJ			00.429.640/0001-11		
TELEFONE/FAX			: 11 2171-3244		
REPRESENTANTE LEGAL			André Luis Lopes Bueno		
CPF REPRESENTANTE			130.721.488-64		
Email			rta@rta.com.br		
ITE M	UNID.	QTD.	ESPECIFICAÇÃO	Preço Unitário (R\$)	Preço Total (R\$)
23	UNIDA DE	10.0	NOBREAK 10 KVA - TORRE Características mínimas: Potência →10 kVA /10 kW; Tensão entrada → 115/220V~ (Bivolt); Tensão saída → 110/220V (De acordo com a solicitação de cada Câmpus indicada em AF); Fator de potência de saída →1; Conexão de entrada → bornes; Conexão de saída → Bornes + 8 tomadas NBR 14136 (20A); Formato → Torre; Transformador → Isolador; Microprocessador → Microprocessador DSP (Processador Digital de Sinais); Bypass → Automático e Manutenção; Gerenciamento → USB; Topologia → Nobreak (UPS) online monofásico; Forma de Onda → Senoidal pura; Tempo de autonomia → 20 minutos no mínimo; Expansível com módulos externos; Garantia → 3 anos; Proteções para a carga: 1. Queda de rede (Blackout); 2. Ruído de rede	16.000,00	160.000,00



		<p>elétrica; 3. Sobretensão de rede elétrica; 4. Subtensão de rede elétrica; 5. Surtos de tensão na rede; 6. Correção linear de variação da rede elétrica; 7. Variação de frequência da rede elétrica; 8. Distorção harmônica da rede elétrica; 9. Afundamento de tensão (SAG). Outras funcionalidades: Hotswap de baterias; Autodiagnóstico de bateria; Baterias inclusas; Garantia das Baterias ≈ 1 ano; Disjuntor; Autoteste; Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração.*****Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012; Durante o período de garantia dos equipamentos, em caso de troca de baterias, a empresa vencedora deverá recolher as mesmas e dar destinação final de acordo com Resolução CONAMA nº 401, de 04/11/2008. Marca: RTA Fabricante: RTA</p>		
Total				R\$ 160.000,0 0

EMPRESA (2)			TELTEC SOLUTIONS LTDA		
ENDEREÇO			MIGUEL DAUX 100. Bairro: COQUEIROS, FLORIANÓPOLIS / SC		
CNPJ			04.892.991/0001-15		
TELEFONE/FAX			(48) 3031-3450		
REPRESENTANTE LEGAL			Rafael Araújo Silva		
CPF REPRESENTANTE			003.392.439-29		
Email			teltec@teltecsolutions.com.br		
ITEM	UNID.	QTD.	ESPECIFICAÇÃO	Preço Unitário (R\$)	Preço Total (R\$)



1	UNIDA DE	15.0	<p>SWITCH TIPO 2 <i>ou</i> SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA ---</p> <p>> Características Mínimas:</p> <ol style="list-style-type: none">1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;2. 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);3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;5. Deve possuir capacidade de comutação de pelo menos 56 Gbps e ser capaz de encaminhar até 80 Mpps (milhões de pacotes por segundo);6. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;7. Deve possuir tabela MAC com suporte a 8.000 endereços;8. Deve implementar Flow Control baseado no padrão IEEE 802.3X;9. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol <i>ou</i> LACP);10. Deve suportar a comutação de Jumbo Frames;11. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;12. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;10.13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;14. Deve implementar serviço de DHCP Relay;15. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentas) entradas na tabela;16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);17. Deve implementar Spanning Tree conforme	4.900,00	73.500,00
---	-------------	------	---	----------	-----------



		<p>os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;</p> <p>18. 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;</p> <p>19. 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;</p> <p>20. 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;</p> <p>21. 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;</p> <p>22. 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;</p> <p>23. 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;</p> <p>24. 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, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;</p> <p>25. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;</p> <p>26. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);</p> <p>27. Deverá implementar priorização de tráfego baseada nos valores do campo Differentiated Services Code Point (DSCP) do cabeçalho IP, conforme definições do IETF;</p> <p>28. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;</p> <p>29. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-</p>		
--	--	--	--	--



		<p>middle que utilizam o protocolo ARP;</p> <p>30. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;</p> <p>31. 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;</p> <p>32. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;</p> <p>33. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;</p> <p>34. Deve suportar MAC Authentication Bypass (MAB);</p> <p>35. Deve implementar RADIUS CoA (Change of Authorization);</p> <p>36. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;</p> <p>37. 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;</p> <p>38. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;</p> <p>39. 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;</p> <p>40. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;</p> <p>41. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;</p> <p>42. 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;</p> <p>43. 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);</p> <p>44. Deve ser capaz de gerar log de eventos</p>		
--	--	--	--	--



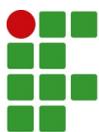
		<p>quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;</p> <p>45. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;</p> <p>46. Deve suportar o envio de mensagens de log para servidores externos através de syslog;</p> <p>47. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;</p> <p>48. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);</p> <p>49. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;</p> <p>50. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);</p> <p>51. Deve permitir ser gerenciado através de IPv6;</p> <p>52. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;</p> <p>53. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;</p> <p>54. 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;</p> <p>55. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;</p> <p>56. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch;</p> <p>57. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;</p> <p>58. Deverá suportar ser configurado e monitorado através de REST API;</p> <p>59. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;</p> <p>60. Deve suportar temperatura de operação de até 45º Celsius;</p> <p>61. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;</p> <p>62. Deve ser fornecido com fonte de</p>		
--	--	---	--	--



			<p>alimentação interna com capacidade para operar em tensões de 110V e 220V; 63. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 64. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 65. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 66. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 67. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V \propto atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET</p>		
2	UNIDA DE	15.0	<p>SWITCH TIPO 3 \propto SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA</p> <ol style="list-style-type: none">1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;2. 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);3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet \propto PoE) e IEEE 802.3at (Power over Ethernet Plus \propto PoE+) com PoE budget de 180W;5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;	8.200,00	123.000,00



		<p>6. Deve possuir capacidade de comutação de pelo menos 56 Gbps e ser capaz de encaminhar até 80 Mpps (milhões de pacotes por segundo);</p> <p>7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;</p> <p>8. Deve possuir tabela MAC com suporte a 8.000 endereços;</p> <p>9. Deve implementar Flow Control baseado no padrão IEEE 802.3X;</p> <p>10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol o LACP);</p> <p>11. Deve suportar a comutação de Jumbo Frames;</p> <p>12. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;</p> <p>13. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;</p> <p>14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;</p> <p>15. Deve implementar serviço de DHCP Relay;</p> <p>16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentas) entradas na tabela;</p> <p>17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);</p> <p>18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;</p> <p>19. 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;</p> <p>20. Deve implementar mecanismo de proteção da o root bridge o do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo o Denial of Service o no ambiente nível 2;</p> <p>21. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo o fast forwarding o (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;</p> <p>22. 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;</p>		
--	--	---	--	--



		<p>23. 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;</p> <p>24. 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;</p> <p>25. 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, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;</p> <p>26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;</p> <p>27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);</p> <p>28. Deverá implementar priorização de tráfego baseada nos valores do campo DDifferentiated Services Code PointP (DSCP) do cabeçalho IP, conforme definições do IETF;</p> <p>29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;</p> <p>30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;</p> <p>31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;</p> <p>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;</p> <p>33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;</p> <p>34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;</p> <p>35. Deve suportar MAC Authentication Bypass (MAB);</p> <p>36. Deve implementar RADIUS CoA (Change of Authorization);</p> <p>37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;</p> <p>38. Em caso de indisponibilidade dos</p>		
--	--	---	--	--



		<p>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;</p> <p>39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;</p> <p>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;</p> <p>41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;</p> <p>42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;</p> <p>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;</p> <p>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);</p> <p>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;</p> <p>46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;</p> <p>47. Deve suportar o envio de mensagens de log para servidores externos através de syslog;</p> <p>48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;</p> <p>49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);</p> <p>50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;</p> <p>51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);</p> <p>52. Deve permitir ser gerenciado através de IPv6;</p>		
--	--	---	--	--



		<p>53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;</p> <p>54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;</p> <p>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;</p> <p>56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;</p> <p>57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch;</p> <p>58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;</p> <p>59. Deverá suportar ser configurado e monitorado através de REST API;</p> <p>60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;</p> <p>61. Deve suportar temperatura de operação de até 45º Celsius;</p> <p>62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;</p> <p>63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;</p> <p>64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;</p> <p>65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo;</p> <p>66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;</p> <p>67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;</p> <p>68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V \mathcal{O} atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e</p>		
--	--	--	--	--



			garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET		
3	UNIDA DE	15.0	Switch Tipo 4 SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. 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); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet PoE) e IEEE 802.3at (Power over Ethernet Plus PoE+) com PoE budget de 370W a serem alocados em qualquer uma das portas 1000Base-T; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 6. Deve possuir capacidade de comutação de pelo menos 56 Gbps e ser capaz de encaminhar até 80 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 8.000 endereços; 9. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol LACP); 11. Deve suportar a comutação de Jumbo Frames; 12. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 13. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;	10.200,00	153.000,00



		<p>15. Deve implementar serviço de DHCP Relay;</p> <p>16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 500 (quinhentas) entradas na tabela;</p> <p>17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);</p> <p>18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;</p> <p>19. 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;</p> <p>20. 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;</p> <p>21. 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;</p> <p>22. 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;</p> <p>23. 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;</p> <p>24. 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;</p> <p>25. 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, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;</p> <p>26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;</p> <p>27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do</p>		
--	--	---	--	--



		<p>frame ethernet (IEEE 802.1p CoS);</p> <p>28. Deverá implementar priorização de tráfego baseada nos valores do campo Differentiated Services Code Point (DSCP) do cabeçalho IP, conforme definições do IETF;</p> <p>29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;</p> <p>30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;</p> <p>31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;</p> <p>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;</p> <p>33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;</p> <p>34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;</p> <p>35. Deve suportar MAC Authentication Bypass (MAB);</p> <p>36. Deve implementar RADIUS CoA (Change of Authorization);</p> <p>37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;</p> <p>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;</p> <p>39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;</p> <p>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;</p> <p>41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface de telefone IP;</p> <p>42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;</p> <p>43. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos</p>		
--	--	--	--	--



		<p>em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;</p> <p>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);</p> <p>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;</p> <p>46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;</p> <p>47. Deve suportar o envio de mensagens de log para servidores externos através de syslog;</p> <p>48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;</p> <p>49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);</p> <p>50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;</p> <p>51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);</p> <p>52. Deve permitir ser gerenciado através de IPv6;</p> <p>53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;</p> <p>54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;</p> <p>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;</p> <p>56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;</p> <p>57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch;</p> <p>58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;</p> <p>59. Deverá suportar ser configurado e</p>		
--	--	--	--	--



