AUDIÊNCIA PÚBLICA
Nº 01/2019

OBJETO – CONTRATAÇÃO DE EMPRESA PARA AQUISIÇÃO, INSTALAÇÃO, CONFIGURAÇÃO, MANUTENÇÃO E GARANTIA DE PONTO DE ACESSO WIFI COM SOLUÇÃO DE CONTROLADORA WIRELESS EM NUVEM PARA REDE PÚBLICA DE EDUCAÇÃO DO ESTADO DE SÃO PAULO.

EMPRESA: Compwire
RESPONSÁVEL: Lígia Moreira
E-MAIL: ligia.moreira@compwire.com.br
DATA: 27/05/19 as 17:29

Srs.
Boa tarde!
Com a finalidade de participar da Contratação supracitada, solicitamos esclarecer:

QUESTIONAMENTO 01:

Referente ao item 4.1.2.10: Deve implementar recursos de firewall stateful.

Entendemos que esse recurso é muito comum aos equipamentos de Firewall, e são utilizados como boas práticas de implantação de soluções WLAN o uso do Appliance de Firewall para executar as regras de permissões e políticas de acesso associadas a cada SSID, não fazendo sentido a aplicação de políticas de firewall para cada Access Point, visto que tais recursos podem onerar a performance para a principal função do Access Points que é entregar um “throughput”, capacidade de conexão de usuários e da cobertura de sinal, além da complexidade de gestão de políticas e regras de firewall de maneira “standalone” (gestão para cada Access Point de maneira individual), visto a grande volumetria de Access Points que serão adquiridas e pelo Firewall essas políticas são aplicadas de maneira ampla, atendendo a todos os Access Points, pois associa as políticas ao SSID e não ao Access Point. Dessa maneira entendemos que esse recurso não se faz necessário. Está correto nosso entendimento?

R.: Entendimento incorreto. Conforme informado na audiência pública, levando em considerações as boas práticas de segurança, sempre que possível, os controles de acesso devem ser realizados o mais próximo da origem, que neste caso é o próprio access point. Além disso, a solução de stateful no access point servirá para controlar a comunicação entre equipamentos da rede Wifi e os equipamentos da rede cabeada, uma vez que o access point terá a sua porta ethernet conectada em um seguimento de rede que compartilha acessos com outros dispositivos.

QUESTIONAMENTO 02:

Referente aos itens 4.1.2.12, 4.1.2.16 a 4.1.2.20:

Especificações referente a performance dos equipamentos, como por exemplo taxa de transferência, números de usuário conectados e recursos avançados de propagação do sinal, que possibilitam a cobertura de uma are maior e consequentemente um número maior de usuários com menos Pontos de Acesso estão sendo negligenciados, tornando uma futura aquisição dentro desses parâmetros obsoleta em poucos anos.

R.: A FDE entende que a especificação técnica não negligencia parâmetros de performance, uma vez que os próprios itens mencionados na consideração acima, dentre outros muitos descritos no termo de referência, estão relacionados a este assunto.

QUESTIONAMENTO 03:

Referente ao item 4.1.2.7:

Deve implementar, localmente ou em conjunto com a solução de controladora Wireless em nuvem, Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Indentity Providers - IDP's) de terceiros.
Poderiam por favor nos esclarecer melhor essa solicitação e sua usabilidade.

R.: Conforme informado na audiência pública, a solicitação do protocolo SAML se dá devido as parcerias existentes entre Secretaria da Educação com a Microsoft e o Google. Ambos os provedores possuem uma base de usuários da secretaria da Educação e suportam o protocolo SAML para autenticação de usuários. Esta funcionalidade poderá ser utilizada em um futuro próximo como opção de autenticação da rede WiFi.

EMPRESA: Sonda
RESPONSÁVEL: Orlando Sabato Carro
E-MAIL: orlando.carro@ctis.com.br
DATA: 28/05/19 as 10:57

SUGESTÕES A AUDIÊNCIA PÚBLICA nº 01/2019 DA FUNDAÇÃO PARA O DESENVOLVIMENTO DA EDUCAÇÃO – FDE.

Prezados Senhores

Para possibilitar a ampla concorrência, com consequente possibilidade de redução de custos no certame, mantendo a qualidade do fornecimento pretendida pela FDE, sugerimos as alterações elencadas abaixo, no texto original do Anexo II – Especificações Técnicas – Projeto Técnico.

Caso estas sugestões não sejam aceitas, entendemos que a competitividade ficará restrita, prejudicando, assim, a busca de preços mais vantajosos para a administração com a mesma qualidade requerida.

1. Item 4 - Especificação Técnica dos Equipamentos e Serviços.

Texto original do TR

“O prazo para entrega, instalação e configuração dos equipamentos será de até 30 dias a contar da data de assinatura da Ordem de Fornecimento/Serviço.”

- Sugerimos aumentar o prazo de entrega para 90 dias, pois os prazos de importação e desembaraço são, normalmente, maiores do que 30 dias.

Texto com nossa sugestão em negrito:

“O prazo para entrega, instalação e configuração dos equipamentos será de até 90 dias a contar da data de assinatura da Ordem de Fornecimento/Serviço.”

R.: Caso o Access Point seja adquirido juntamente com o serviço de instalação/configuração o mesmo deverá ser entregue e instalado em no máximo até 60 dias da data da assinatura da Ordem de Fornecimento/Ordem de Serviços.
Caso o Access Point seja adquirido sem o serviço de instalação/configuração o mesmo deverá ser entregue em até 30 dias da data da assinatura da Ordem de Fornecimento.

