opengear
A DIGI COMPANY

WHITE PAPER

Por que você precisa de administração fora-de-banda?

As interrupções no sistema podem resultar de ataques cibernéticos, erro humano ou outras diversas condições ambientais.

Uma ampla variedade de elementos de rede também pode causar interrupções. Interconexões de cabos, fontes de alimentação, switches, chassis de computação densa, matrizes de armazenamento e até ar condicionado são fontes potenciais de problemas.
E os dispositivos de rede estão cada vez mais complexos, com diversos softwares frequentemente atualizados e suscetíveis a bugs, explorações e ataques cibernéticos.

ACESSO SEMPRE DISPONÍVEL AOS SEUS DISPOSITIVOS DE REDE

Se a sua rede principal ficar indisponível, todas as partes da sua rede, desde as centrais de dados e filiais até as redes de ponta e dispositivos de IoT, têm resiliência na conexão? À medida que sua empresa cresce, sua rede se torna cada vez mais complexa e novas implantações ou aquisições podem não conseguir se conectar tranquilamente através da Internet.

Considere estes exemplos recentes de grandes interrupções e invasões:

- 2015 e novamente em 2018 - Google: Roubo de informações privadas nos perfis do Google+, incluindo nome, empregador e cargo, endereço de email, data de nascimento, idade e status do relacionamento. A violação resultou no desligamento permanente do serviço do Google+ pelo Google.
- 2018 - British Airways: Uma invasão no site e no aplicativo da BA permitiu o roubo de dados financeiros e pessoais de mais de 380 mil clientes.
- 2019 - Target: Uma interrupção de duas horas nos registros da empresa lhes custou US$ 50 milhões em vendas.
- 2019 - Facebook: Várias interrupções de rede, ao custo de US$ 6,3 milhões por cada hora de inatividade do Facebook. Isso não leva em consideração as perdas adicionais que a empresa sofreu quando suas ações foram atingidas.

Nenhuma empresa pode arcar com interrupções. No entanto, quanto maior a rede, maior a probabilidade disso ocorrer. Interrupções são caras e podem exigir técnicos no local a qualquer momento para resolver o problema. E mesmo atualizações de firmware, alterações de configuração e oscilação de tensão para corrigir erros requerem ajuda prática. Você precisa de acesso remoto através de uma conexão secundária para sempre ter acesso aos seus dispositivos de rede.

O QUE CAUSA INTERRUPÇÕES?

As interrupções no sistema podem resultar de ataques cibernéticos, erro humano ou diversas outras condições ambientais. Interrupções também podem ser causadas por falhas e vulnerabilidades no hardware de rede em softwares com atualizações frequentes. Uma das causas mais comuns de interrupções é a vulnerabilidade no último quilômetro da rede primária.

Em junho de 2019, os projetos do Google Cloud com serviços em várias regiões dos EUA sofreram uma grande perda de pacotes como resultado do congestionamento da rede por várias horas. Ao analisar a interrupção, eles informaram que "Os engenheiros da Google foram alertados sobre a falha dois minutos após começar e rapidamente iniciaram os protocolos de administração de incidentes usados para incidentes de produção mais significativos. A resolução do problema foi significativamente prejudicada pela falha de ferramentas concorrendo pelo uso da rede, que agora está congestionada." Eles perceberam que tinham um problema, ***mas não tinham uma outra forma de resolvê-lo.***

Enquanto a conectividade com o provedor de serviços de Internet tenha melhorado nos últimos anos, um dos pontos fracos que esses serviços não conseguem superar é o problema que se refere ao segmento final da rede de produção que conecta sua rede ao seu ISP. Este é o elo mais fraco da sua conectividade.

Todo o tráfego de rede de um único escritório, loja, filial ou centro de distribuição é canalizado por meio de links únicos. A largura da banda desses links efetivamente limita a quantidade de dados que pode ser transmitida ao seu ISP. Esse gargalo deixa você exposto a ataques de DDoS e a erros humanos básicos que levam a interrupções. E esse ponto final vulnerável pode ser vítima de uma falha física. Um corte acidental na fibra ótica pode interromper toda a sua rede e deixá-lo desconectado dos seus serviços de internet por períodos significativos.

GERENCIAMENTO EM BANDA E FORA-DE-BANDA

Sua empresa possui uma conexão ISP de produção para tráfego de rede, incluindo VPN, web, e-mail, aplicativos em nuvem e muito mais. Geralmente, há apenas uma rede principal, (T1, cabo, SD-WAN ou MPLS), que direciona esse tráfego para a internet.

