((TÍTULO))((NG))**ATA DA CONSULTA PÚBLICA Nº 002/2022**

((TEXTO)) ((NG)) **ATA DE REGISTRO DE PREÇOS PARA FUTURA E EVENTUAL PRESTAÇÃO DE SERVIÇO PARA FORNECIMENTO DE EQUIPAMENTOS DE REDE WIRELESS, COM SUPORTE, MANUTENÇÃO E SOLUÇÃO DE GERENCIAMENTO.** ((CL))

(PERGUNTAS E RESPOSTAS)

No dia quinze do mês de julho de dois mil e vinte e dois, a Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo – PRODAM-SP torna públicas as respostas aos questionamentos e sugestões apresentados pelas empresas abaixo, na Consulta Pública referenciada:

Empresa: ((NG)) **"9 NET"**((CL))

PERGUNTA: Agradecemos a convocação e propomos a divisão em lotes com quantidades menores para ampliar a participação de empresas no processo. A elevada quantidade de AP's exigida nos atestados impede nossa participação.

RESPOSTA: Entendemos que a divisão em lotes seria prejudicial para a distribuição das mesmas redes Wireless em diversos ambientes, de diversas secretarias, limitando a integração.

Empresa: ((NG))**"IT ONE"**((CL))

PERGUNTA: Para conseguirmos atender tecnicamente ao solicitado e participarmos deste projeto, solicitamos os esclarecimentos dos pontos abaixo:

Item 1 – Access Point Indoor 802.11 a/g/n/ac/ax nas frequências de 2.4GHz e 5GHz

Sobre o item 6.3.3.5. Entendemos que, como esta arquitetura causa impacto negativo no desempenho da rede, sem grandes ganhos na segurança e monitoramento do tráfego, visto que a solução solicita tunelamento e criptografia de dados além da possibilidade de DPI, entendemos que será facultado o atendimento deste item, ao menos no que tange o tráfego centralizado na controladora e/ou gerenciamento.

Está correto nosso entendimento?

RESPOSTA: O entendimento está incorreto. A rede PRODAM é baseada atualmente em redes MPLS com internet centralizada e estamos caminhando para uma rede SD-WAN com links de internet locais, assim, necessitamos que enquanto não temos essa nova rede necessitamos de redes tuneladas para o pleno funcionamento, sem transportes de VLAN e demais configurações pela rede.

PERGUNTA: Sobre o item 6.3.10 “Opções de Antena”, subitens 6.3.10.1 e 6.3.10.2. Entendemos que, para viabilizar a participação de grandes fabricantes de WLAN do mercado internacional, líderes do Gartner Group na área de rede com e sem fio, além de aumentar a competitividade do certame, será aceito equipamento que possua 2.6 dBi em 2.4GHz e 3.7 dBi em 5 GHz, desde que ele atenda as demais exigências do termo de referência.

Está correto nosso entendimento?

RESPOSTA: Iremos rever o dimensionamento de antenas. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: Item 2 - Access Point Indoor 802.11 a/g/n/ac/ax nas frequências de 2.4GHz e 5GHz

Sobre o item 6.4.4.5. Entendemos que, como esta arquitetura causa impacto negativo no desempenho da rede, sem grandes ganhos na segurança e monitoramento do tráfego, visto que a solução solicita tunelamento e criptografia de dados além da possibilidade de DPI,

entendemos que será facultado o atendimento deste item, ao menos no que tange o tráfego centralizado na controladora e/ou gerenciamento.

Está correto nosso entendimento?

RESPOSTA: O entendimento está incorreto. A rede PRODAM é baseada atualmente em redes MPLS com internet centralizada e estamos caminhando para uma rede SD-WAN com links de internet locais, assim, necessitamos que enquanto não temos essa nova rede necessitamos de redes tuneladas para o pleno funcionamento, sem transportes de VLAN e demais configurações pela rede.

PERGUNTA: Sobre o item 6.4.11 "Opção de Antena", subitens 6.4.11.1 e 6.4.11.2. Entendemos que, para viabilizar a participação de grandes fabricantes de WLAN do mercado internacional, líderes do Gartner Group na área de rede com e sem fio, além de aumentar a competitividade do certame, será aceito equipamento que possua 4.0 dBi em 2.4GHz e 4.7 dBi em 5 GHz, desde que ele atenda as demais exigências do termo de referência.

Está correto nosso entendimento?

RESPOSTA: Iremos rever o dimensionamento de antenas. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: Item 3 - Access Point Indoor 802.11 a/g/n/ac/ax nas frequências de 2.4GHz e 5GHz

Sobre o item 6.5.3.4. Visto que APs 8X8:8SS são mais caros e necessitam de mais energia, além de apenas serem úteis quando o dispositivo final dá suporte à 8x8:8 e MU-MIMO 802.11ax - levando em conta que a grande parte dos dispositivos finais são 2x2:2ss e no futuro alguns serão 4x4:4ss -, fica evidente que não há vantagem prática para a exigência de rádios 8x8:8ss, mesmo que a tecnologia suporte este limite. Por isso, visando um melhor posicionamento do certame e um investimento ainda a prova de futuro, utilizando de forma eficiente a tecnologia OFDMA, serão aceitos

access points que suportem 4x4:4ss em 2.4GHz e 4x4:4ss em 5GHz, desde que possa ser selecionado através de software a operação em dual 5GHz.

Está correto nosso entendimento?

RESPOSTA: Entendemos que, apesar de ser um access point específico, temos demanda para tal tipo de equipamento. A quantidade de equipamentos é baixa, são apenas 16 equipamentos. Será mantido.

PERGUNTA: Sobre o item 6.5.3.6. Entendemos que, apesar da tecnologia 802.11ax suportar uma associação teórica de 2048 clientes, esta não reflete em divisões de banda com geração de tráfego, sendo fisicamente impossível que a banda permita que 2048 clientes estejam trafegando de forma satisfatória em apenas 1 ponto de acesso. Logo, entendemos que será aceito ponto de acesso que suporte 1024 clientes associados constando em documentação, a não ser que possa ser comprovada através de PoC a associação dos 2048 clientes num único ponto de acesso, no ambiente do contratante, sem prejudicar a operação do hardware do equipamento.

Está correto nosso entendimento?

RESPOSTA: Iremos rever a quantidade de clientes associados.

PERGUNTA: Sobre o item 6.5.3.6. Entendemos que, como esta arquitetura causa impacto negativo no desempenho da rede, sem grandes ganhos na segurança e monitoramento do tráfego, visto que a solução solicita tunelamento e criptografia de dados além da possibilidade de DPI, entendemos que será facultado o atendimento deste item, ao menos no que tange o tráfego centralizado na controladora e/ou gerenciamento.

Está correto nosso entendimento?

RESPOSTA: O entendimento está incorreto. A rede PRODAM é baseada atualmente em redes MPLS com internet centralizada e estamos caminhando para uma rede SD-WAN com links de internet locais, assim, necessitamos que enquanto não temos essa nova rede necessitamos de redes tuneladas para o pleno funcionamento, sem transportes de VLAN e demais configurações pela rede.

PERGUNTA: Sobre o item 6.5.10 “Opção de Antena”, subitens 6.5.10.1 e 6.5.10.2. Entendemos que, para viabilizar a participação de grandes fabricantes de WLAN do mercado internacional, líderes do Gartner Group na área de rede com e sem fio, além de aumentar a competitividade do certame, será aceito equipamento que possua 4.6 dBi em 2.4GHz e 5.7 dBi em 5 GHz, desde que ele atenda as demais exigências do termo de referência.

Está correto nosso entendimento?

RESPOSTA: Iremos rever o dimensionamento de antenas. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

Empresa: ((NG)) **“LETTEL”**((CL))

PERGUNTA: Bom dia, temos interesse em participar do processo, porém a solução exigida está acima do nosso portfólio WLAN homologado na Anatel para esse semestre. Em anexo envio uma análise de toda a especificação técnica contendo os comentários e alterações necessários para nossa participação e os datasheets da solução ofertada. Ficamos a disposição para maiores detalhes.

A Anatel homologou o novo modelo 8x8 da Alcatel-Lucent e conseguimos participar do processo de forma competitiva realizando pequenos ajustes. Segue análise e Datasheet.

Sugestões da tabela enviada:

6.3.7.1. Implemetar gerencia criptografada com a controladora e coleta SNMP v2c/v3, inclusive com TRAP SNMP.

RESPOSTA: Entendemos que a especificação atual é mais abrangente e permite a participação de mais empresas.

PERGUNTA: 6.4.8.1. Implemetar gerencia criptografada com a controladora e coleta SNMP v2c/v3, inclusive com TRAP SNMP.

RESPOSTA: Entendemos que a especificação atual é mais abrangente e permite a participação de mais empresas.

PERGUNTA: 6.4.11.1. Mínimo antena omnidirecional interna ou externa de, no mínimo, 06 dBi para a frequência de 2,4GHz.

RESPOSTA: Iremos rever o dimensionamento de antenas. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA:6.4.11.2. Mínimo antena omnidirecional interna ou externa de, no mínimo, 06 dBi para a frequência de 5GHz.

RESPOSTA: Iremos rever o dimensionamento de antenas. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: 6.5.3.6. Suportar 1536 usuários simultâneos.