2. Item 4.1.1 Condição de Fornecimento.

Para o item 4.1.1.2. sugerimos incluir no texto Controladora Wireless em Nuvem ou “on premisses” instalada em Data Center no Brasil.

Texto original do TR

4.1.1.2 – A configuração dos seus parâmetros operacionais, o gerenciamento das políticas de segurança e de radiofrequência devem ser gerenciadas por uma solução de Controladora Wireless em nuvem. Esta solução de controladora wireless em nuvem deverá ser do mesmo fabricante do ponto de acesso afim de garantir uma perfeita interoperabilidade.

Dessa forma o prazo passaria a ser:

Texto com nossa sugestão em negrito:

4.1.1.2 – A configuração dos seus parâmetros operacionais, o gerenciamento das políticas de segurança e de radiofrequência devem ser gerenciadas por uma solução de Controladora Wireless em nuvem ou “on premisses” instalada em Data Center no Brasil. Esta solução de controladora wireless em nuvem ouon premisses deverá ser do mesmo fabricante do ponto de acesso afim de garantir uma perfeita interoperabilidade.

Justificativa: O licitante poderá fornecer a(s) controladora(s) instaladas e custeadas pelo licitante em Data Center no Brasil, criando desta forma uma solução baseada em nuvem, como requer o FDE. Essa alteração irá permitir o posicionamento de fabricantes que hoje possuem uma solução on premisses mais aderente ao termo de referência.

R.: Nos estudos realizados pela FDE, pôde-se observar que para suportar uma demanda tão alta de access points e com escalabilidade, seria necessário um cluster de várias controladoras on premisse. Neste cenário haveria a necessidade de uma configuração mais complexa, dividindo por exemplo grupos de access point por grupos de controladoras. Perdendo assim a simplicidade na operacionalização e administração da rede WiFi.

Já no cenário de controladora em nuvem, pôde-se observar que para o access point se associar a controladora wifi basta uma conexão ativa com a internet, não havendo a necessidade de configurações extras no AP ou mesmo nos equipamentos de rede, como por exemplo, entradas de DNS e DHCP options. Este cenário também unifica software de gerenciamento wifi e funcionalidade de controladora wifi no mesmo portal, facilitando e simplificando a operacionalização e administração da rede.

4.1.2 Características Gerais.

3. Para o item 4.1.2.7 sugerimos incluir no texto “SAML ou similar”.

Texto original do TR

4.1.2.7 Deve implementar, localmente ou em conjunto com a solução de controladora Wireless em nuvem, Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Indentity Providers - IDP's) de terceiros.

Texto com nossa sugestão em negrito:

4.1.2.7 Deve implementar, localmente ou em conjunto com a solução de controladora Wireless em nuvem, Security Assertion Markup Language (SAML) ou similar, agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Indentity Providers - IDP's) de terceiros

R.: Conforme explicado em audiência publica o protocolo SAML poderá ser usado para autenticação dos usuários utilizando a base localizada na Microsoft ou no Google. Soluções que não estejam em conformidade com o protocolo SAML inviabilizará o uso desta funcionalidade com os provedores em questão. Entretanto, a FDE irá incluir o protocolo oauth2 como opção ao protocolo SAML, tendo em vista que este protocolo também é compatível com tais provedores de serviços.

4. Para o item 4.1.2.11 sugerimos alterar o texto para deixar mais aderente às boas práticas de mercado, pois a forma usada no mercado é o padrão IEEE 802.1X e em conjunto filtros de segurança L2-L7 para permitir a segmentação segura dos clientes.

Texto original do TR

4.1.2.11 Deve permitir a definição de endereços MAC para controle de acesso a rede WiFi.

Dessa forma o prazo passaria a ser:

4.1.2.11 Deve permitir o controle de acesso através do padrão IEEE 802.1X e em conjunto filtros de segurança L2-L7 para permitir a segmentação segura dos clientes para controle de acesso a rede WiFi.

R.: A FDE entende que a sugestão já está contemplada no termo de referência conforme os itens 4.1.2.8, 4.1.2.11 e 4.1.2.37.

5. No item 4.1.2.13. Incluir que se aceita um AP dedicado para a função de análise de espectro.

Texto original do TR

4.1.2.13 Deve localmente ou em conjuntos com a solução de controladora wireless em nuvem, implementar análise de espectro de RF em 2.4GHz e 5gHZ para identificação de outros pontos de acesso intrusos e não autorizados (rogues), além de interferências no canal habilitado no ponto de acesso e nos demais canais configurados na rede WiFi. A análise de espectro deve ser realizada de forma simultânea ao atendimento dos clientes do ponto de acesso, sem que estes sejam desconectados.

Dessa forma o prazo passaria a ser:

4.1.2.13 Deve localmente ou em conjuntos com a solução de controladora wireless em nuvem, implementar análise de espectro de RF em 2.4GHz e 5gHZ para identificação de outros pontos de acesso intrusos e não autorizados (rogues), além de interferências no canal habilitado no ponto de acesso e nos demais canais configurados na rede WiFi. A análise de espectro deve ser realizada de forma simultânea ao atendimento dos clientes do ponto de acesso, sem que estes sejam desconectados, sendo aceito um AP dedicado para a função de análise de espectro.

R.: Com o objetivo de ampliar a concorrência do certame e por entender que não terá prejuízos para a qualidade do projeto, abriu-se a possibilidade técnica de que esta funcionalidade seja atendida sem uma antena dedicada, mas de forma simultânea ao atendimento dos clientes wifi.

