A Internet das Coisas (IoT) para o Setor Público

Construa uma base segura para utilizar a IoT e obter melhores serviços no setor público, infraestrutura mais inteligente e melhores condições de vida e segurança IoT

Resumo da Solução
IoT no Setor Público

Alcatel·Lucent
Enterprise

A IoT altera fundamentalmente a equação para o Setor Público

A Internet das Coisas (IoT) tem o potencial de transformar o setor público, modificando profundamente a forma como as entidades governamentais coletam dados e informações, unindo as grandes tendências tecnológicas e comerciais para mobilidade, automação e análise de dados. A IoT refere-se à rede de objetos físicos interligados por meio de sensores integrados, atuadores e outros dispositivos que coletam e transmitem informações sobre atividades na rede, em tempo real. Os dados acumulados por esses dispositivos podem ser analisados pelos funcionários públicos, a fim de:

- Conectar os cidadãos e as entidades públicas para oferecer serviços e recursos de alta qualidade, ágeis e seguros que melhorem o engajamento e a confiança entre os governos e o público, melhorando a qualidade de vida, as condições de trabalho e sustentabilidade.
- Aumentar a segurança do tráfego, conhecendo melhor as operações do sistema de transporte através de dados de sensores que rastreiam tudo : desde anomalias na velocidade dos trens, temperatura nas rodovias, até a localização em tempo real dos ônibus de transporte coletivo.
- Reduzir o congestionamento e o uso de energia com as tecnologias Smart City, que utilizam dados em tempo real para melhorar a forma como os funcionários alocam os recursos para atender à demanda, e oferecer a agilidade para reagir rapidamente aos padrões de tráfego dinâmicos, variações no uso de água ou energia, ou mudanças na qualidade do ar.
- Melhorar o desempenho operacional e a manutenção, monitorando proativamente a infraestrutura pública crítica e criando processos mais eficientes para reduzir custos operacionais e melhorar a capacidade do sistema.
- Melhorar a segurança pública, atendendo as emergências de maneira mais rápida e eficaz.

Cenários de IoT no Setor Público

As soluções de IoT prometem tornar as instituições do setor público mais inteligentes e bem-sucedidas. A IoT está no núcleo das forças para remodelar as entidades governamentais, para que possam proporcionar melhores serviços, maior segurança, tráfego eficiente, infraestruturas públicas mais inteligentes e gerenciamento de tráfego estratégico. Exemplos de cenários de IoT para o setor público incluem:

- Transporte coletivo mais eficiente e barato, utilizando uma rede de sensores, câmeras digitais e veículos conectados para aumentar a capacidade do sistema, a segurança e o conforto dos passageiros, ao mesmo tempo em que diminui custos e riscos.
- Soluções de vigilância por vídeo, com câmeras de circuito fechado de alta resolução para proteger o transporte público e a infraestrutura, monitorar o movimento de pessoas e multidões e acelerar os atendimentos de emergência. E softwares de análise de vídeo inteligentes, que automatizam a detecção precoce de comportamento suspeito e bagagem abandonada.
- Sinalização dinâmica para sistemas rodoviários inteligentes, que exibem o status das estradas em tempo real, tarifas de pedágio, fechamento de faixas e tempo de viagem, transmitidos automaticamente pelos sensores e câmeras.
- Soluções inteligentes que monitoram o uso de energia, para criar sistemas de energia mais resilientes que reduzem o consumo e diminuem as emissões de energia, melhorando a eficiência energética e a sustentabilidade do município.

Desafios na implantação da IoT

A IoT traz fluxos de dados sem precedentes, apresentando desafios de desempenho, operacionais e de gerenciamento para a infraestrutura da rede, junto com maiores riscos de segurança. Para solucionar esses problemas, as agências governamentais precisam adaptar seus projetos de rede tradicionais para fornecer novos níveis de inteligência, automação e segurança.

Essas organizações precisam de uma infraestrutura de rede com o melhor custo-benefício, que possa tratar com segurança o grande fluxo de dados, mas que também seja simples de gerenciar e operar. A infraestrutura deve:

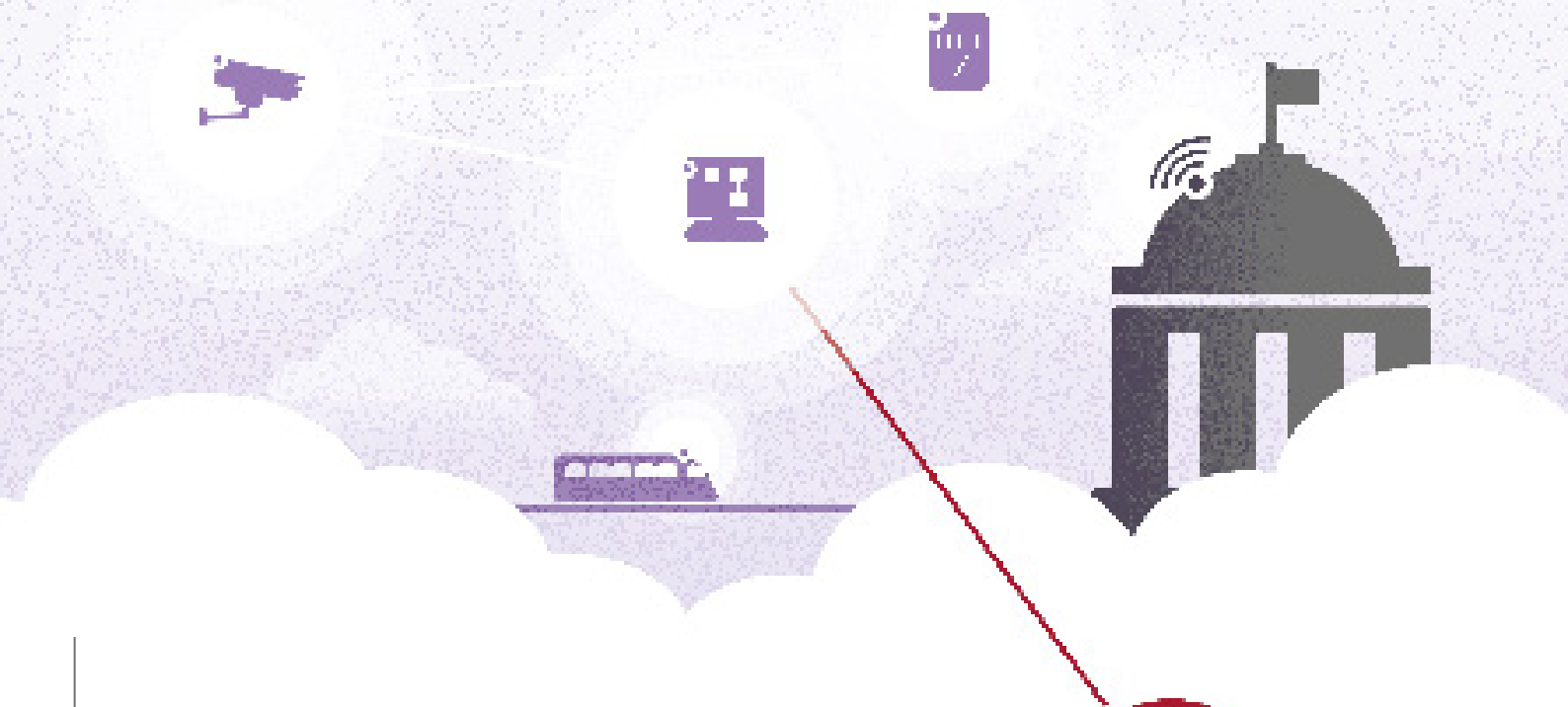
- **Utilizar um processo simples e automatizado para a integração de dispositivos IoT.** Grandes sistemas IoT podem conter milhares de dispositivos e sensores, portanto adicionar e gerenciar manualmente todos esses terminais é complexo e propenso a erros. A integração automatizada permite que a infraestrutura de rede reconheça dinamicamente os dispositivos e os atribua para a rede de segurança correta.
- **Fornecer os recursos de rede apropriados para que o sistema de IoT funcione de forma adequada e eficiente.** Muitos dispositivos no sistema de IoT utilizam informações essenciais, que exigem um nível específico de QoS. Por exemplo, alguns aplicativos requerem uma determinada largura de banda, em uma infraestrutura de rede de alto desempenho, para garantir a confiabilidade e o fornecimento do serviço.
- **Fornecer um ambiente seguro contra ataques cibernéticos e perda de dados.** Os inúmeros dispositivos e sensores conectados na rede IoT levam a uma abundância de possíveis vetores de ataque, e por isso a segurança é fundamental para reduzir os riscos de crimes cibernéticos. A segurança é necessária em vários níveis, incluindo a contenção das próprias redes IoT.

Os profissionais de TI estão fazendo planos para mais IoT

Profissionais de TI de vários setores já estão planejando o aumento no uso de soluções de IoT, em um futuro próximo. De acordo com a pesquisa da 451 Research de 2017, Tendências na Internet das Coisas, 67% dos profissionais de TI pesquisados disseram que suas empresas já implantaram uma solução de IoT ou tinham um sistema IoT em piloto. 21% dos entrevistados disseram que suas empresas planejavam implantar soluções de IoT dentro de 12 meses, e 11% dizem que suas empresas planejam implementar IoT em mais de um ano.