"Conseguir acessar o equipamento que você precisa; conseguir gerenciar, independentemente de ter ou não conectividade por meios normais. Então, o 4G, o wireless, toda essa conectividade é enorme."

Steve DiCicco
Engenheiro de Redes Sênior

As informações administrativas fluem por meio das mesmas interfaces que os dados do usuário. Quando a administração e os dados compartilham a mesma esfera, você acaba usando o plano de dados para acessar seu equipamento de rede. Isso é conhecido como gerenciamento em banda. Quando você gerencia seu equipamento usando uma rede "In-Band", os comandos de controle e dados passam pela mesma rota de rede. Sendo assim, sua esfera de administração tem as mesmas vulnerabilidades de segurança que sua esfera de dados. E você pode ficar de fora da esfera de administração por causa da interrupção.

A vantagem do In-Band é que ele é barato e simples, pois você só precisa de uma rede. Mas também é muito menos seguro, porque você mistura o tráfego do usuário, que geralmente tem regras de acesso e tráfego de administração que são menos rigorosas. Interrupções e ataques podem comprometer não apenas os dados do usuário, mas também a administração e a integridade do seu equipamento de rede. Além disso, quando há uma interrupção, você não consegue se comunicar com seus dispositivos.

Como alternativa, você pode executar o tráfego de administração através de uma rede autônoma que lida apenas com o tráfego de administração. Esta é a administração fora-de-banda (OOB). A OOB oferece uma forma alternativa de conectar-se ao seu equipamento remoto, como roteadores, switches e servidores, através da esfera de administração, sem acessar diretamente o endereço IP de produção do dispositivo na esfera de dados e independentemente da conexão ISP principal usada por sua empresa. Esse caminho fora-de-banda é completamente separado da rede de produção e permite que os administradores monitorem, acessem e gerenciem com segurança todos os dispositivos sem interferir nas operações normais e, o que é mais importante, sem ter que permitir que a esfera dos dados acesse a esfera da administração.

Como a rede fora-de-banda separa o tráfego do usuário e da administração, você pode bloquear, restringir o acesso e proteger completamente a esfera de administração. Além disso, você pode configurar, gerenciar e solucionar problemas de seus dispositivos, mesmo quando a esfera de dados estiver inativa. Uma solução OOB oferece uma conexão secundária, geralmente por meio de 4G LTE, que permite ao técnico da rede resolver problemas de qualquer lugar e, o mais importante, economizando tempo e dinheiro da empresa.

TRÊS ESFERAS SÃO MELHORES QUE UMA

Considere que uma rede tem três esferas[1]:

A **Esfera de Dados** consiste nos componentes de infraestrutura que transportam dados do usuário". Seu objetivo é permitir que os dados passem, por exemplo, de um servidor da web para o computador de um cliente e vice-versa.

A **Esfera de Controle** é responsável por manter os dados em constante movimentação. Ela contém as regras que permitem o roteamento de informações de um lugar para outro. Por exemplo, ela permite que os roteadores de rede criem um caminho para levar dados de um servidor da web para o computador de um cliente.

A **Esfera de Administração** é usada para configurar e administrar os switches e roteadores de rede.

Em muitas configurações, a Esfera de Administração é combinada com a Esfera de Dados, o que pode ser problemático quando ela apresenta problemas.

1 Saiba mais sobre planos de rede.

A desvantagem é o custo extra de configurar uma rede separada apenas para administração, mas como verá mais adiante neste documento, o ROI compensa a despesa muito rapidamente.

POR QUE VOCÊ PRECISA DO OOB?

Você realmente precisa adicionar o custo e a complexidade de uma forma secundária de se conectar ao seu equipamento? Sim, você precisa. Há várias razões pelas quais a OOB faz sentido, mesmo com um custo extra. Primeiro, você aumentará a segurança. Sem ele, as entradas do console serão conectadas à sua rede de produção in-band; portanto, se um vírus, bot ou hacker invadir sua rede, toda as esferas estarão em risco.

Estávamos operando nossos switches e a atualização falhou, então não conseguimos mais acessá-los. Em vez de entrar no escritório e conectar-se através de uma porta de console, pudemos nos conectar através do Opengear, por meio do módulo de telefonia móvel, e recuperá-lo em 10 minutos. Isso nos economizou muito tempo e angústia."