Considerar a possibilidade de um AP dedicado para esta função impossibilitaria o uso da análise de espectro em todos os ambientes, uma vez que um AP dedicado para análise de espectro em uma escola que possua 5 APs, por exemplo, cobriria somente os locais de alcance do sinal wifi do access point exclusivo para esta funcionalidade. Além disso haveria um custo extra de infraestrutura para instalação deste equipamento.

4.1.3 Funcionalidades da Solução de Controladora Wireless em nuvem.

6. 4.1.3.9. Sugerimos deixar genérico para permitir outras criptografias, como IPSec, por exemplo.

Texto original do TR

4.1.3.9 Deve empregar criptografia de dados TLS ou SSL no canal de comunicação com os pontos de acesso WiFi.

Texto com nossa sugestão em negrito

4.1.3.9 Deve empregar criptografia de dados TLS, SSL, IPSec ou similar, no canal de comunicação com os pontos de acesso WiFi.

R.: Será incluído no termo de referência o protocolo IPSec, uma vez que, a FDE entende que o mesmo não trará prejuízos a qualidade do projeto.

EMPRESA: Diretoria de Ensino Jundiaí
RESPONSÁVEL: Diego Roberto Cabral
E-MAIL: diego.cabral@educacao.sp.gov.br
DATA: 28/05/19 as 11:05

Bom dia,

Quem serão os responsáveis pela instalação da infraestrutura física (elétrica e rede) para instalação dos APs?

R.: Os responsáveis pela instalação de infraestrutura física (lógica e elétrica) será a Secretaria da Educação em conjunto da FDE com contratação de serviço a partir de Ata de Registro de Preços.

Vocês tem noção que há escolas com cabeamento precário (rede e elétrica)? Antes de instalar os APs esta infraestrutura será refeita?

R.: A Secretaria realizará a manutenção da infraestrutura onde for necessário, garantindo a segurança e a funcionalidade dos Access Points.

Tem escolas que estamos colocando SoniWall devido o Fortinet apresentar problemas e a empresa contratada não efetuar a troca. A infraestrutura dos APs foi pensada para este cenário? Ou todos os firewalls serão substituídos para atender esta demanda?

R.: As unidades escolares que estão atualmente em funcionamento com Firewall SonicWall serão atendidas através da nova Ata de Registro de Preços de Firewall e Switch para substituição de tais equipamentos. Para as escolas que contingencialmente estão funcionando com SonicWall, estas serão atendidos até a instalação do Access Point.

EMPRESA: Luach Teconologia
RESPONSÁVEL: Paulo Lima
E-MAIL: paulo.limas@hotmail.com
DATA: 28/05/19 as 11:05, 11:14, 11:28

OLá Pessoal!

1) Qual é seria a média de alunos por escola?

R.: A média atual gira em torno de 676 alunos por escola.

2) O tempo do atendimento para substituição de equipamento poderia contemplar a remessa via Sedex. Ou na localidade precisa ter um equipamento sobressalente?

R.: Não será necessário manter um equipamento sobressalente nas unidades escolares. O fornecedor deverá entregar e/ou fazer a substituição dos equipamentos de acordo com a modalidade de transporte que melhor lhe convier desde que o prazo determinado no edital seja devidamente cumprido.

3) A empresa prestadora dos serviços terá acesso a controladora para o suporte?

R.: Sim, o acesso será permitido.

4) Os equipamentos serão instalados nos corredores das salas ou dentro das salas de aula?

R.: O local de instalação ainda será definido, mas poderá ser em qualquer ambiente interno da unidade.

EMPRESA: CISCO
RESPONSÁVEL: Andre Luiz Gallon
E-MAIL: agallon@cisco.com
DATA: 28/05/19 as 11:13

Conforme apresentado em audiência publica na data de 28/Maio 2019, entendemos que segurança é um pre-requisito fundamental no projeto de conectividade Wi-Fi nas escolas. Isto posto, seria interessante aprofundar mais o debate sobre:

1 - Criptografia dos dados no canal de gerenciamento entre os Access Points e a Controladora Nuvem. Seria importante uma criptografia forte (AES256) com gerenciamento de chaves automotico feito pela controladora

R.: A FDE entende que as criptografias solicitadas no item 4.1.3.9 são suficientes para garantir uma segurança aceitável para o projeto. Também será incluído no item a possibilidade de atendimento utilizando o protocolo IPSEC.

2 - AP com suporte a Change Of Authorization (CoA) para autenticação dos usuários, permitindo assim revogação de acesso,

R.: A FDE entende que a solicitação de suporte ao RADIUS e ao 802.1x já são suficientes para atender as necessidades do projeto.

3 - AP com Radio dedicado para função de wIPS, sendo que esse wIPS deva receber automaticamente da nuvem as atualizações de assinaturas de ataques no Wi-Fi.

R.: A FDE entende que poucos players de mercado conseguiriam atender esta funcionalidade com radio dedicado. Sendo assim, esta questão foi endereçada no item 4.1.2.49, permitindo uma maior concorrência do certame e ao mesmo tempo atendendo às necessidades básicas do projeto.

4 - AP com capacidade de fazer traffic-shapping;
R.: A FDE entende que esta funcionalidade já é solicitada nos itens 4.1.2.9 e 4.1.2.45.

5 - AP que impossibilite troca do firmware para utilização como Stand-Alone. Isso impede que exista um comercio paralelo dessas antenas, roubo.
R.: A FDE entende que solicitar esta funcionalidade no AP, irá limitar a concorrência no certame. Entretanto, pensando justamente na segurança física do equipamento, é solicitado no item 4.1.1.4, um kit antifurto.