RESPOSTA: Iremos rever a quantidade de clientes associados.

PERGUNTA: 6.5.7.1. Implemetar gerencia criptografada com a controladora e coleta SNMP v2c/v3, inclusive com TRAP SNMP.

RESPOSTA: Entendemos que a especificação atual é mais abrangente e permite a participação de mais empresas.

PERGUNTA:6.5.10.1. Mínimo antena omnidirecional interna ou externa de, no mínimo, 3.9 dBi para a frequência de 2,4GHz.

RESPOSTA: Iremos rever o dimensionamento de antenas. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA:6.5.10.2. Mínimo antena omnidirecional interna ou externa de, no mínimo, 3.9 dBi para a frequência de 5GHz.

RESPOSTA: Iremos rever o dimensionamento de antenas. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: 6.5.11.1. No mínimo 02 (duas) portas Ethernet (1000/2500/5000Base-T – 802.3z e 802.3bz) autosense.*Atendemos com 2x portas 1/2.5/5/10G-BaseT

RESPOSTA: Entendemos que a especificação atual é mais abrangente e permite a participação de mais empresas.

PERGUNTA: 6.5.11.3. EIRP: O conjunto rádio com antenas deve proporcionar nível de sinal no mínimo 21dBm para todas modulações exigidas neste termo de referência.

RESPOSTA: Iremos rever o dimensionamento de potência. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

Empresa: ((NG)) **"TELESUL"**((CL))

PERGUNTA: Prezados Senhores, bom dia. Com o intuito de melhor atender ao processo, solicitamos gentilmente, que a data para o envio de nossos questionamentos/solicitação de esclarecimentos, seja adiada até 23/06/2022.

RESPOSTA: Recepcionamos o documento enviado dia 23/06/2022.

PERGUNTA: 1-Visto a dimensão do objeto em contratação, onde constam mais de 13 mil Access Points, serviços de alta disponibilidade, atendimento especializado, entendemos que os participantes, possuam nível máximo de certificação junto aos fabricantes ao quais representam. Está correto o entendimento?

RESPOSTA: Iremos rever o mínimo de certificação para esta ARP, entendemos que não ter nenhum nível de certificação é ruim e que todos

os fabricantes possuem esse modelo de relacionamento com as integradoras, de forma a qualificar as melhores/maiores.

PERGUNTA:2-Afim de garantir a execução do contrato de serviço, que contempla mais de 13 mil Access Points, entendemos que para finalidade de certificado de capacidade técnica, o proponente deve comprovar ter executado projetos com pelo menos 25% da quantidade total do objeto.

RESPOSTA: Por ser um serviço, entendemos que a divisão em lotes seria prejudicial para a distribuição das mesmas redes Wireless em diversos ambientes, de diversas secretarias, limitando a integração, assim necessitamos que a empresa integradora tenha capacidade de atender esta demanda e tenha esse tipo de comprovação no mercado. Iremos rever este quantitativo.

PERGUNTA:3-Entendemos que o termo de referência atende os principais fabricantes de mercado, como Cisco Meraki, Aruba Networks e Ruckus, mas também está aberto a possibilidade para fabricantes de segmentos inferiores, de baixo custo, visto a flexibilidade colocada referente aos softwares de gerênciamento e controlador wireless, podendo ser físico, virtual, hibrido, etc. Para equilibrar o participante a nível de atuação de mercado e custo, solicitamos a exigência de redes tuneladas conectadas a appliances físicos.

RESPOSTA: A rede PRODAM é baseada atualmente em redes MPLS com internet centralizada e estamos caminhando para uma rede SD-WAN com links de internet locais, assim, necessitamos que enquanto não temos essa nova rede necessitamos de redes tuneladas para o pleno funcionamento, sem transportes de VLAN e demais configurações pela rede. Desta forma, entendemos que cada fabricante pode entregar o tunelamento de redes da forma que achar melhor.

Empresa: ((NG)) **“SEGER”**((CL))

PERGUNTA: Solicitações as seguintes alterações no EDITAL DE CONSULTA PÚBLICA Nº 002/2022:

Item 6.8.7. Para os demais contratos, advindos da adesão à Ata de Registro de Preços, o prazo de entrega dos equipamentos constantes no itens 6.3, 6.4, 6.5 e 6.6 deste Termo de referência, será de até 45 dias corridos.

Devido à crise mundial refere a fabricação de semicondutores, ocorre a falta de insumos no mercado atrasando a fabricação de equipamentos, sendo assim requeremos que o prazo de entrega seja estendido para em até 180 (cento e oitenta) dias.

RESPOSTA: Entendemos o agravamento de fornecimento de equipamentos devido a falta de semicondutores, devido a guerra e pandemia. Iremos ampliar o prazo de entrega, mas não podemos para o prazo solicitado, pois entendemos como muito elástico.

PERGUNTA: Item 6.3.3.3. Caso seja utilizado trunk por rádio, este deve operar em frequências distintas às do tráfego de dados da rede.

Solicitamos a retirada deste item.

RESPOSTA: Entendemos que a retirada deste item inviabiliza a implantação da tecnologia mesh de forma satisfatória.

PERGUNTA: Item 6.3.5.3. AES, TKIP, 802.1X - EAP-MD5. EAP-FAST (Flexible Authentication via Secure Tunneling). EAP-GTC (EAP – Generic Token Card). PEAPMSCHAPv2 (PEAP – Microsoft Challenge Authentication Protocol Version 2). EAP-TLS (EAP – Transport Layer Security).

Solicitamos a alteração do item: 6.3.5.3. AES, TKIP, 802.1X - EAP-MD5. PEAPMSCHAPv2 (PEAP – Microsoft Challenge Authentication Protocol Version 2). EAP-TLS (EAP – Transport Layer Security).

RESPOSTA: Manteremos os protocolos de autenticação, todos são populares e utilizados.

PERGUNTA: Item 6.3.6.3. Seleção de endereço padrão (RFC3484).

Solicitamos a retirada deste item.

RESPOSTA: Manteremos, pois seguimos os requisitos básicos de IPv6 do ipv6.br, descritos no documento RIPE 554 https://ipv6.br/download/requisitos-suporte-ipv6-ripe-554-pt.pdf segundo o guia para compras ou licitações de equipamentos com suporte a IPv6 https://ipv6.br/post/guia-para-compras-ou-licitacoes-de-equipamentos-com-suporte-a-ipv6/

PERGUNTA: Item 6.3.8.2. Implementação de Class of Service (CoS) segundo o padrão IEEE 802.1p.

Solicitamos a retirada deste item.

RESPOSTA: Manteremos o protocolo de classificação layer 2, pois é necessário para integração com switches.

PERGUNTA: Item 6.3.10.1. Mínimo antena omnidirecional interna ou externa de, no mínimo, 4.9 dBi para a frequência de 2.4GHz.

Solicitamos a alteração do item: 6.3.10.1. Mínimo antena omnidirecional interna ou externa de, no mínimo, 3 dBi para a frequência de 2.4GHz.

RESPOSTA: Iremos rever o dimensionamento de potência. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: Item 6.3.10.2. Mínimo antena omnidirecional interna ou externa de, no mínimo, 5.7 dBi para a frequência de 5GHz.

Solicitamos a alteração do item: 6.3.10.2. Mínimo antena omnidirecional interna ou externa de, no mínimo, 3 dBi para a frequência de 5GHz.

RESPOSTA: Iremos rever o dimensionamento de potência. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: Item 6.3.11.2. 01 (uma) interface de console para gerenciamento por linha de comando.

Solicitamos a retirada deste item.

RESPOSTA PRODAM: Entendemos que este item é mandatório para o troubleshooting em access points e utilizamos atualmente.

PERGUNTA: Item 6.3.11.4. A sensibilidade de recepção dos Access points deve ser de no mínimo de -75 dBm para todas modulações exigidas neste termo de referência.

Solicitamos a alteração do item: 6.3.11.4. A sensibilidade de recepção dos Access points deve ser de no mínimo de -61 dBm para todas modulações exigidas neste termo de referência.

RESPOSTA: Iremos rever a sensibilidade mínima para cada frequência.

PERGUNTA: Item 6.4.4.3. Caso seja utilizado trunk por rádio, este deve operar em frequências distintas às do tráfego de dados da rede.

Solicitamos a retirada deste item.

RESPOSTA: Entendemos que a retirada deste item inviabiliza a implantação da tecnologia mesh de forma satisfatória.

PERGUNTA: Item 6.4.6.3. AES, TKIP, 802.1X - EAP-MD5. EAP-FAST (Flexible Authentication via Secure Tunneling). EAP-GTC (EAP – Generic Token Card). PEAPMSCHAPv2 (PEAP – Microsoft Challenge Authentication Protocol Version 2). EAP-TLS (EAP – Transport Layer Security).

Solicitamos a alteração do item: 6.4.6.3. AES, TKIP, 802.1X - EAP-MD5. PEAPMSCHAPv2 (PEAP – Microsoft Challenge Authentication Protocol Version 2). EAP-TLS (EAP – Transport Layer Security).

RESPOSTA: Manteremos os protocolos de autenticação, todos são populares e utilizados.