A IoT contribui para a exposição do Setor Público aos crimes cibernéticos

O crescimento da IoT no setor público também traz uma explosão de ameaças à segurança cibernética, pois a proliferação de sensores e dispositivos conectados expande muito a superfície de ataque da rede. A IoT é especialmente sensível, porque muitos dispositivos IoT são fabricados sem ter a segurança em mente, ou são criados por empresas que não entendem os requisitos de segurança atuais. Consequentemente, cada vez mais, os sistemas de IoT representam o elo mais fraco na segurança da rede dos órgãos de governo.



- O ataque de ransomware WannaCry, em maio de 2017, atingiu redes governamentais em todo o mundo, criptografando dados e paralisando computadores durante dias no Ministério do Interior da Federação Russa, no Ministério das Relações Exteriores da Romênia e em mais quatro governos estaduais na Índia.[1]
- Em março de 2018, o governo municipal de Atlanta foi paralisado quando hackers ransomware exploraram as vulnerabilidades na rede Smart City da cidade, criptografando arquivos do governo, bloqueando o acesso a serviços online (inclusive email) e impedindo a prefeitura de processar casos e mandados judiciais.[2]

A Administração Sueca de Transportes - Trafikverket foi atingida por um ataque DDoS (Distributed Denial of Service) em 2017, que derrubou o sistema automatizado de operação dos trens, bem como os emails e a rede de comunicação da organização, deixando os passageiros ferroviários parados em todo o país sem informações sobre o que havia acontecido com o serviço.[3]

Criando uma infraestrutura de rede IoT segura

Proteger o tráfego e os dispositivos IoT é um desafio que não pode ser resolvido por qualquer tecnologia de segurança. Exige uma abordagem estratégica que tira proveito de várias medidas de segurança.

Para ajudar sua empresa a aproveitar os benefícios e reduzir os riscos da implantação de IoT, a Alcatel-Lucent Enterprise (ALE) oferece uma estratégia de segurança em vários níveis. A estratégia da ALE fornece proteção em cada camada da infraestrutura, a partir de cada usuário e dispositivo individual até a própria infraestrutura da rede. Ela também fornece uma estratégia de contenção de IoT para simplificar e proteger a integração de dispositivos, e oferece os recursos de rede apropriados para que o sistema funcione de forma correta e eficiente, tudo em um ambiente seguro para garantir a proteção dos sistemas de tráfego contra ataques cibernéticos.

IoT containment

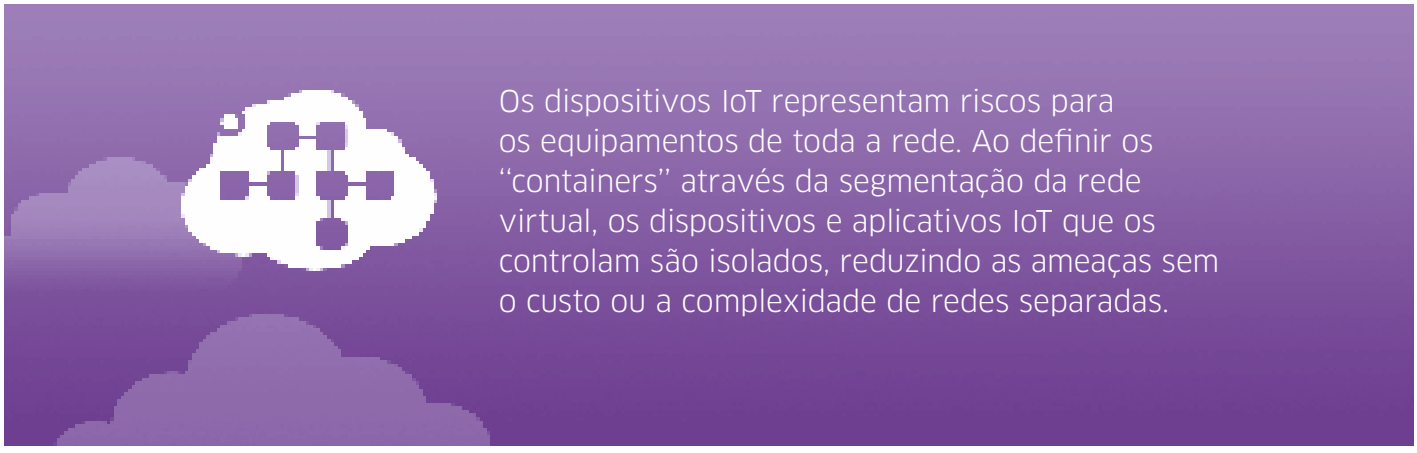
Para habilitar o IoT Containment, todos os usuários, dispositivos e aplicativos dentro da rede da ALE são associados a perfis. Esses perfis, que definem funções, autorizações de acesso, níveis de QoS e outras informações sobre políticas, são transmitidos a todos os switches e pontos de acesso na rede..