6 - Acesso a controladora nuvem feita por MFA.
R.: A FDE entende que para este projeto não há a necessidade de utilizar o MFA.

7 - Garantir criptografia para o acesso entre Captive Portal server (Nuvem) e o AP. Geralmente captive portals sao HTTP (aberto) e os dados que trafegaram nele precisam ser criptografamos,
R.: A FDE incluirá no texto do item 4.1.2.5 que o acesso ao Captive Portal seja via HTTPS.

8 - wIPS com mitigação de rogues AP
R.: A FDE entende que este recurso de mitigação de rogues AP já está sendo solicitado no item 4.1.2.13.

9 - Garantir que o AP tenha capacidade de operar com duas Vlans de gerencia, nao expondo assim o AP para Internet e também. Servidores AD e Radius.
R.: A FDE entende que um IP de gerência no AP é suficiente para atender às necessidades do projeto.

10 - Garantir que a nuvem seja segura (Anti-DDOS, auditoria de segurança feita por terceiros, certificação ISO27001.
R.: A FDE entende que solicitar a certificação ISO27001 trará mais segurança para a solução em nuvem. Sendo assim, será solicitado que a solução seja entregue em um ambiente com certificação ISO27001.

11- Auto-Provisionamento de certificado digital X.509 para os dispositivos, garantindo confianca nos dispositivos.

R.: A FDE entende que para este projeto não há a necessidade desta funcionalidade.

Entendemos também que preparação para o futuro é um pre-requisito fundamental no projeto Isto posto, seria interessante aprofundar mais o debate sobre:

1 - AP pronto para operar com BLE (bluetooth) para futuros projetos de IOT, RFID, asset tracking e aplicativos de smartphones que sejam interativos.
R.: A FDE entende que para este projeto não há a necessidade desta funcionalidade.

2 - Mapa de Calor, Analytics.
R.: A FDE entende que para este projeto não há a necessidade desta funcionalidade.

3 - Radios com capacidade 3x3. Entendemos que os 2x2 solicitados tem uma seria limitação de performance quando instalados em ambientes com alta concentração de dispositivos. (Salas de aula.)
R.: A FDE entende que um AP 2x2:2 atenderá as necessidades do projeto. Entretanto as características técnicas solicitadas no certame referem-se à requisitos mínimos, podendo ser ofertados configurações superiores ao solicitado.

4 - detalhamento da alta-disponibilidade que a nuvem deve contemplar. Data Centers duplicados, links Internet duplicados... etc
R.: A FDE entende que ao solicitar o serviço em nuvem, automaticamente estará coberta com algumas redundâncias básicas para o perfeito funcionamento do projeto. Entretanto será solicitado que a controladora em nuvem possua um uptime de 99,6% ao ano.

EMPRESA: Diretoria de Ensino Região de Pindamonhangaba
RESPONSÁVEL: Tiago Nazaré Costa
E-MAIL: depdmnit@educacao.sp.gov.br
DATA: 28/05/19 as 11:17

Prezados senhores, bom dia!

Gostaríamos de esclarecer algumas dúvidas referente à Audiência Pública para implantação de Wi-fi nas escolas.

1) Algumas escolas já enfrentam dificuldades com a largura de banda na rede cabeada. Nesse sentido, há alguma intenção de se rever a velocidade das unidades para uma possível expansão?
R.: A Secretaria da Educação já está estudando um aumento da banda disponibilizada na rede INTRAGOV. Lembrando que não haverá downgrade da mesma. Os últimos dados sobre consumo da rede balizarão o upgrade para as escolas.

2) Atualmente, a equipe do NIT fica limitado quanto alguns procedimentos para testes e configurações nos AP's existentes nas escolas integrais. Dessa forma, nas visitas técnicas tanto os Analistas da Prodesp, quanto os Analistas de Tecnologia entram em contato com a FDE para realizar as operações em conjunto. O grande problema nisso, é que algumas vezes as linhas estão congestionadas, o espaço da escola para acesso ao AP é dificultoso, etc., resultando em procedimentos demorados. Seguindo essa premissa, como seria feito esse atendimento? Seria possível disponibilizar um acesso ao NIT para monitorar/configurar o funcionamento dos AP's para agilizar e facilitar o atendimento às escolas?
R.: O projeto prevê uma configuração simples, automática e padronizada dos APs, sem a necessidade de intervenção do técnico no local. Neste primeiro momento não está previsto liberar acesso ao gerenciamento dos APs.

3) Como o projeto irá tratar da compatibilidade com os diversos tipos de sistemas operacionais? Hoje, em ambientes com wi-fi, muitas vezes percebemos que a controladora não direciona o dispositivo para área de autenticação (dependendo da versão do android, por exemplo), dificultando, e algumas vezes até impedindo, o uso da rede wireless.
R.: A autenticação que será utilizada no projeto, será através de browser, o que simplifica e aumenta a compatibilidade com dispositivos que possuem um browser integrado ao seu sistema operacional. Além disso, casos isolados poderão ser tratados de forma diferente.

4) A implantação de wi-fi nas unidades será integrado ao Projeto Educação Conectada ou será um projeto isolado?
R.: O projeto de implantação do WiFi está integrado ao Projeto Educação Conectada, e ainda conta com recursos próprios do Governo Estadual para sua realização.

5) Como será controlado a largura de banda da unidade dedicado exclusivamente ao wi-fi? Haverá restrições e monitoramento de acesso à conteúdo indevido?
R.: Neste primeiro momento não haverá controle de largura de banda para a rede do WIFI, entretanto havendo a necessidade, alguns controles poderão ser aplicados. Quanto às restrições, o tratamento do acesso da rede WIFI será o mesmo já feito na rede cabeada.