PERGUNTA: Item 6.4.7.3. Seleção de endereço padrão (RFC3484).

Solicitamos a retirada deste item.

RESPOSTA: Manteremos, pois seguimos os requisitos básicos de IPv6 do ipv6.br, descritos no documento RIPE 554 https://ipv6.br/download/requisitos-suporte-ipv6-ripe-554-pt.pdf segundo o guia para compras ou licitações de equipamentos com suporte a IPv6 https://ipv6.br/post/guia-para-compras-ou-licitacoes-de-equipamentos-com-suporte-a-ipv6/

PERGUNTA: Item 6.4.9.2. Implementação de Class of Service (CoS)

Solicitamos a retirada deste item.

RESPOSTA: Manteremos o protocolo de classificação layer 2, pois é necessário para integração com switches.

PERGUNTA: Item 6.4.11.1. Mínimo antena omnidirecional interna ou externa de, no mínimo, 4.2 dBi para a frequência de 2,4GHz.

Solicitamos a alteração do item: 6.4.11.1. Mínimo antena omnidirecional interna ou externa de, no mínimo, 3 dBi para a frequência de 2,4GHz

RESPOSTA: Iremos rever o dimensionamento de potência. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: Item 6.4.11.2. Mínimo antena omnidirecional interna ou externa de, no mínimo, 7.5 dBi para a frequência de 5GHz.

Solicitamos a alteração do item: 6.4.11.2. Mínimo antena omnidirecional interna ou externa de, no mínimo, 3 dBi para a frequência de 5GHz.

RESPOSTA: Iremos rever o dimensionamento de potência. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: Item 6.4.12.2. 01 (uma) interface de console para gerenciamento por linha de comando.

Solicitamos a retirada deste item.

RESPOSTA: Entendemos que este item é mandatório para o troubleshooting em access points e utilizamos atualmente.

PERGUNTA: Item A sensibilidade de recepção dos Access points deve ser de no mínimo de -75 dBm para todas modulações exigidas neste termo de referência.

Solicitamos a alteração do item: A sensibilidade de recepção dos Access points deve ser de no mínimo de -64 dBm para todas modulações exigidas neste termo de referência.

RESPOSTA: Iremos rever a sensibilidade mínima para cada frequência.

PERGUNTA: Item 6.5.3.3. Caso seja utilizado trunk por rádio, este deve operar em frequências distintas às do tráfego de dados da rede.

Solicitamos a retirada deste item.

RESPOSTA: Entendemos que a retirada deste item inviabiliza a implantação da tecnologia mesh de forma satisfatória.

PERGUNTA: Item 6.5.3.4. Deve atender ao padrão MIMO com 8 streams espaciais para as faixas de 5GHz e 4 spatial streams de 2,4GHz. Deve possuir triplo rádio permitindo operação nas faixas de 2,4 GHz e 5 GHz, em modo 8x8 nas faixas de frequência de 5GHz e 4x4 na faixa de 2,4GHz**.**

Solicitamos a alteração do item: 6.5.3.4. Deve atender ao padrão MIMO com 8 streams espaciais para as faixas de 5GHz e 4 spatial streams de 2,4GHz. Deve possuir duplo ou triplo rádio permitindo operação nas faixas de 2,4 GHz e 5 GHz, em modo 8x8 nas faixas de frequência de 5GHz e 4x4 na faixa de 2,4GHz.

RESPOSTA: O item será revisto.

PERGUNTA: Item 6.5.3.6. Suportar 2048 usuários simultâneos.

Solicitamos a alteração do item: 6.5.3.6. Suportar 1024 usuários simultâneos.

RESPOSTA: Iremos rever a quantidade de clientes associados.

PERGUNTA: Item 6.5.5.3. AES, TKIP, 802.1X - EAP-MD5. EAP-FAST (Flexible Authentication via Secure Tunneling). EAP-GTC (EAP – Generic Token Card). PEAPMSCHAPv2 (PEAP – Microsoft Challenge Authentication Protocol Version 2). EAP-TLS (EAP – Transport Layer Security).

Solicitamos a alteração do item: 6.5.5.3. AES, TKIP, 802.1X - EAP-MD5. PEAPMSCHAPv2 (PEAP – Microsoft Challenge Authentication Protocol Version 2). EAP-TLS (EAP – Transport Layer Security).

RESPOSTA: Manteremos os protocolos de autenticação, todos são populares e utilizados.

PERGUNTA: Item 6.5.6.3. Seleção de endereço padrão (RFC3484).

Solicitamos a retirada deste item.

RESPOSTA: Manteremos, pois seguimos os requisitos básicos de IPv6 do ipv6.br, descritos no documento RIPE 554 https://ipv6.br/download/requisitos-suporte-ipv6-ripe-554-pt.pdf segundo o guia para compras ou licitações de equipamentos com suporte a IPv6 https://ipv6.br/post/guia-para-compras-ou-licitacoes-de-equipamentos-com-suporte-a-ipv6/

PERGUNTA: Item 6.5.8.2. Implementação de Class of Service (CoS) segundo o padrão IEEE 802.1p.

Solicitamos a retirada deste item.

RESPOSTA: Manteremos o protocolo de classificação layer 2, pois é necessário para integração com switches.

PERGUNTA: Item 6.5.9.1. Os equipamentos deverão ser alimentados através de Power over Ethernet (Implementar IEEE 802.3bt).

Solicitamos a alteração do item: 6.5.9.1. Os equipamentos deverão ser alimentados através de Power over Ethernet (Implementar IEEE 802.3bt ou at conforme necessidade).

RESPOSTA: Nesta ARP há o fornecimento de power injector capaz de suprir as necessidades energéticas e há também uma ARP de Switches para tal.

Deixaremos claro que se o access point não necessitar de 802.3bt deverá suportar 802.3at, desde desempenhando todas as funções.

PERGUNTA: Item 6.5.10.1. Mínimo antena omnidirecional interna ou externa de, no mínimo, 4.3 dBi para a frequência de 2,4GHz.

RESPOSTA: Iremos rever o dimensionamento de antenas. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

Solicitamos a alteração do item: 6.5.10.1. Mínimo antena omnidirecional interna ou externa de, no mínimo, 2 dBi para a frequência de 2,4GHz.

PERGUNTA: Item 6.5.10.2. Mínimo antena omnidirecional interna ou externa de, no mínimo, 5.8 dBi para a frequência de 5GHz.

RESPOSTA: Iremos rever o dimensionamento de antenas. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

Solicitamos a alteração do item: 6.5.10.2. Mínimo antena omnidirecional interna ou externa de, no mínimo, 2 dBi para a frequência de 5GHz.

RESPOSTA: Iremos rever o dimensionamento de antenas. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: Item 6.5.11.2. 01 (uma) interface de console para gerenciamento por linha de comando.

Solicitamos a retirada deste item.

RESPOSTA: Entendemos que este item é mandatório para o troubleshooting em access points e utilizamos atualmente.

PERGUNTA: Item 6.5.11.4. A sensibilidade de recepção dos Access points deve ser de no mínimo de -75 dBm para todas modulações exigidas neste termo de referência.

Solicitamos a alteração do item: 6.5.11.4. A sensibilidade de recepção dos Access points deve ser de no mínimo de -56 dBm para todas modulações exigidas neste termo de referência.

RESPOSTA: Iremos rever o dimensionamento de potência. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: Item 6.6.2.2.1. Deverá alimentar através de Power over Ethernet (Implementar IEEE 802.3at - 30W).

Solicitamos a alteração do item: 6.6.2.2.1. Deverá alimentada através de Power over Ethernet (Implementar IEEE 802.3at/af ou bt) compatível com os itens 1, 2 e 3 relacionados neste edital seguindo suas respectivas especificações.

RESPOSTA: Devido da necessidade de portas multigigabit, os power injectors são direcionados para clientes que não terão essa necessidade, com equipamentos do tipo 1 e 2. Será mantido.

PERGUNTA: Item 6.7.16. Deve suportar a implantação de alta disponibilidade de modo redundante (ativo/standby).

Solicitamos a alteração do item: 6.7.16. Deve suportar a implantação de alta disponibilidade de modo redundante (ativo/standby) ou Cluster (ativo/ativo) .

RESPOSTA: Será acatada a sugestão.

PERGUNTA: Item 6.7.26. Deverá possuir ferramentas integradas para analisar os requerimentos de rádio frequência para implantação da rede sem fio, incluindo a melhor localização para instalação dos access points na planta física da localidade, configuração e estimativa de desempenho e área de cobertura.

Solicitamos a retirada deste item.

RESPOSTA: Este item é mandatório, uma necessidade do negócio e já utilizado.

PERGUNTA: Item 6.7.39. Deve ter capacidade de gerência da configuração, com armazenamento de diferentes versões de configuração e suporte para realizar "rollback".

Aguardo retorno, dúvidas estou a disposição.

Solicitamos a retirada deste item.

RESPOSTA: Este item é mandatório para quem entregar equipamentos físicos. Deixaremos mais claro que os itens de equipamentos físicos não se aplicam em nuvem ou gerenciamento compartilhado.