			<p>monitorado através de REST API;</p> <p>60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;</p> <p>61. Deve suportar temperatura de operação de até 45º Celsius;</p> <p>62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;</p> <p>63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;</p> <p>64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;</p> <p>65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo;</p> <p>66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;</p> <p>67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;</p> <p>68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i>s atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET</p>		
4	UNIDA DE	15.0	<p>SWITCH TIPO 5 <i>o</i>s SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA</p> <p>1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;</p> <p>2. 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);</p> <p>3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;</p>	7.800,00	117.000,00



		<p>4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;</p> <p>5. Deve possuir capacidade de comutação de pelo menos 104 Gbps e ser capaz de encaminhar até 150 Mpps (milhões de pacotes por segundo);</p> <p>6. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;</p> <p>7. Deve possuir tabela MAC com suporte a 16.000 endereços;</p> <p>8. Deve implementar Flow Control baseado no padrão IEEE 802.3X;</p> <p>9. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol ou LACP);</p> <p>10. Deve suportar a comutação de Jumbo Frames;</p> <p>11. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;</p> <p>12. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;</p> <p>13. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;</p> <p>14. Deve implementar serviço de DHCP Relay;</p> <p>15. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;</p> <p>16. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);</p> <p>17. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;</p> <p>18. 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;</p> <p>19. 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;</p> <p>20. 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;</p>		
--	--	---	--	--



		<p>21. 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;</p> <p>22. 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;</p> <p>23. 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;</p> <p>24. 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, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;</p> <p>25. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;</p> <p>26. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);</p> <p>27. Deverá implementar priorização de tráfego baseada nos valores do campo DDifferentiated Services Code PointD (DSCP) do cabeçalho IP, conforme definições do IETF;</p> <p>28. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;</p> <p>29. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;</p> <p>30. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;</p> <p>31. 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;</p> <p>32. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;</p> <p>33. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;</p> <p>34. Deve suportar MAC Authentication Bypass (MAB);</p> <p>35. Deve implementar RADIUS CoA (Change of</p>		
--	--	--	--	--



		<p>Authorization);</p> <p>36. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;</p> <p>37. 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;</p> <p>38. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;</p> <p>39. 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;</p> <p>40. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;</p> <p>41. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;</p> <p>42. 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;</p> <p>43. 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);</p> <p>44. 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;</p> <p>45. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;</p> <p>46. Deve suportar o envio de mensagens de log para servidores externos através de syslog;</p> <p>47. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;</p> <p>48. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);</p> <p>49. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;</p> <p>50. Deve permitir upload de arquivo e</p>	
--	--	---	--



		<p>atualização do firmware (software) do switch através da interface web (HTTPS);</p> <p>51. Deve permitir ser gerenciado através de IPv6;</p> <p>52. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;</p> <p>53. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;</p> <p>54. 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;</p> <p>55. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;</p> <p>56. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch;</p> <p>57. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;</p> <p>58. Deverá suportar ser configurado e monitorado através de REST API;</p> <p>59. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;</p> <p>60. Deve suportar temperatura de operação de até 45º Celsius;</p> <p>61. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;</p> <p>62. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;</p> <p>63. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;</p> <p>64. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo;</p> <p>65. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;</p> <p>66. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;</p> <p>67. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V o atendimento aos princípios: a) da</p>		
--	--	---	--	--



			padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET		
5	UNIDADE	15.0	SWITCH TIPO 6 <i>ou</i> SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 2. 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); 3. Adicionalmente, deve possuir 4 (quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet <i>ou</i> PoE) e IEEE 802.3at (Power over Ethernet Plus <i>ou</i> PoE+) com PoE budget de 370W; 5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 6. Deve possuir capacidade de comutação de pelo menos 104 Gbps e ser capaz de encaminhar até 150 Mpps (milhões de pacotes por segundo); 7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 8. Deve possuir tabela MAC com suporte a 16.000 endereços; 9. Deve implementar Flow Control baseado no padrão IEEE 802.3X; 10. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol <i>ou</i> LACP); 11. Deve suportar a comutação de Jumbo Frames; 12. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 13. Deve implementar roteamento (camada 3	12.400,00	186.000,00



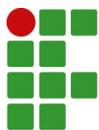
		<p>do modelo OSI) entre as VLANs;</p> <p>14. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;</p> <p>15. Deve implementar serviço de DHCP Relay;</p> <p>16. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;</p> <p>17. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);</p> <p>18. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;</p> <p>19. 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;</p> <p>20. 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;</p> <p>21. 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;</p> <p>22. 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;</p> <p>23. 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;</p> <p>24. 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;</p> <p>25. 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, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;</p> <p>26. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;</p>		
--	--	--	--	--



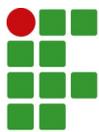
		<p>27. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);</p> <p>28. Deverá implementar priorização de tráfego baseada nos valores do campo DDifferentiated Services Code PointD (DSCP) do cabeçalho IP, conforme definições do IETF;</p> <p>29. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;</p> <p>30. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;</p> <p>31. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;</p> <p>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;</p> <p>33. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;</p> <p>34. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;</p> <p>35. Deve suportar MAC Authentication Bypass (MAB);</p> <p>36. Deve implementar RADIUS CoA (Change of Authorization);</p> <p>37. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;</p> <p>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;</p> <p>39. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;</p> <p>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;</p> <p>41. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;</p> <p>42. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;</p>		
--	--	---	--	--



		<p>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;</p> <p>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);</p> <p>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;</p> <p>46. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;</p> <p>47. Deve suportar o envio de mensagens de log para servidores externos através de syslog;</p> <p>48. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;</p> <p>49. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);</p> <p>50. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;</p> <p>51. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);</p> <p>52. Deve permitir ser gerenciado através de IPv6;</p> <p>53. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;</p> <p>54. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;</p> <p>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;</p> <p>56. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;</p> <p>57. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch;</p> <p>58. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do</p>		
--	--	--	--	--



			<p>equipamento através de controlador SDN; 59. Deverá suportar ser configurado e monitorado através de REST API; 60. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 61. Deve suportar temperatura de operação de até 45º Celsius; 62. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 63. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V; 64. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 65. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 66. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 67. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 68. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET</p>		
6	UNIDA DE	20.0	<p>TRANSCIVER 1000BASE-SX 1. Transceiver SFP para conexão de fibras ópticas multimodo; 2. Deve ser compatível com o padrão 1000BASE-SX para fibras ópticas de até 400 metros; 3. Deve possuir conector LC duplex; 4. Velocidade de 1GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e</p>	530,00	10.600,00



			garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET		
7	UNIDADE	20.0	TRANSCEIVER 1000BASE-LX 1. Transceiver SFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 1000BASE-X para fibras ópticas de até 10 quilômetros; 3. Deve possuir conector LC duplex; 4. Velocidade de 1GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V \propto atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET	1.000,00	20.000,00
8	UNIDADE	20.0	TRANSCEIVER 10GBASE-SR 1. Transceiver SFP para conexão de fibras ópticas multimodo; 2. Deve ser compatível com o padrão 10GBASE-SR para fibras ópticas de até 300 metros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V \propto atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET	1.100,00	22.000,00
9	UNIDADE	20.0	TRANSCEIVER 10GBASE-LR 1. Transceiver SFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 10GBASE-LR para fibras ópticas de até 10 quilômetros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBE; 5. Deve ser compatível com os switches deste	1.364,00	27.280,00



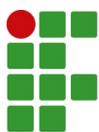
			<p>processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET</p>		
10	LICENÇA A	2.0	<p>FERRAMENTA DE GERENCIAMENTO CENTRALIZADO <i>o</i> SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA</p> <ol style="list-style-type: none">1. Solução que permita administrar de maneira centralizada todos os elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede dos campus e que garanta suporte a processos relativos à LGPD;2. Deverá ser totalmente compatível com a solução proposta para gerenciamento da segurança e infraestrutura de rede dos campus;3. A solução deverá estar devidamente licenciada para administrar todos os pontos de acesso, switches e elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede deste processo pelo período do contrato;4. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;5. A solução deverá ser composta por elemento ou elementos fornecido(s) na forma de appliance virtual (máquina virtual) compatível com Vmware ESXi, Microsoft Hyper-V ou Linux KVM;6. A solução deverá garantir a integridade da configuração de um determinado item através de bloqueio de alterações quando ocorrer acesso simultâneo de dois ou mais administradores no mesmo ativo;7. A solução deverá possibilitar a criação e administração de políticas de firewall, controle de aplicação e filtro de URL;8. A solução deverá permitir criar, de forma centralizada, novos objetos que poderão ser utilizados nas políticas;9. A solução deverá permitir que o administrador localize em quais regras um determinado objeto (ex: computador, serviço, etc.) está sendo utilizado;10. A solução deverá atribuir sequencialmente	53.000,00	106.000,00



		<p>um número a cada regra de firewall, de NAT ou de QoS;</p> <p>11. A solução deverá permitir a criação de regras de filtragem de tráfego que fiquem ativas apenas em horários pré-definidos;</p> <p>12. A solução deverá permitir a criação de regras de filtragem de tráfego com data de expiração;</p> <p>13. A solução deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem/conflitem com outras (shadowing) ou ainda garantir que esta exigência seja plenamente atendida por meio diverso;</p> <p>14. A solução deve permitir a criação de templates de configuração de túneis VPN IPSec a serem aplicados de maneira centralizada e padronizada em elementos concentradores VPN;</p> <p>15. A solução deve permitir agendamento para a execução de configurações nos elementos administrados;</p> <p>16. A solução deve permitir a criação e execução de scripts em elementos administrados de maneira programada;</p> <p>17. A solução deve permitir a criação de templates de configuração a serem aplicados de maneira centralizada e padronizada em elementos da rede sem fio e switches;</p> <p>18. As seguintes características do SSID devem ser configuradas nos pontos de acesso através dos templates: nome do SSID, endereçamento DHCP a ser entregue aos clientes wireless, métodos de autenticação e agendamento da disponibilidade do SSID;</p> <p>19. As seguintes características devem ser configuradas nos pontos de acesso através dos templates: potência de transmissão Wi-Fi, escolha do canal, tamanho do canal, configuração do algoritmo de seleção automática de potência e canal, configuração de short guard interval, modo de operação e acesso administrativo ao ponto de acesso;</p> <p>20. As seguintes características de segurança devem ser configuradas na rede sem fio através dos templates: configuração da detecção de Rogue Aps e configuração de assinaturas de wIDS ou wIPS;</p> <p>21. As seguintes características de Bluetooth Low Energy (BLE) devem ser configuradas nos pontos de acesso através dos templates: configuração do UUID, Major ID, Minor ID, Beacon Interval e potência;</p> <p>22. As seguintes características de VLAN devem ser configuradas nos switches através dos templates: VLAN, VLAN ID e</p>		
--	--	---	--	--