EMPRESA: Compwire
RESPONSÁVEL: Daniel Lima
E-MAIL: daniel.lima@compwire.com.br
DATA: 28/05/19 as 11:25

Prezados senhores.

Solicitamos esclarecer:

Com relação a citado na apresentação:

Sobre o item Statefull Firewall, que haverá facilidade de gestão das políticas de Firewall para cada Access Point além da proteção para aplicações diretamente em cada Access Point.

Entendemos que pelo documento apresentado haverá: 3 SSIDs por escola x 5000 escolas = 15000 SSID. Está correto nosso entendimento?
R.: Entendimento incorreto. Os SSIDs serão padronizados, ou seja, os mesmos SSIDs serão divulgados em todas as unidades.

Quem será o default gateway das vlans (vlan admin - vlan apoio - vlan ped)?
R:. Vlan admin e Vlan Ped default gateway o firewall. No caso da vlan apoio, o gateway dos clientes WiFi será o Access point, e o gateway do Access Point será o firewall.

Quem será o default Gateway de cada SSID de cada Escola?
R.: Será o AP, por esta razão, a operação em modo NAT é solicitada.

Como será a proteção inter vlan da rede Cabeada para a Rede Wireless?
R.: Através da funcionalidade de firewall stateful e controle de aplicação.

Pelo informado na apresentação, atualmente cada escola possui um firewall fazendo a proteção do trafego de entrada e trafego interno que faz a segregação e proteção das redes? Está correto nosso entendimento?
R.: Entendimento correto. O Firewall da escola controla o tráfego entre os seguimentos de rede cabeada. Exemplificando, a rede pedagógica não possui permissão de acesso com a rede administrativa.

EMPRESA: HPE

RESPONSÁVEL: Julianna Knauer

E-MAIL: juliannaknauer@hpe.com

DATA: 28/05/19 as 11:36

Consulta Publica FDE

Sugestão 01

Sugerimos que é fundamental garantir a continuidade de operação da rede, mesmo no caso de encerramento das subscrições da solução de gerência em nuvem, permitindo a administração local da solução neste caso. Caso a solução ofertada não possua este recurso, sugerimos que a contratada inclua mais 2 anos aos custos para que a solução continue operando sem restrições, mesmo após a finalização da garantia e licenciamento.

R.: Em pesquisa realizada pela FDE pode-se observar que 60 meses de licenciamento em nuvem era o mais comum para as empresas. Desta forma a FDE entende que manter 60 meses de licenciamento para controladora em nuvem garante ampla concorrência do mercado e não oferece ônus negativo para o projeto.

Sugestão 02

Sugerimos que os Access Points propostos devem possuir a funcionalidade de IP reputation, permitindo a filtragem de blocos de endereços IP maliciosos que podem conter ameaças como botnets e phishing. Este recurso é importante para evitar a sobrecarga do firewall existente na escola, o qual vale lembrar é um dispositivo para uma arquitetura small size.

R.: A FDE entende, que para este projeto não há necessidade desta funcionalidade porque ela já é tratada no data center da FDE.

Sugestão 03

Sugerimos que a solução de rede Wireless deve proporcionar ferramentas que permita identificar problemas nas conexões do usuário, realizando a medição da taxa falhas em serviços essenciais para a comunicação dos usuários como Associação, Autenticação DHCP e DNS e mostrando o resultado em um dashboard ou gráfico para rápida identificação.

R.: A FDE entende que para este projeto não há a necessidade desta funcionalidade.

Sugestão 04

Sugerimos que a solução de rede wireless deve possuir uma funcionalidade de analytics que permita analisar o padrão de tráfego dos usuários, identificando quantos usuários passaram por um determinado local, mesmo que não tenham se associado à rede Wi-Fi e quanto tempo ficaram, em média, no local. Esta forma é possível extrair informações úteis sobre a utilização dos espaços, auxiliando no planejamento.

R.: A FDE entende que para este projeto não há a necessidade desta funcionalidade.

Sugestão 05

Sugerimos que é fundamental que o Acess Point proposto possua, além dos rádios Wi-Fi, rádio BLE (Bluetooth Low Energy) para proporcionar soluções futuras de localização, que frequentemente utilizam este padrão, para localizar ativos através de tags bluetooth ou usuários através de aplicações em dispositivos móveis que utilizam bluetooth.

R.: A FDE entende que para este projeto não há a necessidade desta funcionalidade.

Sugestão 06

Deve permitir conexão entre APs sem a necessidade de conexão cabeada, implementando assim uma rede padrão mesh

R.: A FDE entende que a inclusão do padrão mesh não trará prejuízos para o projeto. Sendo assim, o texto será inserido no item 4.1.2.28.

Sugestão 07

Sugerimos pela quantidade de usuários o suporte de no mínimo mais que 50 usuários Guest por AP

R.: A FDE entende que esta questão está endereçada no item 4.1.2.12.

Sugestão 08

Deve suportar multi-Tenant (MSP)

R.: A FDE entende que para este projeto não há a necessidade desta funcionalidade.

Sugestão 09

Sugerimos suporte a categorização Web para classificação e aplicação de políticas de firewall.

R.: A FDE entende que para este projeto não há a necessidade desta funcionalidade.

Sugestão 10

Sugerimos suporte a análise de spectro para identificar fontes de interferência, como monitores de bebê, dispositivos Bluetooth, telefones sem fio digitais (apenas na banda de frequência de 2,4GHz), transmissores de áudio sem fio (tanto nas bandas de frequência de 2,4GHz quanto 5GHz), controladores de jogos sem fio e micro-ondas.

