Fernandópolis, 06 de Novembro de 2024.

PROJETO FIREWALL TIPO Roteador Ubiquiti Unifi Dream Machine Pro UDM-PRO-BR

A/C.: Camara Municipal de Indiaporã

DESCRIÇÃO DO OBJETO
● O firewall deverá desempenhar prevenção de acessos não autorizados à rede, garantindo a integridade, confidencialidade e disponibilidade dos dados e sistemas, com funcionalidades de filtragem de tráfego, detecção e prevenção de intrusões (IDS/IPS), proteção contra malware e vírus, VPN integrada, segmentação de rede e gerenciamento centralizado, atualizações e firmware redundância de links, compatibilidade com IPV6, bloqueio de sites, captive portal e alerta de links através de aplicativo de comunicação por mensagens;
● Todos os equipamentos necessários para o fornecimento da solução deverão ser fornecidos pela Contratada, através de comodato;
● A empresa contratada deverá fornecer e gerenciar dispositivos de segurança, efetuar manutenção preventiva e corretiva, e ainda, fornecer através de comodato, todos os equipamentos necessários para implantação e funcionamento da solução, inclusive providenciar a proteção de todos os equipamentos (hardwares que compõem o sistema) através da instalação de nobreak e equipamento de monitoramento deenergia, que também serão disponibilizados à Contratante através de comodato;
● O firewall deverá filtrar todo o tráfego de entrada e saída, permitindo apenas o tráfego autorizado com base em políticas de segurança predefinidas;
● Deverá identificar e bloquear tentativas de intrusão em tempo real. Como padrão todas as portas mais vulneráveis possuem um sistema de detecção inteligente, caso um IP de origem tentar o acesso por 3 vezes na mesma porta ou em portas diferentes automaticamente esse IP ficará bloqueado por 14 dias;
● Deverá inspecionar todos conteúdos, para detectar e bloquear ameaças de malware e vírus; Permitir conexões seguras para funcionários remotos. Para evitar a abertura de portas a forma mais segura de conexão remota é por VPN. Sendo que o responsável da Câmara Municipal definirá quem vai acessar, e esse acesso poderá ser monitorado ou bloqueado de acordo com a sua decisão. Sempre o log de última conexão deverá estar disponível;
● Deverá contar com recursos que visam facilitar a administração e monitoramento da segurança de toda a rede. Podendo subdividir redes, tais como redes de clientes separada totalmente por VLAN de uma rede administrativa. Assim impossibilitando acessos indevidos à estrutura interna de servidores e computadores.
● Deverá manter as definições de segurança e firmware do equipamento de firewall atualizadas para proteção contra novas ameaças emergentes.
● Além de proteção, o sistema firewall também deverá ter disponibilidade de monitoramento de Links de internet, sendo que caso o link principal venha a ficar indisponível, automaticamente o link secundário deverá entrar em ação, garantindo assim a maior disponibilidade possível de internet sem precisar de nenhuma intervenção.
● Junto com o monitoramento de links também deverá ser fornecido alertas por meio do aplicativo de comunicação por mensagens (aplicativos já existentes e de uso comum), quando algum link vier a falhar uma mensagem é enviada no aplicativo de mensagens, para que o responsável possa entrar em contato com o provedor de internet, para que o mesmo, possa realizar o reparo.