		<p>endereçamento IP;</p> <p>23. As seguintes características de segurança devem ser configuradas nos switches através dos templates: Autenticação 802.1X, Autenticação MAB e Guest VLAN;</p> <p>24. As seguintes características de rede devem ser configuradas nos switches através dos templates: configuração das portas com respectivas VLANs tagged e untagged, configuração do protocolo LLDP e configurações de QoS;</p> <p>25. A solução deve permitir que o administrador selecione em quais elementos os templates de configuração deverão ser aplicados;</p> <p>26. A solução deve listar os elementos administrados e seu status de operação;</p> <p>27. A solução deve listar todos os clientes conectados na rede sem fio, o nome do ponto de acesso ao qual o cliente está conectado, qualidade do sinal da conexão de cada cliente, tipo de dispositivo utilizado na conexão e nome do SSID;</p> <p>28. A solução deve listar todos os Rogue APs na rede sem fio, nome do SSID do propagado, canal impactado, nível de sinal detectado e nome do ponto de acesso que detectou o Rogue AP;</p> <p>29. A solução deve incorporar mapa mundi para visão unificada do status de operação dos elementos. Deve ainda permitir a adição de planta baixa de múltiplas localidades;</p> <p>30. A solução deve garantir visão centralizada do status e estatísticas de uso das interfaces dos switches;</p> <p>31. A solução deve apresentar a topologia da rede com status dos elementos e informações sobre a atuação do protocolo Spanning-Tree em interfaces;</p> <p>32. A solução deve permitir a execução de testes remotos para identificação de problemas em cabos de rede conectados aos switches;</p> <p>33. A solução deve permitir o agrupamento dos elementos administrados para aplicação de políticas ou templates de configuração;</p> <p>34. A solução deverá realizar o backup automático das configurações dos elementos e permitir o retorno (rollback) de uma versão de configuração salva previamente;</p> <p>35. A solução deverá possibilitar que o administrador visualize e compare diferentes versões de configurações dos elementos, sejam elas configurações vigentes, configurações anteriores e configurações antigas;</p>	
--	--	---	--



		<p>36. A solução deverá possuir sistema de backup e restauração de todas as configurações da própria ferramenta de administração centralizada;</p> <p>37. A solução deverá identificar a versão de firmware em execução nos elementos administrados e garantir que quando houver novas versões de software para eles, que seja realizada a distribuição e instalação remota de maneira centralizada;</p> <p>38. A solução deve permitir criar políticas/templates que definam a versão de firmware a ser distribuída e instalada em elementos administrados. Deve permitir ainda que o administrador da rede agende a atualização da versão de firmware de maneira automática nos elementos administrados;</p> <p>39. A solução deve garantir visão centralizada das estatísticas de uso da rede sem fio;</p> <p>40. A solução deve garantir visão centralizada das aplicações mais acessadas na rede, com informações sobre o volume total de dados trafegados para cada aplicação e a identificação dos usuários que fizeram os acessos;</p> <p>41. A solução deve garantir visão centralizada das categorias de websites mais acessados na rede, com informações sobre o volume total de dados trafegados para cada categoria e a identificação dos usuários que fizeram os acessos;</p> <p>42. A solução deve garantir visão centralizada dos usuários que mais trafegaram dados na rede, com informações sobre os hosts aos quais o usuário estava conectado, volume de dados trafegados e os endereços de destino que foram acessados;</p> <p>43. A solução deve garantir visão centralizada das estatísticas de uso dos túneis VPN, com informações sobre volume de dados trafegados, horário da conexão e identificação do usuário que conectou na VPN;</p> <p>44. A solução deverá ser capaz de receber os logs dos elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede das unidades e apresentá-los de forma centralizada;</p> <p>45. A solução deverá ser capaz de receber, no mínimo, 5GB de logs diários;</p> <p>46. A solução deverá ser capaz de armazenar, no mínimo, 3TB de informação;</p> <p>47. A solução deverá ser capaz de armazenar os logs por 12 meses;</p> <p>48. A solução deverá possuir mecanismo para que logs antigos sejam removidos automaticamente;</p>		
--	--	--	--	--



		<p>49. A solução deverá permitir a exportação dos logs;</p> <p>50. A solução deverá permitir que o administrador realize download de um determinado conjunto de logs em formato texto ou CSV;</p> <p>51. A solução deverá garantir a geração de relatórios com mapas geográficos ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego;</p> <p>52. A solução deverá permitir a extração de relatórios;</p> <p>53. A solução deverá possuir relatórios pré-definidos;</p> <p>54. A solução deverá possibilitar a duplicação de relatórios e gráficos existentes para edição dos mesmos logo em seguida;</p> <p>55. A solução deverá permitir a personalização de capas para os relatórios;</p> <p>56. A solução deverá permitir a geração de relatórios de logs de tráfego de dados;</p> <p>57. A solução deverá permitir a personalização dos relatórios para inserção de gráficos dos tipos barra, linha, tabela e pizza;</p> <p>58. A solução deverá possibilitar o envio de relatórios por e-mail de maneira automática;</p> <p>59. A solução deverá permitir a customização de quaisquer relatórios fornecidos pela solução, exclusivamente a critério da contratante, adaptando-o às suas necessidades;</p> <p>60. A solução deverá permitir a definição de filtros nos relatórios;</p> <p>61. A solução deverá ser capaz de definir o layout do relatório, incluir gráficos, inserir textos e imagens, alinhamento, quebras de páginas, definir fontes, cores, entre outros;</p> <p>62. A solução deverá garantir a capacidade de criar consultas avançadas em sua base de dados que para as informações sejam utilizadas em gráficos e tabelas dentro dos relatórios;</p> <p>63. A solução deverá implementar autenticação administrativa através do protocolos RADIUS ou TACACS;</p> <p>64. A solução deverá permitir a criação de múltiplos perfis de usuários administradores com permissões granulares para limitar o acesso a determinadas funções e garantir privilégios de somente leitura e/ou leitura-escrita a outras;</p> <p>65. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7. Durante o período de garantia deve ser possível a atualização do software para novas versões.</p> <p>Marca: SEM MARCA</p>		
--	--	---	--	--



			Fabricante: SEM MARCA		
11	SERVIÇO	10.0	<p>UNIDADE DE SERVIÇO TÉCNICO PARA SITE SURVEY</p> <p>1. O serviço de Site Survey será utilizado para análise técnica do ambiente real dos campus do IFSC em todas as localidades do estado de Santa Catarina de forma presencial nos respectivos endereços, apoiada por ferramentas e softwares adequados, que indiquem:</p> <p>1.1. O melhor posicionamento dos dispositivos pontos de acesso de rede sem fio para a maximização da cobertura do sinal de RF;</p> <p>1.2. A quantidade exata de pontos de acesso a serem instalados por prédio;</p> <p>1.3. Fontes e zonas de interferência;</p> <p>1.4. O canal de frequência a ser utilizado por cada ponto de acesso;</p> <p>1.5. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF em desenho colorido;</p> <p>2. A unidade de serviço deve contemplar um campus independente da sua localidade;</p> <p>3. Será de responsabilidade da CONTRATANTE a disponibilização de planta arquitetônica em CAD (*.dwg) para realização de predição teórica e confecção de as-built;</p> <p>4. Será de responsabilidade da CONTRATADA os seguintes serviços abaixo:</p> <p>4.1. A disponibilização de um ou mais técnicos para realização de testes em campos para determinar a melhor disposição dos pontos de acesso de rede sem fio;</p> <p>4.2. Relatório técnico de vistoria resultante da predição teórica das plantas fornecidas pela CONTRATANTE com as seguintes informações:</p> <p>4.2.1. As possíveis limitações físicas ou dificuldades de implementação detectados nos locais e restrições da construção, obstáculos, etc.;</p> <p>4.2.2. Melhor posicionamento dos dispositivos em cada andar das localidades visando a maximização da cobertura do sinal de RF;</p> <p>4.2.3. A quantidade exata de pontos de acesso a ser instalados em cada andar e locais previstos no projeto;</p> <p>4.2.4. As zonas e faixas de interferência detectadas durante o mapeamento de rádio frequência;</p> <p>4.2.5. As faixas de frequência a serem utilizadas para cada ponto de acesso;</p> <p>4.2.6. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF avaliados durante o mapeamento;</p> <p>5. O relatório técnico deverá ser emitido com</p>	7.300,00	73.000,00



			<p>timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;</p> <p>6. Todos os instrumentos/equipamentos e softwares necessários para a execução do serviço serão fornecidos pela CONTRATADA;</p> <p>7. O relatório técnico de vistoria com o resultado do estudo de site survey deverá ser entregue ao analista ou técnico de TI lotados no câmpus em avaliação, em via impressa ou em meio digital em até 30 (trinta) dias úteis após assinatura do contrato para os itens acima citados.</p> <p>Marca: SEM MARCA Fabricante: -</p>		
12	SERVIÇO	10.0	<p>SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE REDES E SEGURANÇA PARA CAMPUS TIPOS 1, 2, 3 E 4 --> Características Mínimas:</p> <p>1. Entende-se por configuração da solução a configuração lógica de todos os equipamentos e softwares envolvidos, de acordo com o cenário requerido pela CONTRATANTE;</p> <p>2. O serviço deverá contemplar a configuração de uma unidade da Solução de gerenciamento de redes e segurança para campus tipos 1, 2, 3 ou 4 especificados nesse processo;</p> <p>3. Deverá contemplar também a adição do(s) dispositivo(s) da solução na ferramenta de gerenciamento centralizado;</p> <p>4. O serviço de configuração poderá ser realizado de maneira 100% remota, desde que devidamente acordado e documentado entre a CONTRATANTE e a CONTRATADA;</p> <p>5. São de responsabilidade da CONTRATADA, entre outras atividades:</p> <p>5.1. Analisar o ambiente atual como topologia de rede, configurações de camada 2, camada 3 e migração de regras dos firewalls em produção no ambiente atual para a nova solução;</p> <p>5.2. Efetuar a configuração dos perfis de acesso da solução de gerência com as devidas permissões;</p> <p>5.3. Configurar as funcionalidades relevantes a implementação da solução como: Endereçamento, VLANs, LACP, DHCP e tipos NAT;</p> <p>5.4. Configurações de roteamento estático e protocolos dinâmicos como BGP e OSPF;</p> <p>5.5. Realizar a configuração das políticas de firewall analisando a configuração dos equipamentos atuais e sugerindo novas regras para implementação de controles, políticas por porta e protocolo, políticas por aplicações, categorias de aplicações, políticas por usuários</p>	22.000,00	220.000,00