PERGUNTA: Item 6.7.43. Deve implementar assinaturas de ataques de rádio frequência e prevenção de intrusão para auxiliar o administrador a detectar rapidamente os ataques de RF (rádio frequência) no mínimo "Denial of Service (DoS)" e "Fake AP".

Solicitamos a alteração do item: 6.7.43. Deve implementar assinaturas de ataques de rádio frequência e prevenção de intrusão para auxiliar o administrador a detectar rapidamente os ataques de RF (rádio frequência) no mínimo "Denial of Service (DoS)" ou "Fake AP".

RESPOSTA: Entendemos que a solução deve implementar a prevenção de ambos os ataques. Será mantido.

PERGUNTA: Item 6.7.56.2. Implementar WEP com chaves estáticas e dinâmicas (40 bits e 128 bits).

Solicitamos a alteração do item: 6.7.56.2. Implementar WEP com chaves estáticas e dinâmicas.

RESPOSTA: Será mantido. Alteração deixa o protocolo vago e vulnerável.

PERGUNTA: Item 6.7.56.6. Implementar IEEE 802.1X, com pelo menos os seguintes métodos EAP : EAP-MD5, PEAP-GTC, PEAP-MSCHAPv2 e EAP-TLS.

Solicitamos a alteração do item: 6.7.56.6. Implementar IEEE 802.1X, com pelo menos os seguintes métodos EAP : EAP-MD5, PEAP-MSCHAPv2 ou EAP-TLS

RESPOSTA: Manteremos os protocolos de autenticação, todos são populares e utilizados.

PERGUNTA: Item 6.7.56.7. Deve ser capaz de autenticar usuários IEEE 802.1x utilizando o método PEAP sem a necessidade de servidor Radius Externo. Os usuários devem ser criados na base local do Controlador WLAN. **Solicitamos a retirada deste item.**

RESPOSTA: Item será revisto.

PERGUNTA: Item 6.7.56.16. Implementar suporte a assinaturas de ataques de RF (rádio frequência) e prevenção de intrusão, auxiliando o administrador a customizar arquivos de assinatura de ataques, detectando rapidamente ataques de RF (rádio frequência) no mínimo “Denial of Service (DoS)” e “Fake AP”.

Solicitamos a alteração do item: 6.7.56.16. Implementar suporte a assinaturas de ataques de RF (rádio frequência) e prevenção de intrusão, auxiliando o administrador a customizar arquivos de assinatura de ataques, detectando rapidamente ataques de RF (rádio frequência) no mínimo “Denial of Service (DoS)” ou “Fake AP”.

RESPOSTA: Entendemos que a solução deve implementar a prevenção de ambos os ataques. Será mantido.

PERGUNTA: Item 6.7.56.17. Implementar interface de gerenciamento de todas as funcionalidades localmente no controlador WLAN com suporte SSH, HTTPS via web browser, porta console e SNMP.

Solicitamos a alteração do item: 6.7.56.17. Implementar interface de gerenciamento de todas as funcionalidades localmente no controlador WLAN com suporte SSH, HTTPS via web browser, porta console ou SNMP.

RESPOSTA: Mudaremos a redação para:

Item 6.7.56.17. Implementar interface de gerenciamento de todas as funcionalidades localmente no controlador WLAN com suporte a:

SSH;

HTTPS via web browser;

Porta console;

SNMP;

Item 6.7.56.17.1. Deverá ser atendido por pelo menos 3 formas, conforme item 6.7.56.17.

PERGUNTA: Item 6.7.58.1.2. Utilização por equipamento (em kbps).

Solicitamos a alteração do item: 6.7.58.1.2. Utilização por equipamento (em kbps, Mbps ou Gbps).

RESPOSTA: Será acatado.

PERGUNTA: Item 6.7.58.1.3. Utilização por usuário (em kbps).

Solicitamos a alteração do item: 6.7.58.1.3. Utilização por usuário (em kbps, Mbps ou Gbps).

RESPOSTA: Será acatado.

Empresa ((NG))**CISCO**((CL))

PERGUNTA: Resposta à Prodam EDITAL DE CONSULTA PÚBLICA Nº 002/2022, PROCESSO SEI Nº 7010.2021/0007094-1.

Agradecemos a oportunidade de responder a consulta pública para prestação de serviço para fornecimento de equipamentos de rede wireless com suporte, manutenção e solução de gerenciamento.

6.3. Item 1 – Access Point Indoor 802.11 a/g/n/ac/ax nas frequências de 2.4GHz e 5GHz

Itens que necessitam serem removidos para viabilizar participação de solução Cisco.

6.3.3.5. Deve permitir redes locais, em que o tráfego dos APs não é encaminhado para a controladora e/ou gerenciamento, e redes centralizadas/tuneladas, em que todo tráfego de rede deve ser encaminhado para a controladora e/ou gerenciamento.

Observação: Entendemos que o processo permitindo os recursos avançados de ter uma controladora em nuvem e respectivos benefícios, não faz sentido solicitar a centralização do tráfego, ou seja, qual o motivador para o tráfego dos usuários serem submetidos antes a nuvem e retornar para o ambiente local para completar os acessos, já que todo o controle e segmentação de segurança pode ser feito diretamente no Access Point? A nossa solução permite que o tráfego seja tratado localmente sem a necessidade de um controle único e específico, limitador inclusive, do tráfego do cliente estar associado a um ponto central, sendo isso uma evolução dos novos formados de gerenciamento de uma solução Wifi, mesmo que em nuvem. Pedimos então retirar a exigência de redes centralizadas/toneladas.

RESPOSTA: A rede PRODAM é baseada atualmente em redes MPLS com internet centralizada e estamos caminhando para uma rede SD-WAN com links de internet locais, assim, necessitamos que enquanto não temos essa nova rede necessitamos de redes tuneladas para o pleno funcionamento, sem transportes de VLAN e demais configurações pela rede. A retirada de redes centralizadas/tuneladas inviabiliza a utilização a contento de redes wireless e geraria um passivo gigantesco de alterações de rede que é inviável de se fazer no fim de vida de uma tecnologia. Em um ambiente 100% SD-WAN entendemos que não teremos mais a necessidade de redes centralizadas/tuneladas e será removido. Durante esta transição, não temos como.

PERGUNTA: 6.3.6.1. Especificação básica de IPv6 (RFC2460).

6.3.6.2. Arquitetura de endereçamento IPv6 (RFC4291).

6.3.6.3. Seleção de endereço padrão (RFC3484).

6.3.6.4. ICMPv6 (RFC4443).

6.3.6.5. SLAAC (RFC4862).

Alterar para:

6.3.6.1. Suportar o uso de IPv6 para endereçamento de tráfego e gerenciamento, semelhante ao básico da RFC 2460

6.3.6.2. Suportar o uso de IPv6 para endereçamento de tráfego e gerenciamento, semelhante a arquitetura citada na RFC 4291

6.3.6.3. Utilizar os padrões de endereço IPv6 como citado na RFC3484 ou na mais recente RFC6724

6.3.6.4. Suportar o uso do ICMP sobre IPv6 (ICMPv6) para o tratamento de pacotes semelhante a RFC4443

6.3.6.5. Realizar o uso da autoconfiguração de endereçamento IPv6 semelhante a RFC4862

RESPOSTA: Entendemos que qualquer alteração que exista a oportunidade de fabricantes não demonstrarem atendimento as RFCs podem ser um ponto de vulnerabilidade por protocolos mal implementados e/ou que não funcionem a contento e/ou que não tenham interoperabilidade com outros equipamentos. Os itens serão mantidos. Seguimos os requisitos básicos de IPv6 do ipv6.br, descritos no documento RIPE 554 https://ipv6.br/download/requisitos-suporte-ipv6-ripe-554-pt.pdf segundo o guia para compras ou licitações de equipamentos com suporte a IPv6 https://ipv6.br/post/guia-para-compras-ou-licitacoes-de-equipamentos-com-suporte-a-ipv6/

PERGUNTA: 6.3.7.2. Telnet ou SSH(IPSEC).

Justificativa: Tendo em vista que uma solução de uso em nuvem provê muitos outros recursos, como escalabilidade e gerenciamento, entendemos que não existe uma finalidade exclusiva para o uso destes protocolos para qualquer atividade específica, já que na própria console em nuvem existe a possibilidade de realizar os troubleshootings necessários e

de maneira individual nos Access Points. Pedimos então retirar a exigência de desses protocolos.

RESPOSTA: Este item é mandatório para quem entregar equipamentos físicos. Deixaremos mais claro que os itens de equipamentos físicos não se aplicam em nuvem ou gerenciamento compartilhado.

PERGUNTA: 6.3.7.5. Suporte à configuração individual de, no mínimo, 16 (dezesseis) SSID

Justificativa: Hoje o mercado, na prática, utiliza entre 3 e 8 SSIDs por implementação, mesmo assim, aqui fala em suportar um mínimo de 16 individualmente, mas isso não é o que ocorre, uma vez que múltiplos SSID são distribuídos em redes distintas, aumentando as possibilidades. Pedimos então ajustar o valor para 15 para que permita nossa participação.

RESPOSTA: Será acatado.

PERGUNTA: 6.3.11.2. 01 (uma) interface de console para gerenciamento por linha de comando.