R.: A FDE entende que esta questão já está sendo endereçada no item 4.1.2.13.

Sugestão 11

Sugerimos suporte a Zero Touch Provisioning (ZTP) solução permite a autoconfiguração dos APs no primeiro boot sem requerer qualquer intervenção do administrador. Essa funcionalidade facilita enormemente a instalação a ser feita pela equipe da própria unidade ou das subsecretarias.

Esta tecnologia está disponível em mais de um fabricante.

R.: A FDE entende que no modelo de controladora em nuvem esta funcionalidade ou funcionalidade similar já é embarcada na solução em questão, ou seja, ao conectar o access point com conexão para a internet, o access point se registra na controladora e recebe as configurações.

Sugestão 12

Sugerimos por exemplo uma quantidade mínima de 1.500 unidades de APs outdoor.

Caso não seja licitado no momento modelos Outdoors o FDE ficará limitado no futuro à compra do fornecedor vencedor dos APs Indoors (caso a licitação seja somente de Aps Indoors).

O instrumento registro de preço permite que se coloque uma quantidade estimada de outdoors sem associar uma obrigação de compra de tal modelo e ou na totalidade registrada.

R.: A FDE entende que para este momento não será necessário APs outdoor.

Sugestão 13

Em relação aos serviços que serão realizados pela equipe da FDE como fica a garantia on site. A troca/configuração dos APs será de responsabilidade da contratada ou da FDE?

R.: Conforme descrito no item 6.1.7 a troca é de responsabilidade da contratada.

Sugestão 14

Serão indicadas as escolas que será feita a instalação do AP pela contratada.

R.: Qualquer escola pública estatual de São Paulo poderá receber a instalação dos access points.

EMPRESA: Multilaser

RESPONSÁVEL: Marcel Reno

E-MAIL: marcel.reno@multilaser.com.br

DATA: 28/05/19 as 11:39

Srs(a),

Em pesquisa realizada nas escolas municipais e estaduais que já possuem rede AP para acesso a internet, identificamos que na prática, aproximadamente 2 a 3 SSIDs são utilizados, sendo que em pouquíssimos casos utilizam-se 4 SSIDs.

Considerando essa prática comum junto as escolas, as novas tecnologias de AP estão sendo desenvolvidas com um número menor de SSIDs, sendo 4 o númeo mínimo aceitável.

Isso traz certa economia aos cofres públicos e não limitaria a competitividade da concorrência, além de manter o ível técnico do produto, obtendo 4 SSIDs livres para o devido agrupamento como pro exemplo: professores, alunos 1° ao 5° ano, alunos 6° ao 9° e assim por diante.

Vale ressaltar que essa economia pode permitir o aumento do quantitativo, que traria um beneficio bem maior que um maior numero de SSID.

Ressaltamos que mesmo com mínimo 4 SSID, os fabricantes que ainda possuem 8 ou 16 SSIDs poderiam participar, do contrário podemos ter impuganções e/ou questionamentos e número reduzido de licitantes.

R.: Em pesquisas realizadas pela FDE pode-se observar que a grande maioria dos Access Points contam com a capacidade de 8 SSIDs. Além disso a quantidade mínima de 8 SSIDs é adequada para o atendimento da demanda atual e futura da rede.

EMPRESA: Bedu Tech
RESPONSÁVEL: Renato Rappoli
E-MAIL: rrappoli@bedu.tech
DATA: 28/05/19 as 11:57

Deve ser fornecido kit antifurto “Kensington security lock” ou equivalente com a finalidade de evitar o furto do equipamento.
para
Deve ser instalado com mecanismo ou sistema adicional de fixação antifurto com a finalidade de evitar o furto do equipamento.
Motivo: O texto diz que o AP deve possuir mecanismo antifurto mas não diz como será instalado, o novo texto é genérico mas garante que haverá um dispositivo adicional instalado.
R.: A FDE entende que conforme o item 5.1.10 já é solicitado que o AP seja instalado juntamente com o kit antifurto.

Deve implementar recursos de firewall stateful.
para
Deve implementar recursos de firewall stateful em camada 7.
Motivo: O termo firewall stateful é genérico e permite firewalls de cada 3 ou 4 apenas. A solução atual são firewalls de camada 7 que garantam segurança por aplicação.
R.: Conforme definição do IETF, trata-se de um processo de encaminhamento ou rejeição de tráfego com base no conteúdo de uma tabela de estado, ou seja, não existe atendimento genérico à funcionalidade de firewall stateful. Portanto, a FDE entende que seria impossível o atendimento desta funcionalidade somente na camada 3. Quanto às camadas superiores de aplicação, já está endereçado no item 4.1.2.8 onde é solicitado a implementação de controle de aplicação.
Deve possuir antenas internas integradas (embutidas) com ganho de, no mínimo, 3.8 dBi para 2,4 GHz e 3.8 dBi para 5 GHz.
para:
Deve possuir antenas internas integradas (embutidas) com ganho de, no mínimo, 5 dBi para 2,4 GHz e 5 dBi para 5 GHz.
Motivo: 3.8dbi é uma potência de antena muito baixa para os tipos de construção das escolas.

R.: A FDE entende que uma antena de 3.8 dBi atenderá às necessidades do projeto. Entretanto as características técnicas solicitadas no certame, referem-se à requisitos mínimos, podendo ser ofertados configurações superiores ao solicitado.

Deve possuir suporte a CSD ou CDD.
Remover item.
Motivo: Protocolos depreciados, produtos atuais não possuem mais suporte.
R.: A FDE entende que estas funcionalidades contribuem para melhorar o sinal do Wifi. Entretanto também será aceito a funcionalidade de MRC como opção para atender este projeto.