		<p>e grupos de usuários;</p> <p>5.6. Implementar políticas de bloqueios de arquivos;</p> <p>5.7. Configurar limitações de banda com base no IP de origem, usuários e grupos;</p> <p>5.8. Configurar regras de IPS, Anti-Malware e Filtro URL;</p> <p>5.9. Configuração da ferramenta de gerenciamento centralizado;</p> <p>5.10. Configuração da autenticação dos usuários wireless por meio da base de usuários do servidor de diretório da CONTRATANTE, utilizando o protocolo IEEE 802.1x, de modo que o acesso do usuário seja liberado pela solução apenas após sua autenticação;</p> <p>5.11. Configuração para permitir autenticação Web para estações de trabalho sem cliente 802.1x instalado;</p> <p>5.12. Configuração para permitir autenticação pelo MAC Address, para dispositivos sem cliente 802.1x e sem browser;</p> <p>5.13. Configuração das assinaturas de wIDS/Wips;</p> <p>5.14. Configuração de políticas de bloqueio de rogue APs;</p> <p>5.15. Configuração para classificação/detecção de interferências WiFi e não-WiFi;</p> <p>5.16. Configuração dos pontos de acesso sem fio;</p> <p>5.17. Configuração de SSIDs;</p> <p>5.18. Configuração do controle de aplicações permitindo ao administrador filtrá-las para que seja obedecida a política de segurança;</p> <p>5.19. Configuração de um portal de autenticação web para os usuários visitantes, com as seguintes funcionalidades:</p> <p>5.19.1. Funcionar de forma criptografada com o uso de certificados (SSL);</p> <p>5.19.2. Customizar com logotipo e políticas de acesso;</p> <p>5.19.3. Check-box para aceite com as políticas de acesso da rede;</p> <p>6. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento;</p> <p>7. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais</p>		
--	--	--	--	--



		<p>atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes;</p> <p>8. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação;</p> <p>9. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE;</p> <p>10. A CONTRATADA deverá elaborar relatório de instalação (RI), em formulário timbrado próprio da CONTRATADA, com registro das ordens de serviço, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da Contratante, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE;</p> <p>11. Quando aprovado o funcionamento de todo o escopo, tendo como base os itens do RI para a solução, deverão ser considerados instalados e aptos a serem utilizados, devendo ser confirmado pelo nome, matrícula, data e assinatura do representante técnico da CONTRATANTE no RI;</p> <p>12. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação;</p> <p>13. O RI não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento da solução, o qual deverá ser estendido ao longo de todo o período de garantia;</p> <p>14. A falta da configuração completa de um ou mais itens previamente acordados e aprovados por ambas as partes constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de configuração da solução correspondente, enquanto perdurar a configuração incompleta;</p> <p>15. Concluídos a configuração e os testes de</p>		
--	--	---	--	--



			<p>funcionalidade, a CONTRATADA deverá elaborar a DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO contendo todas as informações da implantação:</p> <p>15.1. Aspecto da arquitetura implantada; 15.2. Configuração; 15.3. Descrição das características e recursos utilizados; 15.4. Testes e integração dos ambientes de redes locais da instalação; 16. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA; 17. A documentação poderá ser entregue em via impressa ou meio digital; 18. A documentação deverá ser validada pela equipe técnica da CONTRATANTE; 19. Toda informação manuseada durante a instalação, configuração e testes são de uso restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE; 20. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas; Marca: SEM MARCA Fabricante: -</p>		
13	SERVIÇO	1.0	<p>SERVIÇO DE CONFIGURAÇÃO DA SOLUÇÃO DE REDES E SEGURANÇA PARA CAMPUS TIPO 5</p> <p>1. Entende-se por configuração da solução a configuração lógica de todos os equipamentos e softwares envolvidos, de acordo com o cenário requerido pela CONTRATANTE; 2. O serviço deverá contemplar a configuração de uma unidade da Solução de gerenciamento de redes e segurança para campus tipo 5 e a instalação e configuração da ferramenta de gerenciamento centralizado especificado nesse processo; 3. O serviço de configuração poderá ser realizado de maneira 100% remota, desde que devidamente acordado e documentado entre a CONTRATANTE e a CONTRATADA; 4. São de responsabilidade da CONTRATADA, entre outras atividades: 4.1. Analisar o ambiente atual como topologia de rede, configurações de camada 2, camada 3</p>	39.500,00	39.500,00



		<p>e migração de regras dos firewalls em produção no ambiente atual para a nova solução;</p> <p>4.2. Efetuar a configuração dos perfis de acesso da solução de gerência com as devidas permissões;</p> <p>4.3. Configurar as funcionalidades relevantes a implementação da solução como: Endereçamento, VLANs, LACP, DHCP e tipos NAT;</p> <p>4.4. Configurações de roteamento estático e protocolos dinâmicos como BGP e OSPF;</p> <p>4.5. Realizar a configuração das políticas de firewall analisando a configuração dos equipamentos atuais e sugerindo novas regras para implementação de controles, políticas por porta e protocolo, políticas por aplicações, categorias de aplicações, políticas por usuários e grupos de usuários;</p> <p>4.6. Implementar políticas de bloqueios de arquivos;</p> <p>4.7. Configurar limitações de banda com base no IP de origem, usuários e grupos;</p> <p>4.8. Configurar regras de IPS, Anti-Malware e Filtro URL;</p> <p>4.9. Configuração da ferramenta de gerenciamento centralizado;</p> <p>4.10. Configuração da autenticação dos usuários wireless por meio da base de usuários do servidor de diretório da CONTRATANTE, utilizando o protocolo IEEE 802.1x, de modo que o acesso do usuário seja liberado pela solução apenas após sua autenticação;</p> <p>4.11. Configuração para permitir autenticação Web para estações de trabalho sem cliente 802.1x instalado;</p> <p>4.12. Configuração para permitir autenticação pelo MAC Address, para dispositivos sem cliente 802.1x e sem browser;</p> <p>4.13. Configuração das assinaturas de WIDS/WiPs;</p> <p>4.14. Configuração de políticas de bloqueio de rogue APs;</p> <p>4.15. Configuração para classificação/detecção de interferências WiFi e não-WiFi;</p> <p>4.16. Configuração dos pontos de acesso sem fio;</p> <p>4.17. Configuração de SSIDs;</p> <p>4.18. Configuração do controle de aplicações permitindo ao administrador filtrá-las para que seja obedecida a política de segurança;</p> <p>4.19. Configuração de um portal de autenticação web para os usuários visitantes, com as seguintes funcionalidades:</p> <p>4.19.1. Funcionar de forma criptografada com o uso de certificados (SSL);</p>		
--	--	--	--	--



		<p>4.19.2. Customizar com logotipo e políticas de acesso;</p> <p>4.19.3. Check-box para aceite com as políticas de acesso da rede;</p> <p>5. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento;</p> <p>6. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes;</p> <p>7. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação;</p> <p>8. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE;</p> <p>9. A CONTRATADA deverá elaborar relatório de instalação (RI), em formulário timbrado próprio da CONTRATADA, com registro das ordens de serviço, anotações de irregularidades encontradas e de todas as ocorrências relativas à execução do contrato, o qual será feito na periodicidade definida pela fiscalização da Contratante, em 2 (duas) vias, sendo a primeira para uso da CONTRATANTE e a segunda para a CONTRATADA, devendo ser assinado conjuntamente pelo representante da CONTRATADA e pela fiscalização da CONTRATANTE;</p> <p>10. Quando aprovado o funcionamento de todo o escopo, tendo como base os itens do RI para a solução, deverão ser considerados instalados e aptos a serem utilizados, devendo ser confirmado pelo nome, matrícula, data e assinatura do representante técnico da CONTRATANTE no RI;</p> <p>11. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA</p>		
--	--	---	--	--



			<p>deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação;</p> <p>12. O RI não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento da solução, o qual deverá ser estendido ao longo de todo o período de garantia;</p> <p>13. A falta da configuração completa de um ou mais itens previamente acordados e aprovados por ambas as partes constitui-se em motivo de suspensão de todos os compromissos financeiros, vinculados ao evento de configuração da solução correspondente, enquanto perdurar a configuração incompleta;</p> <p>14. Concluídos a configuração e os testes de funcionalidade, a CONTRATADA deverá elaborar a DOCUMENTAÇÃO TÉCNICA DA INSTALAÇÃO contendo todas as informações da implantação:</p> <p>14.1. Aspecto da arquitetura implantada;</p> <p>14.2. Configuração;</p> <p>14.3. Descrição das características e recursos utilizados;</p> <p>14.4. Testes e integração dos ambientes de redes locais da instalação;</p> <p>15. A documentação deverá ser emitida com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA;</p> <p>16. A documentação poderá ser entregue em via impressa ou meio digital;</p> <p>17. A documentação deverá ser validada pela equipe técnica da CONTRATANTE;</p> <p>18. Toda informação manuseada durante a instalação, configuração e testes são de uso restrito da CONTRATANTE. A CONTRATADA deverá assumir compromisso de manter em sigilo, bem como não fazer uso indevido de qualquer configuração do ambiente e informações prestadas por funcionários da CONTRATANTE e quaisquer outras informações pertencentes à CONTRATANTE;</p> <p>19. Após toda a configuração devidamente realizada e validada a CONTRATADA deverá realizar um treinamento da solução implementada no formato de repasse de conhecimentos com carga horária mínima de 8 horas;</p> <p>Marca: SEM MARCA Fabricante: -</p>		
14	UNIDA DE	270.0	INJETOR POE  SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA	1.200,00	324.000,00



			<p>1. Injetor PoE (power injector) para alimentação de dispositivos PoE onde não há switch com esta tecnologia;</p> <p>2. Deve permitir o fornecimento de energia capaz de alimentar os pontos de acesso deste processo</p> <p>3. Deve fornecer no mínimo 30 Watts para alimentação do dispositivo com suporte PoE atendendo ao padrão IEEE 802.3at;</p> <p>4. Deve acompanhar cabos de energia e acessórios para o seu perfeito funcionamento;</p> <p>5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V ou 220V com comutação automática. Deve acompanhar o cabo de alimentação;</p> <p>6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V \propto atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).*****</p> <p>Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012.</p> <p>Marca: FORTINET Fabricante: FORTINET</p>		
15	UNIDA DE	6.0	<p>SWITCH TIPO 1 \propto SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA</p> <p>1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;</p> <p>2. 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);</p> <p>3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo</p>	19.900,00	119.400,00



		<p>e devem operar simultaneamente em conjunto com as interfaces do item anterior;</p> <ol style="list-style-type: none">4. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;5. Deve possuir 1 (uma) interface USB;6. Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 260 Mpps (milhões de pacotes por segundo);7. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;8. Deve possuir tabela MAC com suporte a 32.000 endereços;9. Deve operar com latência igual ou inferior à 1us (microsegundo);10. Deve implementar Flow Control baseado no padrão IEEE 802.3X;11. Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente;12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol ou LACP);13. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos os switches como uma única interface lógica;14. Deve suportar a comutação de Jumbo Frames;15. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;16. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;17. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;18. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIPv1, RIPv2, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;19. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de		
--	--	--	--	--