● O sistema de firewall deverá contar com a adoção em massa de IPV6, pelos provedores, sendo imprescindível que o firewall também seja compatível, principalmente pelo motivo de que cada dispositivo na rede receber um endereço de IP válido, que podem ser acessados de qualquer lugar do mundo.
● Deve contar com o recurso de realizar bloqueio de sites, tais como redes sociais, sites de download e URLS de sites de anúncios, garantindo um controle otimizado de rede, melhor aproveitamento da banda disponível e ajudando a impedir instalações de aplicativos indesejados nos computadores.
● Possibilidade de oferecer acesso à internet para visitantes, forçando a realização de um cadastro prévio, para limitar o tempo de uso e em caso de ordem judicial seja possível identificar o usuário.
● O sistema de firewall deverá oferecer proteção de classe empresarial/corporativa, garantindo que a rede esteja segura contra todas possíveis ameaças, inclusive, as ameaças mais recentes.
● O serviço de firewall gerenciado, deverá oferecer recursos visando a não necessidade de se preocupar com a configuração, manutenção e atualizações do firewall, economizando tempo e recursos internos.
● Deverá contar com controle de aplicativos que visem ajudar a evitar o uso improdutivo da rede, aumentando a produtividade dos funcionários.
● Os equipamentos utilizados para instalação do firewall (na sede da contratante) deverão estar conectados a nobreak e equipamento de monitoramento de energia, sendo que todos os equipamentos necessários à prestação do serviço, deverão ser disponibilizados pela contratada na modalidade de comodato.
● Todos os recursos necessários para instalação de equipamentos, configurações e implantação de demais recursos utilizados no sistema, deverão correr por conta da contratada, incluindo pessoal técnico, equipamentos, ferramentas e demais insumos.
● Os equipamentos permanentes necessários ao funcionamento do sistema de segurança serão fornecidos pela contratada na modalidade de comodato, durante toda a vigência do contrato, e deverão ser atualizados e/ou substituídos sempre que necessário, visando garantir a proteção contra novas ameaças que por ventura, venham a existir.
● Quando da interrupção dos serviços por ocorrência de problemas técnicos ou defeitos físicos, a Contratada deverá realizar o atendimento para as devidas manutenções corretivas destes, dentro do prazo de no máximo 4 horas, a contar do registro da chamada técnica (notificação por parte da Contratante), mesmo quando implicar na substituição parcial ou total dos ativos da rede.
● Os atendimentos para manutenções corretivas, em se tratando de problemas físicos nos equipamentos que compõem o sistema, deverão exclusivamente ser realizados presencialmente por técnicos da contratada. Eventualmente, quando se tratar de problemas relacionados a atualizações ou parametrizações para correção de problemas na configuração do sistema, poderão ser realizados remotamente, desde que não necessitem da intervenção e/ou participação local de funcionários da contratante para auxiliar na correção dos eventuais problemas.
● A contratada deverá ainda, manter um cronograma de manutenção preventiva e atualização dos equipamentos e demais recursos tecnológicos utilizados na solução. Isso inclui a implementação de ferramentas que permitam o monitoramento em tempo integral do sistema, e ainda, verificações regulares de integridade, com frequência mínima de uma vez por mês, para assegurar o perfeito funcionamento do sistema. No caso da necessidade de atualizações para reforçar a segurança contra novas ameaças, tanto no atendimento presencial quanto no remoto, a Contratada seguirá o mesmo critério de prazo estabelecido no parágrafo anterior (Atendimento Técnico).
● A Contratada não realizará em hipótese alguma, qualquer tipo de cobrança por atendimentos para manutenções corretivas ou preventivas, tampouco, pelos serviços de atualizações ou substituição parcial ou total dos equipamentos (ativos permanentes usados no sistema) e fornecidos através de comodato à Contratante.
● Para atendimento de chamados relacionados à problemas de funcionamento do sistema, a Contratada deverá estar disponível durante o horário comercial, para ligações telefônicas, reuniões, e-mails e deverá ter um telefone de plantão para acionamentos em caso de urgência/emergência.

● A Contratada não terá permissão para terceirizar nenhum dos serviços mencionados neste termo de referência. Todos os atendimentos para manutenções corretivas, preventivas, atualizações e substituições parciais ou totais dos equipamentos deverão ser realizados exclusivamente por técnicos próprios da Contratada. Isso garante um controle efetivo sobre a qualidade e o cumprimento dos prazos estabelecidos, mantendo a integridade e a eficiência dos serviços prestados à contratante.

● O sistema de firewall, fornecido pela Contratada é projetado para garantir a segurança de acesso e dos dados da Contratante.