- Os dispositivos são atribuídos a "recipientes (containers) virtuais" usando técnicas de virtualização de rede, permitindo que vários dispositivos e redes usem a mesma infraestrutura física, enquanto permanecem isolados do resto da rede.
- Nesses recipientes virtuais, as regras de QoS e segurança são aplicadas.
- Com a divisão da rede em "containers" virtuais, caso ocorra alguma violação em uma parte da rede virtual, isso não afetará outros dispositivos ou aplicativos em outras redes virtuais.
- Quando um novo dispositivo IoT estiver conectado, a rede reconhecerá automaticamente seu perfil e atribuirá o dispositivo ao ambiente virtual adequado.
- A comunicação é limitada aos dispositivos dentro desse ambiente virtual, e aos aplicativos do datacenter que controlam esses dispositivos.
- Como todos os usuários têm perfis dentro da rede da ALE, o acesso aos "containers" virtuais de IoT pode ser limitado a indivíduos e grupos autorizados.

Segurança aprofundada

Além do IoT Containment, as tecnologias de rede da ALE fornecem a segurança por camada, nos vários níveis da rede.

- No nível do usuário, os perfis garantem que os usuários sejam autenticados e autorizados com os direitos de acesso adequados.
- No nível do dispositivo, a rede assegura que os dispositivos sejam autenticados e estejam de acordo com as regras de segurança estabelecidas.
- No nível do aplicativo, a rede pode estabelecer regras sobre cada aplicativo ou grupo de aplicativos, incluindo bloqueio, limitação de largura de banda e controle de quem pode acessar quais aplicativos.
- No nível da rede, os switches da ALE se beneficiam do secure diversified code . Ele protege redes contra vulnerabilidades intrínsecas, quebras de código, malwares infiltrados e possíveis backdoors que poderiam comprometer os switches, roteadores e outros hardwares essenciais.
- A função smart analytics da ALE usa inspeção profunda de pacotes e outras tecnologias para detectar os tipos de dados e aplicativos se movimentando pela rede, tornando possível identificar padrões incomuns de tráfego, atividades não autorizadas e invasões.



Gerenciamento e operação da rede, de ponta a ponta

As soluções de rede da ALE também oferecem às corporações vantagens significativas para operação e gerenciamento.

- A ALE permite que várias redes distintas operem em uma única infraestrutura comum, eliminando a necessidade de mais investimento CAPEX em múltiplas redes físicas.
- A solução de Acesso Unificado da ALE permite que as tecnologias com fio e sem fio trabalhem juntas, como uma rede única e robusta, com serviços de rede, regras de políticas, um esquema de autenticação em comum, e uma única base de dados de autenticação.
- As soluções de rede da ALE também têm um único sistema de gerenciamento para todos os elementos da infraestrutura, incluindo gerenciamento unificado das redes LAN com fio e sem fio. O gerenciamento Alcatel-Lucent OmniVista® 2500 conta com um painel de controle unificado para gerenciar ambientes virtuais, switches, Access Points e todos os outros componentes da rede.

Um portfólio de rede de alto desempenho

Os switches, Access Points e controladoras da ALE suportam a última geração de recursos de alta largura de banda e baixa latência, e podem gerenciar um grande número de dispositivos em ambientes de alta densidade. Os produtos e soluções de rede da ALE atendem às necessidades de rede das instituições governamentais de todos os tamanhos. A ALE também oferece uma seleção de switches robustos, Access Points e roteadores para implantações externas ou em condições adversas.

Redes e estratégias IoT seguras para o Setor Público. Aqui, e agora

Os produtos e soluções da ALE criam a base para uma rede segura, de forma que as organizações públicas possam utilizar sistemas de IoT para conectar melhor os cidadãos aos serviços públicos, habilitar soluções Smart City e melhorar a eficiência operacional da infraestrutura pública, enquanto reduzem custos e riscos. As estratégias de IoT Containment e segurança por camada, da ALE, reduzem os riscos e simplificam a configuração das redes de IoT ao facilitar a integração dos dispositivos, com operações mais eficientes e mais segurança. A ALE ajuda as instituições de transporte a utilizarem todos os possíveis benefícios da IoT, com melhores níveis de inteligência, automação e segurança da rede.

Quer saber mais?

Para obter mais informações sobre as soluções de IoT da ALE, vá para ALE IoT Security.

Governo Conectado

Ajudamos você a conectar suas comunidades, proporcionando a tecnologia que funciona para sua organização e o público que você atende. Com alcance global e foco local, oferecemos redes ecomunicações projetadas para oferecer mobilidade, segurança e proteção para as organizações do setor público.

[1] WannaCry Ransomware Attack

[2] A Cyberattack Hobbles Atlanta, and Security Experts Shudder

[3] DDoS Attack Halts Swedish Transport Systems

MPR00303783 (dezembro de 2019)