		<p>redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;</p> <p>20. Deverá suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;</p> <p>21. Deve implementar serviço de DHCP Server e DHCP Relay;</p> <p>22. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;</p> <p>23. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);</p> <p>24. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;</p> <p>25. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;</p> <p>26. 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;</p> <p>27. 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;</p> <p>28. 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;</p> <p>29. 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;</p> <p>30. 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;</p> <p>31. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve</p>		
--	--	--	--	--



		<p>descartar os pacotes ou aplicar rate limit;</p> <p>32. 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, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;</p> <p>33. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;</p> <p>34. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);</p> <p>35. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo Differentiated Services Code Point D (DSCP) do cabeçalho IP, conforme definições do IETF;</p> <p>36. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ);</p> <p>37. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;</p> <p>38. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;</p> <p>39. Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;</p> <p>40. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;</p> <p>41. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;</p> <p>42. 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;</p> <p>43. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;</p> <p>44. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;</p> <p>45. Deve suportar MAC Authentication Bypass (MAB);</p> <p>46. Deve implementar RADIUS CoA (Change of</p>		
--	--	---	--	--



		<p>Authorization);</p> <p>47. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;</p> <p>48. 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;</p> <p>49. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;</p> <p>50. 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;</p> <p>51. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;</p> <p>52. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;</p> <p>53. 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;</p> <p>54. 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);</p> <p>55. 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;</p> <p>56. Deve ser capaz de autorizar a transmissão de pacotes nas interfaces somente para aqueles endereços IP que foram aprendidos dinamicamente através de DHCP Snooping. Os pacotes originados por endereços IP desconhecidos deverão ser descartados;</p> <p>57. Deve suportar o protocolo PTP (Precision Time Protocol);</p> <p>58. Deve implementar Netflow, sFlow ou similar;</p> <p>59. Deve suportar o envio de mensagens de log para servidores externos através de syslog;</p> <p>60. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;</p>	
--	--	--	--



		<p>61. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);</p> <p>62. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;</p> <p>63. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);</p> <p>64. Deve permitir ser gerenciado através de IPv6;</p> <p>65. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;</p> <p>66. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;</p> <p>67. 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;</p> <p>68. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;</p> <p>69. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;</p> <p>70. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;</p> <p>71. Deverá suportar ser configurado e monitorado através de REST API;</p> <p>72. Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark;</p> <p>73. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;</p> <p>74. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);</p> <p>75. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;</p> <p>76. Deve suportar temperatura de operação de até 45º Celsius;</p> <p>77. Deve possuir MTBF (Mean Time Between</p>		
--	--	--	--	--



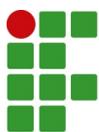
			<p>Failures) igual ou superior a 10 (dez) anos; 78. Deve ser fornecido com fontes de alimentação redundantes e internas ao equipamento, com capacidade para operar em tensões de 110V e 220V; 79. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 80. O switch deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 81. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 82. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 83. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V o atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET</p>		
16	UNIDA DE	250.0	<p>PONTO DE ACESSO INDOOR o SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA</p> <ol style="list-style-type: none">1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança;2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;3. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará;4. Deve permitir ser gerenciado remotamente através de links WAN;5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir	4.330,00	1.082.500,00



		<p>configurações independentes para cada rádio;</p> <p>7. 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;</p> <p>8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;</p> <p>9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;</p> <p>10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;</p> <p>11. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;</p> <p>12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;</p> <p>13. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC;</p> <p>14. 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 a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança;</p> <p>15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPSec;</p> <p>16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os</p>		
--	--	---	--	--



		<p>endereços especificados nas listas de exceção;</p> <p>17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança;</p> <p>18. Deve permitir operação em modo Mesh;</p> <p>19. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;</p> <p>20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;</p> <p>21. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);</p> <p>22. Deve suportar OFDMA;</p> <p>23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;</p> <p>24. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;</p> <p>25. Deve suportar BSS Coloring;</p> <p>26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;</p> <p>27. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);</p> <p>28. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;</p> <p>29. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;</p> <p>30. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;</p> <p>31. Em conjunto com a solução de gerenciamento de redes e segurança, 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;</p> <p>32. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;</p>		
--	--	--	--	--



		<p>33. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);</p> <p>34. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;</p> <p>35. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);</p> <p>36. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3;</p> <p>37. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;</p> <p>38. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;</p> <p>39. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;</p> <p>40. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;</p> <p>41. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;</p> <p>42. Deve implementar o padrão IEEE 802.11e;</p> <p>43. Deve implementar o padrão IEEE 802.11h;</p> <p>44. Deve implementar o padrão IEEE 802.3az;</p> <p>45. Deve suportar ser gerenciado via SNMP;</p> <p>46. Deve suportar consultas via REST API;</p> <p>47. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;</p> <p>48. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;</p> <p>49. Deve suportar sistema antifurto do tipo</p>		
--	--	--	--	--



			<p>Kensington Security Lock ou similar; 50. Deve possuir indicadores luminosos (LED) para indicação de status; 51. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 52. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 53. Deve possuir certificado emitido pela Wi-Fi Alliance; 54. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 55. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V \propto atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET</p>		
17	UNIDA DE	20.0	<p>PONTO DE ACESSO OUTDOOR - SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança; 2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 3. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 4. Deve permitir ser gerenciado remotamente através de links WAN; 5. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 6. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 7. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi</p>	8.600,00	172.000,00



		<p>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;</p> <p>8. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;</p> <p>9. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;</p> <p>10. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T, ou superior, com conector RJ-45 para permitir a conexão com a rede LAN;</p> <p>11. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;</p> <p>12. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;</p> <p>13. Deve permitir sua alimentação através de Power Over Ethernet (PoE). Deve acompanhar injetor PoE para alimentação do equipamento;</p> <p>14. 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 a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança;</p> <p>15. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPSec;</p> <p>16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;</p> <p>17. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local</p>		
--	--	---	--	--



		<p>Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança;</p> <ol style="list-style-type: none">18. Deve permitir operação em modo Mesh;19. Deve possuir potência de irradiação de 25dBm em 2.4GHz e 5GHz;20. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1.2 Gbps em um único rádio;21. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);22. Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL);23. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;24. Deve implementar recurso de Target Wake Time (TWT) configurado por SSID;25. Deve suportar BSS Coloring;26. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;27. Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20);28. Deve possuir antenas internas ao equipamento com ganho mínimo de 6dBi em 2.4GHz e 6dBi em 5GHz;29. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;30. Em conjunto com a solução de gerenciamento de redes e segurança, 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;31. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;32. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);33. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas		
--	--	---	--	--



		<p>de segurança e rede. Deve ser possível criar até 8 (oito) SSIDs com operação simultânea;</p> <p>34. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);</p> <p>35. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3 com 802.1X;</p> <p>36. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;</p> <p>37. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;</p> <p>38. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;</p> <p>39. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;</p> <p>40. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;</p> <p>41. Deve implementar o padrão IEEE 802.11e;</p> <p>42. Deve implementar o padrão IEEE 802.11h;</p> <p>43. Deve implementar o padrão IEEE 802.3az;</p> <p>44. Deve suportar consultas SNMP diretamente no ponto de acesso;</p> <p>45. Deve suportar consultas REST API diretamente no ponto de acesso;</p> <p>46. Deve possuir estrutura robusta para operação em ambientes externos e permitir ser instalado em paredes e postes. Deve acompanhar os acessórios para fixação em paredes e postes;</p> <p>47. Deve ser capaz de operar em ambientes com temperaturas entre -10 e 60º C;</p> <p>48. O equipamento deve possuir grau de proteção IP67. Não serão aceitos equipamentos instalados em acessórios, por exemplo caixas herméticas, para que alcancem este grau de proteção;</p>		
--	--	--	--	--



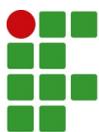
			<p>49. Deve possuir indicadores luminosos (LED) para indicação de status das interfaces físicas e dos rádios Wi-Fi;</p> <p>50. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo;</p> <p>51. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;</p> <p>52. Deve possuir certificado emitido pela Wi-Fi Alliance;</p> <p>53. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;</p> <p>54. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V \propto atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET</p>		
18	UNIDADE	2.0	<p>SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 1---> Características Mínimas:</p> <p>1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus;</p> <p>2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante;</p> <p>3. Cada appliance físico deve possuir, pelo menos, 5 (cinco) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX;</p> <p>4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação;</p> <p>5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de</p>	8.650,00	17.300,00



		<p>falhas;</p> <p>6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;</p> <p>7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo;</p> <p>8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica;</p> <p>9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso;</p> <p>10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;</p> <p>11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados;</p> <p>12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 288 (duzentos e oitenta e oito) portas de switch ou um total de 6 (seis) switches;</p> <p>13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas;</p> <p>14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados;</p> <p>15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;</p> <p>16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;</p> <p>17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;</p> <p>18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;</p> <p>19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;</p> <p>20. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos</p>		
--	--	---	--	--



		<p>switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;</p> <p>21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;</p> <p>22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;</p> <p>23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 8 (oito) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor;</p> <p>24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;</p> <p>25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet;</p> <p>26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;</p> <p>27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6;</p> <p>28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;</p> <p>29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;</p> <p>30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel;</p> <p>31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas</p>		
--	--	--	--	--



		<p>de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;</p> <p>32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel;</p> <p>33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;</p> <p>34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso;</p> <p>35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPsec e SSL com elementos externos;</p> <p>36. A solução deverá ser capaz de encaminhar 1.6 Gbps de tráfego encapsulado via VPN IPsec;</p> <p>37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES;</p> <p>38. A VPN IPsec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard);</p> <p>39. A VPN IPsec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;</p> <p>40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs;</p> <p>41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPsec;</p> <p>42. A solução deverá ser capaz de atuar como um cliente de VPN SSL;</p> <p>43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;</p> <p>44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL;</p> <p>45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN $\&$ ADVPN</p>		
--	--	--	--	--



		<p>ou tecnologia similar;</p> <p>46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;</p> <p>47. 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;</p> <p>48. 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;</p> <p>49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;</p> <p>50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;</p> <p>51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;</p> <p>52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;</p> <p>53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;</p> <p>54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com</p>		
--	--	--	--	--



		<p>configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;</p> <p>55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;</p> <p>56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;</p> <p>57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;</p> <p>58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;</p> <p>59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;</p> <p>60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;</p> <p>61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;</p> <p>62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio;</p> <p>63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;</p> <p>64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente</p>		
--	--	---	--	--