● A Contratante não terá acesso às configurações do sistema. Tais configurações e parametrizações serão realizadas exclusivamente por técnicos da Contratada, mediante solicitação prévia dos representantes da Contratante.

QTD	CLIENTE	Vaor Mensal	Valor Anual
12	CAMARA MUNICIPAL DE INDIAPORÃ	**R$ 1.500,00**	**R$ 18.000,00**

Franslei Thiago Izeli
E-mail: solution@solutiondatacenter.com
CPF: 218.110.508-16 - RG: 32.716.548-0

SOLUTION DATA CENTER LTDA
CNPJ: 27.081.922/0001-27 - IE: 304.099.351.115
RUA: SÃO PAULO, 1726 - ANDAR 1 - SALA 13
FERNANDOPOLIS, SP - CEP: 15600-058 - FONE: 17-996355277

JUSTIFICATIVA PARA CONTRATAÇÃO DE SISTEMA DE FIREWALL PELA CAMARA MUNICIPAL DE INDIAPORÃ

Em um cenário cada vez mais digitalizado, a gestão eficiente de informações torna-se crucial para o funcionamento adequado de órgãos públicos. A crescente quantidade de dados digitais manipulados diariamente demanda não apenas a adoção, mas a otimização de ferramentas que garantam a integridade, confidencialidade e disponibilidade dessas informações. Nesse contexto, a justificativa para a contratação de um sistema de firewall robusto em um órgão público é fundamentada em diversos aspectos.

A segurança da informação é um princípio que deve ser priorizado principalmente na administração pública. Dados sensíveis e estratégicos estão constantemente sob ameaça de perda, seja por falhas técnicas, ataques cibernéticos ou desastres naturais. A implementação de um firewall confiável é imperativa, atuando como uma barreira de proteção contra ameaças cibernéticas, controlando o tráfego de dados e impedindo acessos não autorizados. Isso é essencial para resguardar a integridade das informações, evitar vazamentos de dados e proteger os sistemas contra ataques maliciosos.

Da mesma forma, a necessidade de um sistema de firewall confiável é imperativa. O firewall atua como uma barreira de proteção contra ameaças cibernéticas, controlando o tráfego de dados e impedindo acessos não autorizados. Isso é essencial para resguardar a integridade das informações, evitar vazamentos de dados e proteger os sistemas contra ataques maliciosos. A utilização de um sistema de firewall eficiente proporciona uma abordagem abrangente para a segurança das informações e dados do Município.

Além disso, a implementação de um firewall reduz significativamente a exposição a riscos provenientes de atividades humanas não intencionais ou intencionais. Controles de segurança avançados contribuem para a prevenção de falhas, garantindo a integridade dos dados armazenados e processados pelos setores da Câmara.

A otimização de recursos também é um fator relevante na adoção dessa solução. A eficiência na proteção contra ameaças cibernéticas preserva a produtividade e contribui para a economia de recursos financeiros e humanos que poderiam ser direcionados para outras áreas prioritárias.

A transparência e prestação de contas, valores fundamentais na administração pública, são fortalecidas pela implementação de sistemas automatizados de firewall. A capacidade de documentar e auditar esses processos reforça a transparência na gestão de dados, demonstrando o compromisso do órgão público em assegurar a integridade e a segurança das informações sob sua responsabilidade.

Diante desses argumentos, a contratação de um sistema de firewall robusto é uma medida estratégica e essencial para fortalecer a resiliência, eficiência, integridade e transparência na gestão da informação digital. Essa solução não apenas resguarda os interesses do município, mas também reforça a confiança da população na capacidade da Câmara em lidar responsavelmente com as informações que lhe são confiadas.

1. Atendimento ao Termo de Referência

A contratação proposta busca atender às demandas específicas de proteção contra acessos não autorizados, conforme delineado no termo de referência.

2. Avanço Tecnológico e Complexidade Administrativa

O avanço tecnológico e as demandas crescentes na Administração Pública impuseram desafios significativos. A complexidade das operações e a quantidade massiva de dados acumulados ao longo dos anos requerem uma abordagem proativa para garantir a segurança e disponibilidade dessas informações.