Justificativa: Uma vez que a solução em nuvem é capaz de fornecer o gerenciamento completos dos equipamentos, não temos necessidade de ter tal interface, se necessário a própria interface de rede permitirá uma conexão individual de gerenciamento e não deixando nenhum recurso descoberto na solução. Necessário remover este item para que soluções em nuvem possam concorrer neste processo. Pedimos então retirar a exigência de linhas de console para gerenciamento por linha de comando.

RESPOSTA: Este item é mandatório para quem entregar equipamentos físicos. Deixaremos mais claro que os itens de equipamentos físicos não se aplicam em nuvem ou gerenciamento compartilhado.

PERGUNTA: 6.3.11.4. A sensibilidade de recepção dos Access points deve ser de no mínimo de -75 dBm para todas as modulações exigidas neste termo de referência.

Justificativa: Na especificação técnica não encontramos as modulações citadas, mas entendemos que a sensibilidade dependerá da interferência

do ambiente (noise floor) e com isto não existe uma especificação única de potência necessária (dBm) para que a sensibilidade seja realizada em cálculo único. Recomendamos a remoção do item para que todos os concorrentes possam participar, ou, especificar outra forma de sensibilidade de uso dos canais, como o protocolo 802.11ax permite, ou seja, uso do BBS color field em uma modulação de 1024 QAM.

RESPOSTA: Iremos rever a sensibilidade mínima para cada frequência.

PERGUNTA: **Itens que sugerimos incluir para atender ao escopo do contrato de forma mais ampla em relação a capacidade técnica propiciando assim qualidade e estabilidade a rede proposta.**

a) Deve implementar radio WIFI dedicado para análise de spectro e funcionalidades de segurança através da implementação de Sistema de prevenção de intrusão sem fio (WIPS). Esse rádio devera ser capaz de atuar nas frequências de 2.4Ghz e 5Ghz
Justificativa: Entendemos que o benefício de uso de um rádio exclusivo permite não dividir funções de acesso e proteção, como no caso do uso do WIPS, evitando assim que não haja concorrência entre recursos.

RESPOSTA: O custo envolvido em rádios para análise de spectro e segurança não é algo ainda fácil de ser absorvido pela administração pública, neste momento.

PERGUNTA:

b) Permitir configurar o SSID para trabalhar nos modos NAT e BRIDGE. No modo NAT, o access point deverá distribuir IPs via DHCP para os clientes Wi-Fi, que ao efetuarem alguma navegação, terão os seus IPs traduzidos para o endereço IP adquirido pelo ponto de acesso através da rede cabeada. No modo brige, o ponto de acesso fará uma ponte entre a rede local e a rede WiFi, permitindo que os clientes WiFi adquiram endereçamento IP via DHCP da própria rede local onde o ponto de acesso for instalado;

Justificativa: As duas formas de ação possuem os seguintes benefícios exclusivos, quando usado como Bridge permitir que o cliente obtenha segmentação do seu tráfego até o caminho layer 3 que permitirá o acesso

a múltiplas redes, já no modo tradução, NAT, permite a não preocupação com uso de múltiplas redes, mesmo assim permite a segmentação de acessos e controles individuais, não onerando outros recursos de gestão de redes, como DHCP por exemplo.

RESPOSTA: O edital atual permite redes bridge e entendemos que para administração e troubleshooting que NAT são desaconselhados. Manteremos o edital sem a sugestão.

PERGUNTA:

c) Deve implementar roaming de camada 3 distribuído, onde seja possível configurar VPN e/ou tunelamentos entre access points, sem a necessidade de um appliance e/ou concentrador externo para tal função.
Justificativa: Essa funcionalidade permite não depender de um ponto único de falha, uma vez que isto será a âncora de conexão para manter o acesso ao cliente em processo de roaming

RESPOSTA: A rede PRODAM é baseada atualmente em redes MPLS com internet centralizada e estamos caminhando para uma rede SD-WAN com links de internet locais, assim, necessitamos que enquanto não temos essa nova rede necessitamos de redes tuneladas para o pleno funcionamento, sem transportes de VLAN e demais configurações pela rede. A retirada de redes centralizadas/tuneladas inviabiliza a utilização a contento de redes wireless e geraria um passivo gigantesco de alterações de rede que é inviável de se fazer no fim de vida de uma tecnologia. Em um ambiente 100% SD-WAN entendemos que não teremos mais a necessidade de redes centralizadas/tuneladas e será removido. Durante esta transição, não temos como.

PERGUNTA:

d) Deve permitir ser alimentado através da tecnologia PoE IEEE 802.3af utilizando a porta de switch na qual está conectado, ou através de dispositivo “power injector”, mantendo todas as funcionalidades habilitadas, e não consumindo mais do que 15W. Caso o equipamento necessite do padrão 802.3at para alimentação para manter todas as funcionalidades habilitadas, a proponente devera fornecer um power injector no padrão 802.3at junto com cada access point.

Justificativa: uma vez que o modelo 802.3at possui custo mais alto que o 802.3af entendemos que não há necessidade de adquirir todos do mesmo modelo e assim pode economizar para um item que não precisa ser 802.3at para garantir o perfeito funcionamento.

RESPOSTA: Nesta ARP há o fornecimento de power injector capaz de suprir as necessidades energéticas e há uma ARP de Switches para tal, não entendemos essa necessidade.

PERGUNTA: **6.4. Item 2 - Access Point Indoor 802.11 a/g/n/ac/ax nas frequências de 2.4GHz e 5GHz**

Itens que necessitam alteração e/ou remoção para viabilizar participação de solução Cisco.

6.4.4.5. Deve permitir redes locais, em que o tráfego dos APs não é encaminhado para a controladora e/ou gerenciamento, e redes centralizadas/tuneladas, em que todo tráfego de rede deve ser encaminhado para a controladora e/ou gerenciamento.

Justificativa: Entendemos que o processo permitindo os recursos avançados de ter uma controladora em nuvem e respectivos benefícios, não faz sentido solicitar a centralização do tráfego, ou seja, qual o motivador para o tráfego dos usuários serem submetidos antes a nuvem e retornar para o ambiente local para completar os acessos, já que todo o controle e segmentação de segurança pode ser feito diretamente no Access Point? A nossa solução permite que o tráfego seja tratado localmente sem a necessidade de um controle único e específico, limitador inclusive, do tráfego do cliente estar associado a um ponto central, sendo isso uma evolução dos novos formados de gerenciamento de uma solução Wifi, mesmo que em nuvem. Pedimos então retirar a exigência de redes centralizadas/toneladas.

RESPOSTA: A rede PRODAM é baseada atualmente em redes MPLS com internet centralizada e estamos caminhando para uma rede SD-WAN com links de internet locais, assim, necessitamos que enquanto não temos essa nova rede necessitamos de redes tuneladas para o pleno funcionamento,

sem transportes de VLAN e demais configurações pela rede. A retirada de redes centralizadas/tuneladas inviabiliza a utilização a contento de redes wireless e geraria um passivo gigantesco de alterações de rede que é inviável de se fazer no fim de vida de uma tecnologia. Em um ambiente 100% SD-WAN entendemos que não teremos mais a necessidade de redes centralizadas/tuneladas e será removido. Durante esta transição, não temos como.

PERGUNTA:

6.4.7.1. Especificação básica de IPv6 (RFC2460).

6.4.7.2. Arquitetura de endereçamento IPv6 (RFC4291).

6.4.7.3. Seleção de endereço padrão (RFC3484).

6.4.7.4. ICMPv6 (RFC4443).

6.4.7.5. SLAAC (RFC4862).

Alterar para:

6.4.7.1. Suportar o uso de IPv6 para endereçamento de tráfego e gerenciamento, semelhante ao básico da RFC 2460

6.4.7.2. Suportar o uso de IPv6 para endereçamento de tráfego e gerenciamento, semelhante a arquitetura citada na RFC 4291

6.4.7.3. Utilizar os padrões de endereço IPv6 como citado na RFC3484 ou na mais recente RFC6724

6.4.7.4. Suportar o uso do ICMP sobre IPv6 (ICMPv6) para o tratamento de pacotes semelhante a RFC4443

6.4.7.5. Realizar o uso da autoconfiguração de endereçamento IPv6 semelhante a RFC4862.

RESPOSTA: Entendemos que qualquer alteração que exista a oportunidade de fabricantes não demonstrarem atendimento as RFCs podem ser um ponto de vulnerabilidade por protocolos mal implementados e/ou que não funcionem a contento e/ou que não tenham interoperabilidade com outros

equipamentos. Os itens serão mantidos. Seguimos os requisitos básicos de IPv6 do ipv6.br, descritos no documento RIPE 554 https://ipv6.br/download/requisitos-suporte-ipv6-ripe-554-pt.pdf segundo o guia para compras ou licitações de equipamentos com suporte a IPv6 https://ipv6.br/post/guia-para-compras-ou-licitacoes-de-equipamentos-com-suporte-a-ipv6/

PERGUNTA: 6.4.8.2. Telnet ou SSH(IPSEC).

Justificativa: Tendo em vista que uma solução de uso em nuvem provê muitos outros recursos, como escalabilidade e gerenciamento, entendemos que não existe uma finalidade exclusiva para o uso destes protocolos para qualquer atividade específica, já que na própria console em nuvem existe a possibilidade de realizar os troubleshootings necessários e de maneira individual nos Access Points. Pedimos então retirar a exigência de desses protocolos.