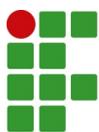
		<p>em 5GHz através do recurso conhecido como Band Steering;</p> <p>65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados;</p> <p>66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;</p> <p>67. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso;</p> <p>68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;</p> <p>69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;</p> <p>70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;</p> <p>71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;</p> <p>72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;</p> <p>73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor;</p> <p>74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:</p> <p>74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);</p> <p>74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication</p>		
--	--	---	--	--



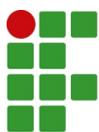
		<p>Flood, Broadcast Deauthentication e Spoofed Deauthentication;</p> <p>74.3. ASLEAP;</p> <p>74.4. Null Probe Response or Null SSID Probe Response;</p> <p>74.5. Long Duration;</p> <p>74.6. Ataques contra Wireless Bridges;</p> <p>74.7. Weak WEP;</p> <p>74.8. Invalid MAC OUI.</p> <p>75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;</p> <p>76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio;</p> <p>77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID;</p> <p>78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);</p> <p>79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;</p> <p>80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;</p> <p>81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;</p> <p>82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP;</p> <p>83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários;</p> <p>84. A solução deverá suportar Single-Sign-On (SSO);</p> <p>85. 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. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada;</p> <p>86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos</p>		
--	--	--	--	--



		<p>pelos servidores RADIUS;</p> <p>87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada;</p> <p>88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;</p> <p>89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;</p> <p>90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;</p> <p>91. A solução deve permitir a configuração do captive portal com endereço IPv6;</p> <p>92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;</p> <p>93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;</p> <p>94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;</p> <p>95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários;</p> <p>96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários;</p> <p>97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente;</p> <p>98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede;</p> <p>99. A solução deverá ser capaz de inspecionar 300 (trezentos) Mbps de tráfego SSL;</p>		
--	--	--	--	--



		<p>100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;</p> <p>101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários;</p> <p>102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar;</p> <p>103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados;</p> <p>104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;</p> <p>105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;</p> <p>106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento;</p> <p>107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos;</p> <p>108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS;</p> <p>109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig;</p> <p>110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6;</p> <p>111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso</p>		
--	--	---	--	--



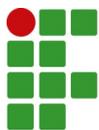
		<p>durante todo o período de garantia da solução;</p> <p>112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas;</p> <p>113. A solução deverá ser capaz de tratar 800 (oitocentos) Mbps de tráfego por meio do filtro de aplicações;</p> <p>114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede;</p> <p>115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações;</p> <p>116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução;</p> <p>117. A solução deverá permitir a criação manual de novos padrões de aplicações;</p> <p>118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;</p> <p>119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra;</p> <p>120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;</p> <p>121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede;</p> <p>122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;</p> <p>123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;</p> <p>124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;</p> <p>125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall;</p> <p>126. A solução deverá ser capaz de tratar 4.2 Gbps de tráfego por meio das regras de firewall stateful;</p>		
--	--	--	--	--



		<p>127. A solução deverá ser capaz de suportar 400.000 (quatrocentas mil) de sessões simultâneas/concorrentes e 28.000 (vinte e oito mil) novas sessões por segundo;</p> <p>128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos ↔ NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;</p> <p>129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura;</p> <p>130. A solução deverá suportar PBR ↔ Policy Based Routing;</p> <p>131. A solução deverá suportar roteamento multicast;</p> <p>132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar;</p> <p>133. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323;</p> <p>134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas;</p> <p>135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego;</p> <p>136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública;</p> <p>137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada;</p> <p>138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada;</p> <p>139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada;</p> <p>140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego;</p>		
--	--	---	--	--



		<p>141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada;</p> <p>142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec;</p> <p>143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo.</p> <p>144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link;</p> <p>145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover).</p> <p>146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6;</p> <p>147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso;</p> <p>148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados;</p> <p>149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica;</p> <p>150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes;</p> <p>151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados;</p> <p>152. A solução deverá suportar Netflow ou sFlow;</p> <p>153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6;</p> <p>154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS;</p> <p>155. A solução deve permitir o envio dos logs</p>		
--	--	--	--	--



			<p>para múltiplos servidores syslog externos; 156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 158. A solução deve possuir ferramentas de diagnósticos e debug 159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 161. A solução deve suportar comunicação com elementos externos através de REST API; 162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V o atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET</p>		
19	UNIDA DE	12.0	<p>SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 2 --> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 8 (oito) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam</p>	10.500,00	126.000,00



		<p>ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX;;</p> <p>4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação;</p> <p>5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas;</p> <p>6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;</p> <p>7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo;</p> <p>8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica;</p> <p>9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso;</p> <p>10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;</p> <p>11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados;</p> <p>12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 672 (seiscentos e setenta e duas) portas de switch ou um total de 14 (quatorze) switches;</p> <p>13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas;</p> <p>14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados;</p> <p>15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;</p> <p>16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;</p> <p>17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;</p>		
--	--	---	--	--



		<p>18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;</p> <p>19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;</p> <p>20. A solução 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;</p> <p>21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;</p> <p>22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;</p> <p>23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 30 (trinta) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor;</p> <p>24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;</p> <p>25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet;</p> <p>26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;</p> <p>27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6;</p> <p>28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;</p> <p>29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;</p> <p>30. A solução deve suportar a configuração de</p>		
--	--	--	--	--



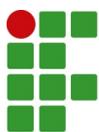
		<p>SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel;</p> <p>31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;</p> <p>32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel;</p> <p>33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;</p> <p>34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso;</p> <p>35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPsec e SSL com elementos externos;</p> <p>36. A solução deverá ser capaz de encaminhar 1.6 Gbps de tráfego encapsulado via VPN IPsec;</p> <p>37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES;</p> <p>38. A VPN IPsec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard);</p> <p>39. A VPN IPsec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;</p> <p>40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs;</p> <p>41. A solução deverá permitir a customização</p>		
--	--	--	--	--



		<p>da porta lógica utilizada pela VPN IPSec;</p> <p>42. A solução deverá ser capaz de atuar como um cliente de VPN SSL;</p> <p>43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;</p> <p>44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL;</p> <p>45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN ^{ou} ADVPN ou tecnologia similar;</p> <p>46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;</p> <p>47. 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;</p> <p>48. 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;</p> <p>49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;</p> <p>50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;</p> <p>51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;</p> <p>52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja,</p>		
--	--	---	--	--



		<p>com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;</p> <p>53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;</p> <p>54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;</p> <p>55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;</p> <p>56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;</p> <p>57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;</p> <p>58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;</p> <p>59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;</p> <p>60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;</p> <p>61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;</p> <p>62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio;</p> <p>63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está</p>		
--	--	--	--	--



		<p>conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;</p> <p>64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;</p> <p>65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados;</p> <p>66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;</p> <p>67. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso;</p> <p>68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;</p> <p>69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;</p> <p>70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;</p> <p>71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;</p> <p>72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;</p> <p>73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de</p>		
--	--	---	--	--



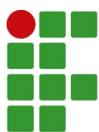
		<p>acesso do tipo indoor com pontos de acesso do tipo outdoor;</p> <p>74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:</p> <p>74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);</p> <p>74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;</p> <p>74.3. ASLEAP;</p> <p>74.4. Null Probe Response or Null SSID Probe Response;</p> <p>74.5. Long Duration;</p> <p>74.6. Ataques contra Wireless Bridges;</p> <p>74.7. Weak WEP;</p> <p>74.8. Invalid MAC OUI.</p> <p>75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;</p> <p>76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio;</p> <p>77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID;</p> <p>78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);</p> <p>79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;</p> <p>80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;</p> <p>81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;</p> <p>82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP;</p> <p>83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários;</p> <p>84. A solução deverá suportar Single-Sign-On (SSO);</p> <p>85. A solução deve implementar recurso de controle de acesso à rede (NAC - Network</p>		
--	--	---	--	--



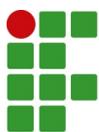
		<p>Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada;</p> <p>86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS;</p> <p>87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada;</p> <p>88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;</p> <p>89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;</p> <p>90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;</p> <p>91. A solução deve permitir a configuração do captive portal com endereço IPv6;</p> <p>92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;</p> <p>93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;</p> <p>94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;</p> <p>95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários;</p> <p>96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política</p>		
--	--	--	--	--



		<p>de controle de URL seja imposta aos usuários;</p> <p>97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente;</p> <p>98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede;</p> <p>99. A solução deverá ser capaz de inspecionar 600 (seiscentos) Mbps de tráfego SSL;</p> <p>100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;</p> <p>101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários;</p> <p>102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar;</p> <p>103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados;</p> <p>104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;</p> <p>105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;</p> <p>106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento;</p> <p>107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos;</p> <p>108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS;</p> <p>109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig;</p>		
--	--	---	--	--



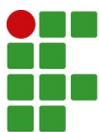
		<p>110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6;</p> <p>111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução;</p> <p>112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas;</p> <p>113. A solução deverá ser capaz de tratar 1.5 Gbps de tráfego por meio do filtro de aplicações;</p> <p>114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede;</p> <p>115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações;</p> <p>116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução;</p> <p>117. A solução deverá permitir a criação manual de novos padrões de aplicações;</p> <p>118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;</p> <p>119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra;</p> <p>120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;</p> <p>121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede;</p> <p>122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;</p> <p>123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam</p>		
--	--	---	--	--



		<p>utilizados como critério para permitir ou bloquear o tráfego;</p> <p>124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;</p> <p>125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall;</p> <p>126. A solução deverá ser capaz de tratar 6.2 Gbps de tráfego por meio das regras de firewall stateful;</p> <p>127. A solução deverá ser capaz de suportar 600.000 (seiscentas mil) de sessões simultâneas/concorrentes e 30.000 (trinta mil) novas sessões por segundo;</p> <p>128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos ↔ NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;</p> <p>129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura;</p> <p>130. A solução deverá suportar PBR ↔ Policy Based Routing;</p> <p>131. A solução deverá suportar roteamento multicast;</p> <p>132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar;</p> <p>133. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323;</p> <p>134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas;</p> <p>135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego;</p> <p>136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública;</p> <p>137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada;</p> <p>138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada;</p> <p>139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam</p>		
--	--	--	--	--



		<p>elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada;</p> <p>140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego;</p> <p>141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada;</p> <p>142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec;</p> <p>143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo.</p> <p>144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link;</p> <p>145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover).</p> <p>146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6;</p> <p>147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso;</p> <p>148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados;</p> <p>149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica;</p> <p>150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes;</p> <p>151. A solução deve recomendar versões de</p>		
--	--	---	--	--