Deve implementar o protocolo NTP (Network Time Protocol) ou o protocolo SNTP (Simple Network Time Protocol) em modo cliente.
para:
Deve implementar o protocolo NTP (Network Time Protocol) ou o protocolo SNTP (Simple Network Time Protocol) em modo cliente ou através da controladora em nuvem.
Motivo: Os APs Meraki atualizam o horário pela cloud e a cloud atualiza por NTP.
R.: A FDE entende que a inclusão do texto proposto não trará prejuízos para o projeto. Sendo assim, o texto será inserido no item 4.1.2.43.

Permitir habilitar e desabilitar a divulgação do SSID.
para:
Permitir habilitar e desabilitar a divulgação do SSID com possibilidade de agendamento.
Motivo: O agendamento permitirá a FDE restringir a divulgação dos SSIDs somente nos horários de uso, evitando o uso indevido da rede e eventuais tentativas de invasão em horários alternativos (madrugadas e finais de semana).
R.: A FDE entende que esta funcionalidade já está sendo solicitada no item 4.1.3.4.

Deve possuir capacidade para operação em modo "repetidor", permitindo a comunicação entre pontos de acesso WiFi sem a necessidade de cabeamento adicional permitindo desta forma o atendimento de usuários em locais isolados da localidade.
para:
Deve possuir capacidade para operação em modo "repetidor" ou “mesh”, permitindo a comunicação entre pontos de acesso WiFi sem a necessidade de cabeamento adicional permitindo desta forma o atendimento de usuários em locais isolados da localidade.

Motivo: a instalação de APs em modo mesh pode ser utilizada em unidades maiores para reduzir os custos de cabeamento e infraestrutura sem as restrição que o modo repetidor possui.
R.: A FDE entende que a inclusão do texto proposto não trará prejuízos para o projeto. Sendo assim, o texto será inserido no item 4.1.2.28.

Deve possuir feature de ser utilizado como equipamento de Site Survey;
Motivo: As realocações de pontos de acesso e ampliações futuras serão constantes e a FDE irá precisar desta funcionalidade para definir os locais de instalação.
R.: A FDE entende que para este projeto não há a necessidade desta funcionalidade.

CONTROLADORA EM NUVEM incluir

A solução de controladora em nuvem (e solução de autenticação de dispositivos) deverá ser do mesmo fabricante do ponto de acesso a fim de garantir uma perfeita interoperabilidade;
Motivo: evitar soluções adaptadas e sem garantia de funcionamento ao longo do tempo quando houverem atualizações dos pontos de acesso.
R.: A FDE entende que para este projeto a utilização da solução RADIUS da FDE juntamente com os protocolos (LDAP, SAML ou OAUTH2) solicitados no termo de referencia são suficientes para atendimento da demanda.

Mapa de calor
Motivo: é imprescindível que uma solução consiga identificar a cobertura WIFI de cada unidade permitindo planejamento de expansões de cobertura, análise de utilização por região e troubleshooting em unidades com chamados recorrentes.
R.: A FDE entende que para este projeto não há a necessidade desta funcionalidade.

Informações de destinos acessados;
Para:
Informações de aplicações acessadas;
Motivo: o termo “destino” dá margem para interpretações a solução ofertada pode mostrar apenas os endereços IP quando o objetivo desta funcionalidade é identificar quais aplicações os usuários estão acessando.
R.: A FDE entende que o suporte para identificação da aplicação já está sendo endereçado no item 4.1.3.16.

SOLUÇÃO DE AUTENTICAÇÃO DE DISPOSITIVOS E CONTROLE DE ACESSO
Motivo: O uso de uma base LDAP para autenticação dos dispositivos é complexa e oferece poucos mecanismos de rastreabilidade e identificação de dispositivos e usuários. Uma solução de controle de acesso (NAC) permite a aplicação de perfis distintos, autenticação de visitantes e uma série de recursos essenciais para evitar que a rede seja utilizada indevidamente e possa incorrer um infrações ao marco civil.

Sugestão de spec
SOLUÇÃO DE AUTENTICAÇÃO DE DISPOSITIVOS (CONTROLE DE ACESSO)

Deve ser uma solução composta por software, dedicada para serviços de autenticação, autorização e contabilidade, também conhecidos como AAA (Authentication, Authorization and Accounting);

O equipamento deve ser fornecido na forma de software (máquina virtual) ou equipamento appliance, para uso exclusivo da solução de autenticação;

Não serão aceitas soluções de software(s) e/ou serviço de autenticação baseado(s) através de nuvem (cloud);

No caso de fornecimento de máquina virtual, a responsabilidade do fornecimento do servidor físico onde será instalada a solução é da CONTRATANTE;

No caso de fornecimento de Dispositivo Físico:

Deve ser totalmente construído em hardware e software dedicado para esta função;

Deve possuir, no mínimo, 2 (duas) interfaces de rede Ethernet 1000Base-T ou 10G;

Deve possuir fontes de alimentação internas ao gabinete, redundantes e hot pluggable, operando automaticamente em tensões de 100 VAC a 240 VAC e em frequência de 60 Hz;

Deve ser compatível com rack de 19 polegadas

Deve fornecer licenças de uso permanente (perpétua) de todos os softwares que compõem a solução proposta, em suas versões mais recentes e sem previsão de descontinuidade até a data de entrega da proposta;