RESPOSTA: Este item é mandatório para quem entregar equipamentos físicos. Deixaremos mais claro que os itens de equipamentos físicos não se aplicam em nuvem ou gerenciamento compartilhado.

PERGUNTA: 6.4.8.5. Suporte à configuração individual de, no mínimo, 16 (dezesseis) SSID

Justificativa: Hoje o mercado, na prática, costuma utilizar entre 3 e 8 SSIDs por implementação, mesmo assim, aqui fala em suportar um mínimo de 16 individualmente, mas isso não é o que ocorre, uma vez que múltiplos SSID são distribuídos em redes distintas, aumentando as possibilidades. Recomendamos ajustar o valor para 15 para que permita nossa participação.

RESPOSTA: Será acatado.

PERGUNTA: 6.4.11.2. Mínimo antena omnidirecional interna ou externa de, no mínimo, 7.5 dBi para a frequência de 5GHz.

Justificativa: Necessário alterar o item para no mínimo 5.9 dBi para permitir nossa participação

RESPOSTA: Iremos rever o dimensionamento de antenas. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: 6.4.12.2. 01 (uma) interface de console para gerenciamento por linha de comando.

Justificativa: Uma vez que a solução em nuvem é capaz de fornecer o gerenciamento completos dos equipamentos, não temos necessidade de ter tal interface, se necessário a própria interface de rede permitirá uma conexão individual de gerenciamento e não deixando nenhum recurso descoberto na solução. Necessário remover este item para que soluções em nuvem possam concorrer neste processo. Pedimos então retirar a exigência de linhas de console para gerenciamento por linha de comando.

RESPOSTA: Entendemos que este item é mandatório para o troubleshooting em access points e utilizamos atualmente.

PERGUNTA: 6.3.11.4. A sensibilidade de recepção dos Access points deve ser de no mínimo de -75 dBm para todas as modulações exigidas neste termo de referência.

Justificativa: Na especificação técnica não encontramos as modulações citadas, mas entendemos que a sensibilidade dependerá da interferência do ambiente (noise floor) e com isto não existe uma especificação única de potência necessária (dBm) para que a sensibilidade seja realizada em cálculo único. Recomendamos a remoção do item para que todos os concorrentes possam participar, ou, especificar outra forma de sensibilidade de uso dos canais, como o protocolo 802.11ax permite, ou seja, uso do BBS color field em uma modulação de 1024 QAM.

RESPOSTA: Iremos rever o dimensionamento de potência. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: **Itens que sugerimos incluir para atender ao escopo do contrato de forma mais ampla em relação a capacidade técnica propiciando assim qualidade e estabilidade a rede proposta.**

a) Deve implementar radio WIFI dedicado para análise de spectro e funcionalidades de segurança através da implementação de Sistema de prevenção de intrusão sem fio (WIPS). Esse radio devera ser capaz de atuar nas frequências de 2.4Ghz e 5Ghz

Justificativa: Entendemos que o benefício de uso de um rádio exclusivo permite não dividir funções de acesso e proteção, como no caso do uso do WIPS

RESPOSTA: O custo envolvido em rádios para análise de spectro e segurança não é algo ainda fácil de ser absorvido pela administração pública, neste momento.

PERGUNTA:

b) Permitir configurar o SSID para trabalhar nos modos NAT e BRIDGE. No modo NAT, o access point deverá distribuir IPs via DHCP para os clientes Wi-Fi, que ao efetuarem alguma navegação, terão os seus IPs traduzidos para o endereço IP adquirido pelo ponto de acesso através da rede cabeada. No modo brige, o ponto de acesso fará uma ponte entre a rede local e a rede WiFi, permitindo que os clientes WiFi adquiram endereçamento IP via DHCP da própria rede local onde o ponto de acesso for instalado;
Justificativa: As duas formas de ação possuem os seguintes benefícios exclusivos, quando usado como Bridge permitir que o cliente obtenha segmentação do seu tráfego até o caminho layer 3 que permitirá o acesso a múltiplas redes, já no modo tradução, NAT, permite a não preocupação com uso de múltiplas redes, mas mesmo assim permite a segmentação de acessos e controles individuais, não onerando outros recursos de gestão de redes, como DHCP por exemplo.

RESPOSTA: O edital atual permite redes bridge e entendemos que para administração e troubleshooting que NAT são desaconselhados. Manteremos o edital sem a sugestão.

PERGUNTA:

c) Deve implementar roaming de camada 3 distribuído, onde seja possível configurar VPN e/ou tunelamentos entre access points, sem a necessidade de um appliance e/ou concentrador externo para tal função

Justificativa: Essa funcionalidade permite não depender de um ponto único de falha, uma vez que isto será a âncora de conexão para manter o acesso ao cliente em processo de roaming.

RESPOSTA: A rede PRODAM é baseada atualmente em redes MPLS com internet centralizada e estamos caminhando para uma rede SD-WAN com links de internet locais, assim, necessitamos que enquanto não temos essa nova rede necessitamos de redes tuneladas para o pleno funcionamento, sem transportes de VLAN e demais configurações pela rede. A retirada de redes centralizadas/tuneladas inviabiliza a utilização a contento de redes wireless e geraria um passivo gigantesco de alterações de rede que é inviável de se fazer no fim de vida de uma tecnologia. Em um ambiente 100% SD-WAN entendemos que não teremos mais a necessidade de redes centralizadas/tuneladas e será removido. Durante esta transição, não temos como.

PERGUNTA:

D) Deve permitir ser alimentado através da tecnologia PoE IEEE 802.3af utilizando a porta de switch na qual está conectado, ou através de dispositivo “power injector”, mantendo todas as funcionalidades habilitadas, e não consumindo mais do que 15W. Caso o equipamento necessite do padrão 802.3at para alimentação para manter todas as funcionalidades habilitadas, a proponente devera fornecer um power injector no padrão 802.3at junto com cada access point

Justificativa: uma vez que o modelo 802.3at possui custo mais alto que o 802.3af entendemos que não há necessidade de adquirir todos do mesmo modelo e assim pode economizar para um item que não precisa ser 802.3at para garantir o perfeito funcionamento.

RESPOSTA: Nesta ARP há o fornecimento de power injector capaz de suprir as necessidades energéticas e há uma ARP de Switches para tal, não entendemos essa necessidade.

PERGUNTA: **6.5. Item 3 - Access Point Indoor 802.11 a/g/n/ac/ax nas frequências de 2.4GHz e 5GHz**

Itens que necessitam alteração e/ou remoção para viabilizar participação de solução Cisco.

6.5.3.4. Deve atender ao padrão MIMO com 8 streams espaciais para as faixas de 5GHz e 4 spatial streams de 2,4GHz. Deve possuir triplo rádio permitindo operação nas faixas de 2,4 GHz e 5 GHz, em modo 8x8 nas faixas de frequência de 5GHz e 4x4 na faixa de 2,4GHz.

Justificativa/Recomendação: Não suporta radio triplo. Alguns concorrentes suportam radio triplo através do slip do radio 5G 8x8:8 em dois radios 5G porém com 4x4:4

RESPOSTA: O item será revisto.

PERGUNTA: 6.5.3.5. Deve permitir redes locais, em que o tráfego dos APs não é encaminhado para a controladora e/ou gerenciamento, e redes centralizadas/tuneladas, em que todo tráfego de rede deve ser encaminhado para a controladora e/ou gerenciamento.

Justificativa/Recomendação: Entendemos que o processo permitindo os recursos avançados de ter uma controladora em nuvem e respectivos benefícios, não faz sentido solicitar a centralização do tráfego, ou seja, qual o motivador para o tráfego do usuários serem submetidos antes a nuvem e retornar para o ambiente local para completar os acessos, já que todo o controle e segmentação de segurança pode ser feito diretamente no Access Point?

A nossa solução permite que o tráfego seja tratado localmente sem a necessidade de um controle único e específico, limitador inclusive, do tráfego do cliente estar associado a um ponto central, sendo isso uma

evolução dos novos formados de gerenciamento de uma solução Wifi, mesmo que em nuvem. Pedimos então retirar a exigência de redes centralizadas/toneladas.

RESPOSTA: A rede PRODAM é baseada atualmente em redes MPLS com internet centralizada e estamos caminhando para uma rede SD-WAN com links de internet locais, assim, necessitamos que enquanto não temos essa nova rede necessitamos de redes tuneladas para o pleno funcionamento, sem transportes de VLAN e demais configurações pela rede. A retirada de redes centralizadas/tuneladas inviabiliza a utilização a contento de redes wireless e geraria um passivo gigantesco de alterações de rede que é inviável de se fazer no fim de vida de uma tecnologia. Em um ambiente 100% SD-WAN entendemos que não teremos mais a necessidade de redes centralizadas/tuneladas e será removido. Durante esta transição, não temos como.

PERGUNTA: 6.5.3.6. Suportar 2048 usuários simultâneos

Justificativa/Recomendação: Suportamos 512 usuários simultâneos por radio, o que totalizam até 1024 usuários simultâneos utilizando os rádios 2.4 e 5Ghz

RESPOSTA: Iremos rever a quantidade de clientes associados.