			<p>firmware a ser instalado nos switches e pontos de acesso por ela gerenciados;</p> <p>152. A solução deverá suportar Netflow ou sFlow;</p> <p>153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6;</p> <p>154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS;</p> <p>155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;</p> <p>156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;</p> <p>157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap;</p> <p>158. A solução deve possuir ferramentas de diagnósticos e debug</p> <p>159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha;</p> <p>160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários;</p> <p>161. A solução deve suportar comunicação com elementos externos através de REST API;</p> <p>162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo;</p> <p>163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;</p> <p>164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET</p>		
20	UNIDA DE	6.0	<p>SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 3 --></p> <p>Características Mínimas:</p> <p>1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus;</p>	19.000,00	114.000,00



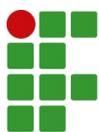
		<p>2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante;</p> <p>3. Cada appliance físico deve possuir, pelo menos, 10 (dez) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX;</p> <p>4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação;</p> <p>5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas;</p> <p>6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;</p> <p>7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo;</p> <p>8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica;</p> <p>9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso;</p> <p>10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;</p> <p>11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados;</p> <p>12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 672 (seiscentos e setenta e duas) portas de switch ou um total de 14 (quatorze) switches;</p> <p>13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas;</p> <p>14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados;</p>		
--	--	---	--	--



		<p>15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;</p> <p>16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;</p> <p>17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;</p> <p>18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;</p> <p>19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;</p> <p>20. A solução 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;</p> <p>21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;</p> <p>22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;</p> <p>23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 40 (quarenta) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor;</p> <p>24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;</p> <p>25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet;</p> <p>26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;</p> <p>27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6;</p> <p>28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando</p>		
--	--	--	--	--



		<p>automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;</p> <p>29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;</p> <p>30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel;</p> <p>31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;</p> <p>32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel;</p> <p>33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;</p> <p>34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso;</p> <p>35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos;</p> <p>36. A solução deverá ser capaz de encaminhar 3.2 Gbps de tráfego encapsulado via VPN;</p> <p>37. A solução deverá suportar os algoritmos de</p>		
--	--	---	--	--



		<p>criptografia para túneis VPN: AES, DES, 3DES;</p> <p>38. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard);</p> <p>39. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;</p> <p>40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs;</p> <p>41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSEc;</p> <p>42. A solução deverá ser capaz de atuar como um cliente de VPN SSL;</p> <p>43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;</p> <p>44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL;</p> <p>45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN ou tecnologia similar;</p> <p>46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;</p> <p>47. 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;</p> <p>48. 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;</p> <p>49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;</p> <p>50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;</p> <p>51. A solução deve identificar automaticamente pontos de acesso intrusos</p>		
--	--	--	--	--



		<p>que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;</p> <p>52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;</p> <p>53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;</p> <p>54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;</p> <p>55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;</p> <p>56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;</p> <p>57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;</p> <p>58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;</p> <p>59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;</p> <p>60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;</p> <p>61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;</p> <p>62. A solução deve implementar técnicas de Call Admission Control para limitar o número</p>		
--	--	--	--	--



		<p>de chamadas simultâneas na rede sem fio;</p> <p>63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;</p> <p>64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;</p> <p>65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados;</p> <p>66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;</p> <p>67. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso;</p> <p>68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;</p> <p>69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;</p> <p>70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;</p> <p>71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;</p> <p>72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar</p>		
--	--	---	--	--



		<p>serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;</p> <p>73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor;</p> <p>3.74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:</p> <p>74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);</p> <p>74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;</p> <p>74.3. ASLEAP;</p> <p>74.4. Null Probe Response or Null SSID Probe Response;</p> <p>74.5. Long Duration;</p> <p>74.6. Ataques contra Wireless Bridges;</p> <p>74.7. Weak WEP;</p> <p>74.8. Invalid MAC OUI.</p> <p>75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;</p> <p>76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio;</p> <p>77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID;</p> <p>78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);</p> <p>79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;</p> <p>80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;</p> <p>81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;</p> <p>82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos</p>		
--	--	--	--	--



		<p>de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP;</p> <p>83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários;</p> <p>84. A solução deverá suportar Single-Sign-On (SSO);</p> <p>85. 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. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada;</p> <p>86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS;</p> <p>87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada;</p> <p>88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;</p> <p>89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;</p> <p>90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;</p> <p>91. A solução deve permitir a configuração do captive portal com endereço IPv6;</p> <p>92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;</p> <p>93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;</p> <p>94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;</p> <p>95. A solução deve implementar recurso para controle de URLs acessadas na rede através de</p>		
--	--	---	--	--



		<p>análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários;</p> <p>96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários;</p> <p>97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente;</p> <p>98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede;</p> <p>99. A solução deverá ser capaz de inspecionar 700 (setecentos) Mbps de tráfego SSL;</p> <p>100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;</p> <p>101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários;</p> <p>102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar;</p> <p>103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados;</p> <p>104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;</p> <p>105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;</p> <p>106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento;</p> <p>107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos;</p> <p>108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS;</p>		
--	--	---	--	--



		<p>109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig;</p> <p>110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6;</p> <p>111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução;</p> <p>112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas;</p> <p>113. A solução deverá ser capaz de tratar 1.5 Gbps de tráfego por meio do filtro de aplicações;</p> <p>114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede;</p> <p>115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações;</p> <p>116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução;</p> <p>117. A solução deverá permitir a criação manual de novos padrões de aplicações;</p> <p>118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;</p> <p>119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra;</p> <p>120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;</p> <p>121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede;</p> <p>122. A solução deve ser capaz de implementar</p>		
--	--	--	--	--



		<p>regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;</p> <p>123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;</p> <p>124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;</p> <p>125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall;</p> <p>126. A solução deverá ser capaz de tratar 9 (nove) Gbps de tráfego por meio das regras de firewall stateful;</p> <p>127. A solução deverá ser capaz de suportar 1.400.000 (um milhão e quatrocentas mil) de sessões simultâneas/concorrentes e 40.000 (quarenta mil) novas sessões por segundo;</p> <p>128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos ↔ NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;</p> <p>129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura;</p> <p>130. A solução deverá suportar PBR ↔ Policy Based Routing;</p> <p>131. A solução deverá suportar roteamento multicast;</p> <p>132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar;</p> <p>133. A solução deverá possuir mecanismo de tratamento para aplicações multimedial (session-helpers ou ALGs) tipo SIP e H323;</p> <p>134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas;</p> <p>135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego;</p> <p>136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública;</p>		
--	--	--	--	--



		<p>137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada;</p> <p>138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada;</p> <p>139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada;</p> <p>140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego;</p> <p>141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada;</p> <p>142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec;</p> <p>143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo.</p> <p>144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link;</p> <p>145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover).</p> <p>146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6;</p> <p>147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso;</p> <p>148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados;</p> <p>149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por</p>		
--	--	--	--	--



		<p>ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica;</p> <p>150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes;</p> <p>151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados;</p> <p>152. A solução deverá suportar Netflow ou sFlow;</p> <p>153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6;</p> <p>154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS;</p> <p>155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;</p> <p>156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;</p> <p>157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap;</p> <p>158. A solução deve possuir ferramentas de diagnósticos e debug</p> <p>159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha;</p> <p>160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários;</p> <p>161. A solução deve suportar comunicação com elementos externos através de REST API;</p> <p>162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo;</p> <p>163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;</p> <p>164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V o atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET</p>		
--	--	--	--	--



21	UNIDA DE	6.0	<p>SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 4 --> Características Mínimas:</p> <ol style="list-style-type: none">1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus;2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante;3. Cada appliance físico deve possuir, pelo menos, 2 (duas) interfaces 1000Base-T e 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede;4. Cada appliance físico deve possuir fontes de alimentações redundantes com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar os cabos de alimentação;5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas;6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo;8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica;9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso;10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados;12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 1440 (um mil, quatrocentas e quarenta) portas de switch ou um total de 30 (trinta) switches;13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente	45.600,00	273.600,00
----	-------------	-----	---	-----------	------------



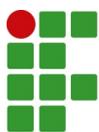
		<p>status dos uplinks para identificação de eventuais problemas;</p> <p>14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados;</p> <p>15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;</p> <p>16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;</p> <p>17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;</p> <p>18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;</p> <p>19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;</p> <p>20. A solução 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;</p> <p>21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;</p> <p>22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;</p> <p>23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 60 (sessenta) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor;</p> <p>24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;</p> <p>25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet;</p> <p>26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;</p>		
--	--	---	--	--



		<p>27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6;</p> <p>28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;</p> <p>29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;</p> <p>30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel;</p> <p>31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;</p> <p>32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel;</p> <p>33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;</p> <p>34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso;</p>		
--	--	--	--	--



		<p>35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos;</p> <p>36. A solução deverá ser capaz de encaminhar 3.2 Gbps de tráfego encapsulado via VPN;</p> <p>37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES;</p> <p>38. A VPN IPSec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard);</p> <p>39. A VPN IPSec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;</p> <p>40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs;</p> <p>41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec;</p> <p>42. A solução deverá ser capaz de atuar como um cliente de VPN SSL;</p> <p>43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;</p> <p>44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL;</p> <p>45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN ou ADVPN ou tecnologia similar;</p> <p>46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;</p> <p>47. 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;</p> <p>48. 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;</p> <p>49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;</p> <p>50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como:</p>		
--	--	---	--	--



		<p>intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;</p> <p>51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;</p> <p>52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;</p> <p>53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;</p> <p>54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;</p> <p>55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;</p> <p>56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;</p> <p>57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;</p> <p>58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;</p> <p>59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;</p> <p>60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;</p>		
--	--	---	--	--



		<p>61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;</p> <p>62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio;</p> <p>63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;</p> <p>64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;</p> <p>65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados;</p> <p>66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;</p> <p>67. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso;</p> <p>68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;</p> <p>69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;</p> <p>70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;</p> <p>71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando</p>		
--	--	--	--	--



		<p>for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;</p> <p>72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;</p> <p>73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor;</p> <p>74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:</p> <p>74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);</p> <p>74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;</p> <p>74.3. ASLEAP;</p> <p>74.4. Null Probe Response or Null SSID Probe Response;</p> <p>74.5. Long Duration;</p> <p>74.6. Ataques contra Wireless Bridges;</p> <p>74.7. Weak WEP;</p> <p>74.8. Invalid MAC OUI.</p> <p>75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;</p> <p>76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio;</p> <p>77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID;</p> <p>78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);</p> <p>79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;</p> <p>80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;</p>		
--	--	--	--	--



		<p>81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;</p> <p>82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP;</p> <p>83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários;</p> <p>84. A solução deverá suportar Single-Sign-On (SSO);</p> <p>85. 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. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada;</p> <p>86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS;</p> <p>87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada;</p> <p>88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;</p> <p>89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;</p> <p>90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;</p> <p>91. A solução deve permitir a configuração do captive portal com endereço IPv6;</p> <p>92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;</p> <p>93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de</p>		
--	--	---	--	--