3. Carência de Sistemas Adequados

Atualmente, a Câmara Municipal carece de sistemas que garantam a segurança dos dados. Os sistemas em uso armazenam informações sensíveis, como Contabilidade Pública Municipal, Gestão de Pessoal, Arrecadação de Tributos, Prontuários e Dados Médicos da População, acumulados ao longo de décadas. A ausência de recursos de segurança apropriados coloca esses dados em risco de acessos não autorizados.

4. Volume Significativo de Dados

O município detém um volume expressivo de dados e informações críticas. Sem um suporte técnico/lógico adequado para segurança, esses dados correm o risco de serem comprometidos, comprometendo a confidencialidade e a integridade das informações.

5. Fase de Aperfeiçoamento Tecnológico

A Administração Municipal encontra-se em fase de aperfeiçoamento físico e profissional no que tange ao ambiente tecnológico. Diante desse contexto, a contratação de um sistema robusto de firewall se apresenta como uma medida necessária para garantir a proteção dos dados.

6. Legislação Pertinente

Ressaltamos que a contratação de sistema de nível corporativo de firewall, alinha-se com as diretrizes legais vigentes para a segurança da informação em órgãos públicos. Conforme a Lei nº 13.709/18, que estabelece as normas gerais sobre a segurança e proteção de dados, é dever do órgão público adotar medidas para proteger seus dados contra acessos não autorizados. Dessa forma, a presente contratação visa não apenas atender às necessidades imediatas, mas também resguardar o patrimônio informacional do município, assegurando a continuidade dos serviços públicos e o cumprimento das normativas legais vigentes.

Contextualização

1. Desafios da Era Digital: O avanço tecnológico e as demandas crescentes na Administração Pública impõem desafios significativos. A complexidade das operações e a quantidade massiva de dados acumulados ao longo dos anos requerem uma abordagem proativa para garantir a segurança e disponibilidade dessas informações.
2. Deficiência Atual: A infraestrutura tecnológica atual demonstra deficiências notáveis em relação à segurança da informação. A falta de um sistema adequado compromete a integridade de informações críticas, desde dados contábeis até registros médicos da população, representando uma ameaça substancial à confidencialidade e confiabilidade desses dados.

Justificativa Técnica

3. Volume e Complexidade dos Dados: A municipalidade abrange diversos setores, cada um gerando e gerenciando uma quantidade significativa e diversificada de dados. A ausência de uma solução técnica robusta para proteção dessas informações representa um risco inaceitável, podendo prejudicar não apenas a eficiência operacional, mas também a prestação de serviços essenciais à comunidade.
4. Segurança da Informação: O presente cenário destaca a urgência em adotar práticas de segurança da informação alinhadas aos padrões legais e regulatórios. A não conformidade poderia resultar não apenas em perda de dados, mas também em consequências legais, comprometendo a imagem e a credibilidade da administração pública.

Conclusão

Em suma, a contratação do sistema de firewall representa um investimento estratégico para a Câmara Municipal. Ao assegurar a segurança e disponibilidade dos dados, a administração não apenas atende aos requisitos legais, mas também resguarda a eficiência operacional e a prestação de serviços públicos essenciais à população. Esta medida não apenas responde às exigências do presente, mas também prepara o município para os desafios futuros da era digital.

Desta forma, visando garantir a segurança dos dados de diversos setores da municipalidade e evitando assim a inviabilidade do desenvolvimento dos trabalhos bem como dos serviços públicos essenciais, pretende-se realizar a locação de sistema de proteção contra acessos não autorizados (firewall) utilizando recursos inovadores que proporcionem maior confiabilidade e flexibilidade para manter em segurança as informações, documentos e dados, além de possibilitar o gerenciamento e a administração dos recursos do sistema onde as informações estarão armazenadas.

Fernandópolis, 06 de Novembro de 2024.

F r a n s l e i T h i a g o I z e l i
E-mail: solution@solutiondatacenter.com
CPF: 218.110.508-16 - RG: 32.716.548-0