PERGUNTA: 6.5.7.2. Telnet ou SSH(IPSEC).

Justificativa/Recomendação: Tendo em vista que uma solução de uso em nuvem provê muitos outros recursos, como escalabilidade e gerenciamento, entendemos que não existe uma finalidade exclusiva para o uso destes protocolos para qualquer atividade específica, já que na própria console em nuvem existe a possibilidade de realizar os troubleshootings necessários e de maneira individual nos Access Points. Pedimos então retirar a exigência de desses protocolos.

6.5.7.5. Suporte à configuração individual de, no mínimo, 16 (dezesseis) SSID

Justificativa/Recomendação: Hoje o mercado, na prática, costuma utilizar entre 3 e 8 SSIDs por implementação, mesmo assim, aqui fala em suportar

um mínimo de 16 individualmente, mas isso não é o que ocorre, uma vez que múltiplos SSID são distribuídos em redes distintas, aumentando as possibilidades. Recomendamos ajustar o valor para 15 para que permita nossa participação.

RESPOSTA: Será acatado.

PERGUNTA: 6.5.11.1. No mínimo 02 (duas) portas Ethernet (100/1000/2500/5000Base-T –IEEE 802.3, 802.3u e 802.3bz) autosense.

Justificativa/Recomendação: Suportamos 1x interface de rede MultiGiga de ate 5GbE

RESPOSTA: O item será revisto.

PERGUNTA:6.5.11.2. 01 (uma) interface de console para gerenciamento por linha de comando.

Justificativa/Recomendação: Access Points gerenciados através de nuvem não suportam linha de comando

RESPOSTA: Este item é mandatório para quem entregar equipamentos físicos. Deixaremos mais claro que os itens de equipamentos físicos não se aplicam em nuvem ou gerenciamento compartilhado.

PERGUNTA: 6.5.11.4. A sensibilidade de recepção dos Access points deve ser de no mínimo de -75 dBm para todas as modulações exigidas neste termo de referência.

Justificativa/Recomendação: Na especificação técnica não encontramos as modulações citadas, mas entendemos que a sensibilidade dependerá da interferência do ambiente (noise floor) e com isto não existe uma especificação única de potência necessária (dBm) para que a sensibilidade seja realizada em cálculo único. Recomendamos a remoção do item para que todos os concorrentes possam participar, ou, especificar outra forma de sensibilidade de uso dos canais, como o protocolo 802.11ax permite, ou seja, uso do BBS color field em uma modulação de 1024 QAM.

RESPOSTA: Iremos rever o dimensionamento de potência. Solicitamos marca/modelo para todas as empresas que fizeram questionamento e balizaremos pelos equipamentos que se posicionam nas necessidades da PMSP, no mínimo 3 fabricantes.

PERGUNTA: **Itens que sugerimos incluir para atender ao escopo do contrato de forma mais ampla em relação a capacidade técnica propiciando assim qualidade e estabilidade a rede proposta.**

a) Deve implementar radio WIFI dedicado para análise de spectro e funcionalidades de segurança através da implementação de Sistema de prevenção de intrusão sem fio (WIPS). Esse radio devera ser capaz de atuar nas frequências de 2.4Ghz e 5Ghz

Justificativa: Entendemos que o benefício de uso de um rádio exclusivo permite não dividir funções de acesso e proteção, como no caso do uso do WIPS

RESPOSTA: O custo envolvido em rádios para análise de spectro e segurança não é algo ainda fácil de ser absorvido pela administração pública, neste momento.

PERGUNTA:

b) Permitir configurar o SSID para trabalhar nos modos NAT e BRIDGE. No modo NAT, o access point deverá distribuir IPs via DHCP para os clientes Wi-Fi, que ao efetuarem alguma navegação, terão os seus IPs traduzidos para o endereço IP adquirido pelo ponto de acesso através da rede cabeada. No modo brige, o ponto de acesso fará uma ponte entre a rede local e a rede WiFi, permitindo que os clientes WiFi adquiram endereçamento IP via DHCP da própria rede local onde o ponto de acesso for instalado;
Justificativa: As duas formas de ação possuem os seguintes benefícios exclusivos, quando usado como Bridge permitir que o cliente obtenha segmentação do seu tráfego até o caminho layer 3 que permitirá o acesso a múltiplas redes, já no modo tradução, NAT, permite a não preocupação com uso de múltiplas redes, mas mesmo assim permite a segmentação de acessos e controles individuais, não onerando outros recursos de gestão de redes, como DHCP por exemplo.

RESPOSTA: O edital atual permite redes bridge e entendemos que para administração e troubleshooting que NAT são desaconselhados. Manteremos o edital sem a sugestão.

PERGUNTA:

c) Deve implementar roaming de camada 3 distribuído, onde seja possível configurar VPN e/ou tunelamentos entre access points, sem a necessidade de um appliance e/ou concentrador externo para tal função

Justificativa: Essa funcionalidade permite não depender de um ponto único de falha, uma vez que isto será a âncora de conexão para manter o acesso ao cliente em processo de roaming

RESPOSTA: A rede PRODAM é baseada atualmente em redes MPLS com internet centralizada e estamos caminhando para uma rede SD-WAN com links de internet locais, assim, necessitamos que enquanto não temos essa nova rede necessitamos de redes tuneladas para o pleno funcionamento, sem transportes de VLAN e demais configurações pela rede. A retirada de redes centralizadas/tuneladas inviabiliza a utilização a contento de redes wireless e geraria um passivo gigantesco de alterações de rede que é inviável de se fazer no fim de vida de uma tecnologia. Em um ambiente 100% SD-WAN entendemos que não teremos mais a necessidade de redes centralizadas/tuneladas e será removido. Durante esta transição, não temos como.

PERGUNTA:

d) Deve implementar e operar com todas as interfaces e funcionalidades habilitadas, com alimentação de energia através da tecnologia PoE+ IEEE 802.3at utilizando a porta de switch na qual está conectado, ou através de dispositivo “power injector”, e não consumindo mais do que 30W.

Justificativa: uma vez que o modelo 802.3at possui custo mais alto que o 802.3af entendemos que não há necessidade de adquirir todos do mesmo modelo e assim pode economizar para um item que não precisa ser 802.3at para garantir o perfeito funcionamento.

PERGUNTA: **6.7. SOLUÇÃO DE CONTROLE E GERENCIAMENTO WIRELESS**

Itens que necessitam alteração e/ou remoção para viabilizar participação de solução Cisco.

6.7.8. Todo o hardware da solução de gerenciamento deverá obedecer ao tamanho de 19”, do rack descrito no item 6.7.7, e cada equipamento deverá possuir no máximo 4U. Assim caso sejam fornecidas 2 (duas) controladoras e 2 (dois) gerenciamentos, não deverá superar a medida de 20U em cada Datacenter, contando com os espaçadores de patch cord.

OBS: Nossa solução de gerenciamento é Nuvem, dessa forma entendemos que item não se aplica.

RESPOSTA: Este item é mandatório para quem entregar equipamentos físicos. Deixaremos mais claro que os itens de equipamentos físicos não se aplicam em nuvem ou gerenciamento compartilhado.

PERGUNTA: 6.7.18. Deve permitir a organização hierárquica dos access points em plantas, de plantas em prédios e de prédios em projetos.

Recomendação: Entendemos que a palavra "Projetos" está aplicada de maneira ampla no texto, ou seja, recomendamos alterar para "de prédios em redes"

RESPOSTA: O item será melhor elaborado.

PERGUNTA: 6.7.26. Deverá possuir ferramentas integradas para analisar os requerimentos de rádio frequência para implantação da rede sem fio, incluindo a melhor localização para instalação dos access points na planta física da localidade, configuração e estimativa de desempenho e área de cobertura.

Recomendação: Ferramentas de cálculo de radio frequência, verificação de ruídos e saúde de maneira geral, não são contempladas por uma solução de gestão de rede sem fio, apesar de habilitarem o uso de diferentes access points para realizar a medição, não é uma função nativa de soluções desta natureza. Necessário retirar tal exigência.

RESPOSTA: Este item é mandatório e utilizamos atualmente. Necessitamos de uma ferramenta que tenha essas funcionalidades, nem que seja adicional como compreendido nos itens 6.7.9. e 6.7.10.

“6.7.9. As funções descritas nos no item **Erro! Fonte de referência não encontrada.** devem ser complementares, ou seja, devem operar em conjunto, independente de que equipamento possui a funcionalidade.”

“6.7.10. Caso seja necessário equipamentos adicionais para suprir as funções solicitadas no item 6.7, serão aceitos, desde que continuem mantendo as características solicitadas e a ocupação de rack definido no item **Erro! Fonte de referência não encontrada.**.”

PERGUNTA: 6.7.32. Deve possuir a capacidade de segmentar os Access Points em grupos de interesse de forma a correlacionar alarmes de dois ou mais access points wireless para uma mesma fonte de interferência, e reportar ao administrador como um só dispositivo.

Recomendação: Entendemos que não há a necessidade de agrupar alertas, uma vez que é possível ter um painel único de todos os alertas, bem como estar segmentado pela rede ou respectiva área física. Pedimos retirar ou alterar item para permitir participação.