		<p>administração da solução;</p> <p>94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;</p> <p>95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários;</p> <p>96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários;</p> <p>97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente;</p> <p>98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede;</p> <p>99. A solução deverá ser capaz de inspecionar 900 (novecentos) Mbps de tráfego SSL;</p> <p>100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;</p> <p>101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários;</p> <p>102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar;</p> <p>103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados;</p> <p>104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;</p> <p>105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;</p> <p>106. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento;</p> <p>107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos</p>		
--	--	---	--	--



		<p>websites/domínios para cada categoria e também para websites/domínios específicos;</p> <p>108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS;</p> <p>109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig;</p> <p>110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6;</p> <p>111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução;</p> <p>112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas;</p> <p>113. A solução deverá ser capaz de tratar 2 (dois) Gbps de tráfego por meio do filtro de aplicações;</p> <p>114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede;</p> <p>115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações;</p> <p>116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução;</p> <p>117. A solução deverá permitir a criação manual de novos padrões de aplicações;</p> <p>118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;</p> <p>119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra;</p> <p>120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao</p>		
--	--	--	--	--



		<p>negócio e permitir a priorização deste tráfego com marcação QoS;</p> <p>121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede;</p> <p>122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;</p> <p>123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;</p> <p>124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;</p> <p>125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall;</p> <p>126. A solução deverá ser capaz de tratar 16 (dezesseis) Gbps de tráfego por meio das regras de firewall stateful;</p> <p>127. A solução deverá ser capaz de suportar 1.400.000 (um milhão e quatrocentas mil) de sessões simultâneas/concorrentes e 50.000 (cinquenta mil) novas sessões por segundo;</p> <p>128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos ↔ NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;</p> <p>129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura;</p> <p>130. A solução deverá suportar PBR ↔ Policy Based Routing;</p> <p>131. A solução deverá suportar roteamento multicast;</p> <p>132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar;</p> <p>133. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323;</p> <p>134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas;</p> <p>135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual</p>		
--	--	--	--	--



		<p>interno ao(s) elemento(s) de filtragem de tráfego;</p> <p>136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública;</p> <p>137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada;</p> <p>138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada;</p> <p>139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada;</p> <p>140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego;</p> <p>141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada;</p> <p>142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec;</p> <p>143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo.</p> <p>144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link;</p> <p>145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover).</p> <p>146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6;</p> <p>147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso;</p> <p>148. A solução deve possuir recurso para</p>		
--	--	---	--	--



		<p>realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados;</p> <p>149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica;</p> <p>150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes;</p> <p>151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados;</p> <p>152. A solução deverá suportar Netflow ou sFlow;</p> <p>153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6;</p> <p>154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS;</p> <p>155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;</p> <p>156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;</p> <p>157. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap;</p> <p>158. A solução deve possuir ferramentas de diagnósticos e debug</p> <p>159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha;</p> <p>160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários;</p> <p>161. A solução deve suportar comunicação com elementos externos através de REST API;</p> <p>162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo;</p> <p>163. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;</p> <p>164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de</p>		
--	--	---	--	--



			desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET		
22	UNIDA DE	1.0	SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA PARA CAMPUS TIPO 5 --> Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 4 (quatro) interfaces 1000Base-T e 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X ou superior para permitir a conexão com a rede; 4. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 5. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 6. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 7. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 8. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 9. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 10. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 11. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados;	126.000,0 0	126.000,00



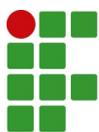
		<p>12. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 3360 (três mil, trezentos e sessenta) portas de switch ou um total de 70 (setenta) switches;</p> <p>13. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas;</p> <p>14. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados;</p> <p>15. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;</p> <p>16. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;</p> <p>17. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;</p> <p>18. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;</p> <p>19. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;</p> <p>20. A solução 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;</p> <p>21. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;</p> <p>22. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;</p> <p>23. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 500 (quinhentos) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor;</p> <p>24. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;</p> <p>25. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou</p>		
--	--	---	--	--



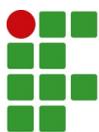
		<p>remotamente através de links WAN e Internet;</p> <p>26. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;</p> <p>27. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6;</p> <p>28. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;</p> <p>29. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;</p> <p>30. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel;</p> <p>31. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;</p> <p>32. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel;</p> <p>33. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo</p>		
--	--	---	--	--



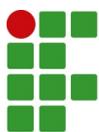
		<p>quando o SSID estiver configurado com autenticação 802.1X;</p> <p>34. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso;</p> <p>35. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPsec e SSL com elementos externos;</p> <p>36. A A solução deverá ser capaz de encaminhar 9 (nove) Gbps de tráfego encapsulado via VPN IPsec;</p> <p>37. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES;</p> <p>38. A VPN IPsec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard);</p> <p>39. A VPN IPsec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;</p> <p>40. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs;</p> <p>41. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPsec;</p> <p>42. A solução deverá ser capaz de atuar como um cliente de VPN SSL;</p> <p>43. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;</p> <p>44. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL;</p> <p>45. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN ↔ ADVPN ou tecnologia similar;</p> <p>46. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;</p> <p>47. 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;</p> <p>48. 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;</p> <p>49. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção</p>		
--	--	---	--	--



		<p>humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;</p> <p>50. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;</p> <p>51. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;</p> <p>52. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;</p> <p>53. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;</p> <p>54. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;</p> <p>55. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;</p> <p>56. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;</p> <p>57. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;</p> <p>58. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;</p> <p>59. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as</p>		
--	--	---	--	--



		<p>decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;</p> <p>60. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;</p> <p>61. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;</p> <p>62. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio;</p> <p>63. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;</p> <p>64. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;</p> <p>65. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados;</p> <p>66. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;</p> <p>67. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso;</p> <p>68. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;</p> <p>69. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os</p>		
--	--	--	--	--



		<p>clientes sejam desconectados;</p> <p>70. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;</p> <p>71. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;</p> <p>72. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;</p> <p>73. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor;</p> <p>74. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:</p> <p>74.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding);</p> <p>74.2. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication;</p> <p>74.3. ASLEAP;</p> <p>74.4. Null Probe Response or Null SSID Probe Response;</p> <p>74.5. Long Duration;</p> <p>74.6. Ataques contra Wireless Bridges;</p> <p>74.7. Weak WEP;</p> <p>74.8. Invalid MAC OUI.</p> <p>75. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;</p> <p>76. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio;</p> <p>77. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID;</p> <p>78. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes</p>		
--	--	---	--	--



		<p>métodos de autenticação: WPA (TKIP) e WPA2 (AES);</p> <p>79. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;</p> <p>80. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;</p> <p>81. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;</p> <p>82. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP;</p> <p>83. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários;</p> <p>84. A solução deverá suportar Single-Sign-On (SSO);</p> <p>85. 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. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada;</p> <p>86. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS;</p> <p>87. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada;</p> <p>88. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;</p> <p>89. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;</p> <p>90. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;</p> <p>91. A solução deve permitir a configuração do captive portal com endereço IPv6;</p>		
--	--	--	--	--



		<p>92. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;</p> <p>93. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;</p> <p>94. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;</p> <p>95. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários;</p> <p>96. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários;</p> <p>97. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente;</p> <p>98. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede;</p> <p>99. A solução deverá ser capaz de inspecionar 4.5 Gbps de tráfego SSL;</p> <p>100. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;</p> <p>101. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários;</p> <p>102. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo Continuar;</p> <p>103. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados;</p> <p>104. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;</p> <p>105. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;</p> <p>106. A solução deve implementar solução de</p>		
--	--	---	--	--



		<p>segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento;</p> <p>107. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos;</p> <p>108. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS;</p> <p>109. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig;</p> <p>110. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6;</p> <p>111. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução;</p> <p>112. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas;</p> <p>113. A solução deverá ser capaz de tratar 14 (quatorze) Gbps de tráfego por meio do filtro de aplicações;</p> <p>114. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede;</p> <p>115. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações;</p> <p>116. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução;</p> <p>117. A solução deverá permitir a criação manual de novos padrões de aplicações;</p> <p>118. A solução deve permitir a criação de regras para bloqueio e limite de banda (em</p>		
--	--	--	--	--



		<p>Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;</p> <p>119. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra;</p> <p>120. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;</p> <p>121. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede;</p> <p>122. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;</p> <p>123. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;</p> <p>124. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC;</p> <p>125. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall;</p> <p>126. A solução deverá ser capaz de tratar 35 (trinta e cinco) Gbps de tráfego por meio das regras de firewall stateful;</p> <p>127. A solução deverá ser capaz de suportar 7.000.000 (sete milhões) de sessões simultâneas/concorrentes e 400.000 (quatrocentas mil) novas sessões por segundo;</p> <p>128. A solução deverá possuir a funcionalidade de tradução de endereços estáticos ↔ NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT;</p> <p>129. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura;</p> <p>130. A solução deverá suportar PBR ↔ Policy Based Routing;</p> <p>131. A solução deverá suportar roteamento multicast;</p> <p>132. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar;</p> <p>133. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323;</p>		
--	--	--	--	--



		<p>134. A solução deverá possuir suporte a criação de, no mínimo, 03 (três) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas;</p> <p>135. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego;</p> <p>136. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública;</p> <p>137. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada;</p> <p>138. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada;</p> <p>139. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada;</p> <p>140. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego;</p> <p>141. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada;</p> <p>142. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec;</p> <p>143. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo.</p> <p>144. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link;</p> <p>145. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP</p>		
--	--	--	--	--



		<p>de origem e destino e/ou transbordo de link (Spillover).</p> <p>146. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6;</p> <p>147. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso;</p> <p>148. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados;</p> <p>149. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica;</p> <p>150. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes;</p> <p>151. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados;</p> <p>152. A solução deverá suportar Netflow ou sFlow;</p> <p>153. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6;</p> <p>154. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS;</p> <p>155. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;</p> <p>156. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;</p> <p>157. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap;</p> <p>158. A solução deve possuir ferramentas de diagnósticos e debug</p> <p>159. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha;</p> <p>160. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários;</p> <p>161. A solução deve suportar comunicação com elementos externos através de REST API;</p> <p>162. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo;</p> <p>163. Garantia de 36 (trinta e seis) meses com</p>		
--	--	---	--	--



		suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V <i>o</i> atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). Marca: FORTINET Fabricante: FORTINET		
Total				R\$ 3.525.680, 00

VALOR TOTAL DA ATA	R\$ 3.685.680,00
---------------------------	-----------------------------------