O licenciamento da solução completa deve permitir a continuidade do uso pela CONTRATANTE em caráter permanente, mesmo após o término do contrato, inclusive sem restrições à futura utilização para atendimento a eventuais novas demandas;

Deve implementar a porção servidor da arquitetura AAA (Authentication, Authorization and Accounting) para controle de acesso a serviços de rede, contemplando os seguintes modelos de conectividade:

Conexão 802.1x através de switches (LAN);

Conexão 802.1x através de pontos de acesso sem fio (WLAN);

A solução deve ser do mesmo fabricante dos Acess Points e Controladora Web, porem com suporte multi-vendor, operando com soluções de outros fabricantes que utilizem o protocolo RADIUS;

A solução deve permitir integração com base de usuários Windows AD (Active Directory), LDAP (Lightweight Directory Access Protocol) e banco de dados SQL (Structured Query Language) para autenticação de usuários;

Deve ser possível definir os grupos de usuários internamente ao Servidor RADIUS, com suporte à definição local de pares usuário/senha;

O equipamento deve ter capacidade para suportar os serviços AAA para, pelo menos, 20.000 (vinte mil) dispositivos (PCs, tablets, smartphones, etc.) conectados simultaneamente;

Deve estar licenciado para autenticar, no mínimo, um total de 5.000 (cinco mil) dispositivos simultâneos;

Deve suportar a configuração redundante em alta disponibilidade utilizando um outro equipamento de mesmo modelo;

Deve permitir a operação como Proxy RADIUS, encaminhando as requisições a outros servidores RADIUS para autenticação;

Deve implementar IPv4 e IPv6;

Deve ser possível atribuir VLANs após resultado dos processos de autenticação/autorização em conexões 802.1x;

A solução deverá suportar atributos RADIUS definidos pelo IETF, inclusive atributos específicos de outros fabricantes de equipamentos IP;

Deve implementar o bloqueio de contas de usuários após um número pré-definido de erros na autenticação;

Deve possibilitar restrições de acesso tendo como base o dia da semana e a hora, podendo impedir conexões em determinados dias ou horários;

Deve permitir a definição de número máximo de conexões simultâneas dos usuários, sendo possível limitar esse valor a apenas um acesso;

Deve permitir a adição e deleção e substituição de atributos de usuários, grupos e perfis;

Deve permitir segmentação de clientes em grupos;

Possuir templates para criação de perfis de usuários e grupos;

Deve permitir a criação de políticas baseadas em grupos e em usuários;

Deve permitir a criação de políticas baseadas em regras com condições do tipo localidade, horário, data, quotas e tipo de acesso;

Deve permitir a integração de política de trocas periódicas de senhas para dispositivos integrados em domínio Microsoft Windows;

Deve permitir desabilitar automaticamente a conta do usuário após excesso de tentativas com erro;

Deve permitir desabilitar automaticamente a conta em data específica;

Deve implementar, no mínimo os seguintes relatórios pré-definidos de utilização dos serviços de controle de acesso:
Usuários autenticados com sucesso;

Falhas de autenticação;

Radius accounting;

Deve implementar SNMP (Simple Network Management Protocol) versões 2 ou 2c e 3;

Deve implementar o protocolo NTP (Network Time Protocol) ou o protocolo SNTP (Simple Network Time Protocol);

Deve implementar SSH ou PowerShell remote ou gerência gráfica;

Autenticação de visitantes:

Deve possuir portal (Captive Portal) para acesso de visitantes em plataformas via web e específicas para smartfones e tablets;

Deve permitir a customização (logos, banners, etc) destes portais para prover interfaces amigáveis de acesso;

Permitir realização de login por meio de redes sociais (social login) de pelo menos rede Facebook ;

Deve possibilitar criação de regras de detecção de ameaças e correlacionar todos os dispositivos gerenciados;

Permitir a configuração de credenciais de acesso de visitantes oriundos de: texto SMS, e-mail e impressão;

Possuir mecanismos de se realizar o auto cadastro (self-registration) para criação de credenciais de acesso por parte do próprio visitante sem a utilização do sistema autenticação;

O licenciamento a ser fornecido deve permitir, no mínimo, 5000 (cinco mil) dispositivos específicos para acesso de visitantes;

Deverá ser fornecida, para cada Software de Gerenciamento, garantia estendida do fabricante de, no mínimo, 05 (cinco) anos, com SLA de 8x5xNBD (próximo dia útil) ou superior contados a partir da data da emissão do Termo de Recebimento e Aceitação Definitivo pelo CONTRATANTE;

Deverá ser permitida à CONTRATANTE a abertura de chamados direto no fabricante;

O Software de Gerenciamento deverá vir acompanhado de todas as licenças e softwares necessários para atender as especificações acima, sem prazo para expirar, fazendo com que os equipamentos continuem operacionais com todas as funcionalidades descritas neste objeto, mesmo após o término do período de suporte ou garantia. Os upgrades dentro do prazo de garantia devem estar contemplados nesta proposta;

Os equipamentos ofertados deverão ser novos e com embalagem do fabricante. Não serão aceitos equipamentos vindos de reparos, recondicionados e/ou outra forma que demonstre que estes tiveram uso anterior;

A solução ofertada deverá ser do mesmo fabricante da controladora em nuvem e dos pontos de acesso afim de garantir total interoperabilidade;

O equipamento e/ou software de autenticação ofertado deverá estar em linha de desenvolvimento e suporte dentro do fabricante. Não será aceito equipamento que se encontra descontinuado e/ou que recebeu notificação de final de venda (EOS – End of Sale) no respectivo sítio da Internet do fabricante;
R.: A FDE entende que para este projeto não há a necessidade desta funcionalidade.