RESPOSTA: Será alterada a redação para deixar claro que a funcionalidade é informar alertas de um grupo criado na união de dois ou mais access points.

PERGUNTA: 6.7.33. Deve permitir a configuração de, pelo menos, 8 (oito) grupos diferentes de usuários e administradores, com níveis de privilégios de acesso e configuração distintos.

Recomendação: Alterar o item para ter configuração gradual de permissões por usuários, pois não suportamos o uso de grupos, solicitamos remover o item ou alterar conforme mencionado.

RESPOSTA: configuração gradual de permissões é um termo vago que poderia gerar questionamentos. O número de grupos foi baseado nos grupos que diversos fabricantes tem de variação entre o ‘read only’,

‘operator’ e ‘system admin’. Por favor, me informem os tipos de grupos disponíveis e pré-existentes.

PERGUNTA: **Itens que sugerimos incluir para atender ao escopo do contrato de forma mais ampla em relação a capacidade técnica propiciando assim qualidade e estabilidade a rede proposta.**

e) A plataforma de gerência na nuvem, e conjunto com equipamentos de ponto de acesso, devem implementar localização de ativos ("Asset Location") baseada no protocolo BLE (Bluetooth Low Energy) e WIFI. As informações apresentadas devem incluir capacidade de visualizar graficamente no mapa onde estão geograficamente distribuídos os ativos em questão.

Justificativa: Com esta tecnologia é possível, além de fornecer acesso a rede sem fio, a possibilidade de monitorar dispositivos que possuam a tecnologia Bluethooth para controle de ativos, como a movimentação de etiquetas eletrônicas de patrimônio, por exemplo.

RESPOSTA: Neste momento não temos interesse em tal funcionalidade.

PERGUNTA:

f) Deve implementar padrão IPV6, incluindo conectividade com a gerência na nuvem através de dual-stack (IPv4 e IPv6) e regras de saída (outbound) de firewall de camada 3 com endereços IPv4 e IPv6 de destino.

Justificativa: Entendemos que mais além do que suportar o uso de IPv6, solicitados nos itens 1, 2 e 3, se faz necessário que a gerência suporta ao mesmo tempo operar o Access Points de maneira heterogênea, ou seja, num mesmo painel gerenciar e observar Access Point com IPv4 e IPv6 ao mesmo tempo.

RESPOSTA: Entendemos que no momento é mais importante a utilização de redes em IPv6, seguindo as RFCs do que a gerencia.

PERGUNTA:

g) Deve possuir mecanismo que não permita a utilização do Access Point em outras redes e ambientes, em caso de furto. A ferramenta de

gerência na nuvem deve ser capaz de bloquear o equipamento, e caso ele seja reconectado a internet, detectar e rastrear o equipamento, baseado no endereço IP publico utilizado pelo mesmo.

Justificativa: Com a utilização exclusiva do Serial Number é possível manter a exclusividade do uso na gerência, isto permite que mesmo sendo um dispositivo evoluído para gestão em nuvem o mesmo não seja utilizado por outro controlador exclusivo (tenant). Desta forma não incentivando o uso indevido.

RESPOSTA: O item será analisado.

PERGUNTA:

h) Deve implementar recursos de filtro de aplicação para reconhecimento e bloqueio de conteúdos relacionados a jogos, compartilhamento de arquivos, redes sociais, entre outros. Caso este recurso necessite de licença, a mesma deve ser fornecida pelo mesmo período de tempo coberto pela garantia solicitada neste termo de referência

Justificativa: O grande benefício em controlar aplicações na ponta é a limitação do tráfego indesejado operar em todo o caminho da rede, ou seja, até que chegue em um Firewall por exemplo. Ou seja, esse tráfego já seria tratado ou higienizado muito próximo a origem, ganhando assim mais performance de rede e maior segurança

RESPOSTA: As funções de firewall ficam a cargo da área de segurança, em equipamentos próprios deles para tal.

PERGUNTA:

i) Deve implementar solução segurança baseada em DNS com as seguintes características mínimas: deve possuir no mínimo 50 categorias de URL Filtering; deve possuir logs de bloqueio e liberação de acessos a URL's; Deve ser capaz de bloquear domínios suspeitos de propagar ou implementar atividades que comprometam a segurança dos usuários, tais como propagação de malware, atividades de phishing, botnet e outros.

Justificativa: Mesmo que o controle de consultas DNS não seja o foco de uma gestão de rede sem-fio, é importante prever a integração de um recurso assim, um exemplo a ser citado é o controle de navegação para redes que os usuários não são corporativos e não pode ser feito o controle de navegação granular. Já com o recuso de uso de categorias de DNS isso será possível, como redes de Visitantes, por exemplo. De uso na maioria das empresas. Além disso a consulta DNS é em mais de 90% dos casos o primeiro protocolo de rede a ser utilizada e ter a gestão dessas consultas numa ferramenta assim, permite também higienizar muitas conexões TCP que não seriam necessárias, otimizando a rede.

RESPOSTA: As funções de firewall ficam a cargo da área de segurança, em equipamentos próprios deles para tal.

PERGUNTA:

j) Deve implementar controle e traffic shaping de aplicações por usuário reconhecendo no mínimo 1000 aplicações incluindo a disponibilização de relatórios; deve ser fornecido com todas as licenças necessárias para esta funcionalidade.

Justificativa: Este benefício permite que seja controlado o uso excessivo de aplicações que consumam alto tráfego, hoje é muito importante para não ter que apenas bloquear aquele recurso, mas que ele seja permitido e controlado a contento.

RESPOSTA: As funções de traffic shapping ficam a cargo dos equipamentos próprios para tal.

PERGUNTA:

k) A plataforma de gerencia na nuvem deve implementar interface de software ("application program interface" ou API) que permita interagir diretamente com a plataforma e com os dispositivos gerenciados pela mesma. A API deve conter um conjunto de ferramentas conhecidas como endpoints para criar software e aplicativos que se comunicam com o painel de gerência da nuvem, para casos de uso como provisionamento, alterações de configuração em massa, monitoramento e controles de acesso baseados em função. Essa API deve suportar arquitetura RESTful, utilizando protocolo HTTPS para requisições de URLs e JSON.

Justificativa: O uso de APIs é cada vez mais crescente, pois traz em uma "linguagem comum" a possibilidade de diferentes sistemas cooperarem entre si, ou seja, permite tanto gerenciar parâmetros configuráveis quanto coletar dados gerados por determinada solução.

RESPOSTA: É uma funcionalidade bem-vinda mas não mandatória e necessita análise se pelo menos 3 fabricantes possuem tal funcionalidade para incluir no Termo de Referência.

PERGUNTA:

l) A plataforma de gerencia na nuvem deve implementar apresentação de informações de localização dos usuários e dispositivos, utilizando informações coletadas dos pontos de acesso (APs), através da detecção de requisições e frames do protocolo 802.11 (Wifi), e também de informações coletadas via protocolo Bluetooth, incluindo anonimamente informações de de dispositivos BLE (Bluetooh Low Energy) como parte de seu conjunto de dados de análise de localização. As informações apresentadas devem incluir capacidade de visualizar onde as pessoas estão gastando tempo dentro de um determinado local ao longo do dia (independentemente de seus dispositivos estarem ou não associados à rede sem fio).

Justificativa: Este recurso trará o benefício de triangulação de dispositivos e ativos, uma vez que a gerência poderá fornecer essa visão consolidada, conforme o caso de uso.

RESPOSTA: É uma funcionalidade bem-vinda mas não mandatória e necessita análise se pelo menos 3 fabricantes possuem tal funcionalidade para incluir no Termo de Referência.

PERGUNTA:

m) Deve disponibilizar um formato de relatório sintético, com o resumo das principais informações estatísticas de utilização dos Access Points, como por exemplo: SSIDs mais usados, usuários com maior consumo de dados, aplicações mais utilizadas, tipos de dispositivos mais usados (Sistema Operacional), Access Points mais utilizados, volume total de banda e quantidade total de usuários. Tal relatório ainda deve possibilitar ser enviado por e-mail, para usuários definidos pelo Administrador; O relatório devera ter a possibilidade de agendamento e inserção de logotipo customizado no E-mail a ser enviado pelo sistema.

Justificativa: Importante do ponto de vista de gestão entender o comportamento orgânico de uma rede sem fio, como densidade, posicionamento e clientes conectados nessa malha de uso.

RESPOSTA: Entendemos que os itens 6.7.44, 6.7.45 e 6.7.46 compreendem as necessidades atuais.

PERGUNTA:

n) Deve implementar identificação das principais aplicações de camada 7 no tráfego de dados dos usuários, sem a necessidade de equipamentos externos para tal. Deve também ser capaz de apresentar as informações sobre as principais aplicações de camada 7 que passaram pelo equipamento, correlacionando estas informações com as informações de usuários, e apresentando de maneira clara, gráficos de consumo de aplicações camada 7, por usuário.

Justificativa: Com o uso de controle de aplicação, se faz necessário também entender o uso das mesmas para controle e melhor direcionamentos de esforços de gestão da solução.

RESPOSTA: As funções de firewall ficam a cargo da área de segurança, em equipamentos próprios deles para tal.