Evans Vogas
Analista de Operações de Rede

Em segundo lugar, você poderá encarar uma interrupção no provedor de serviços de Internet e manter sua organização em operação. Sua conexão principal à Internet está sujeita a uma vulnerabilidade de "último quilômetro" ("last mile"). Algo tão simples como uma retroescavadeira pode cortar sua linha e sua principal conexão, seja de fibra ou cabo ou qualquer outra coisa, ficará fora de serviço. E com os consoles OOB avançados, a administração da interrupção pode ser feita quase instantaneamente e remotamente.

Para empresas com escritórios remotos, a OOB é uma escolha fácil. Em vez de ter que enviar um técnico de rede para o local, a solução de problemas e a administração do seu equipamento podem ser realizadas de qualquer lugar, a qualquer hora, através de um sistema centralizado de administração.

Lembre-se de que a largura de banda LTE usada para executar tarefas administrativas é mínima. Basicamente, os técnicos de rede enviam comandos de texto através de um terminal e obtêm informações desses comandos. Como alternativa, eles podem usar um software centralizado de administração que, nos bastidores, não usa uma grande largura de banda, mantendo as tarifas de LTE baixas.

Por fim, essas vantagens geram economia de enorme volume de dinheiro, compensando muito o investimento na OOB.

CONSOLES AVANÇADOS DE ADMINISTRAÇÃO FORA-DE-BANDA DISPONÍVEIS HOJE

Um console de administração fora-de-banda oferece recursos que minimizam substancialmente o tempo de inatividade e reduzem seus custos operacionais:

• Opere independentemente da rede in-band, o que se traduz em uma diversidade de links para verdadeira resiliência da rede.

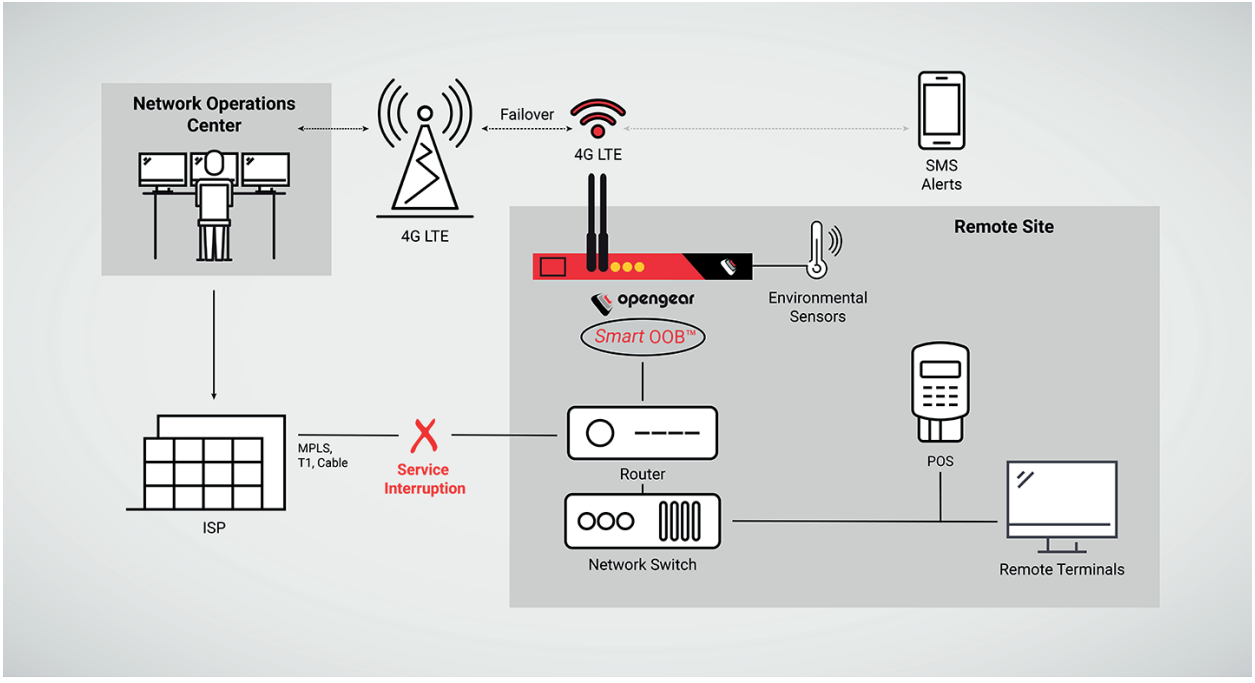
• Transferência automática para rede móvel. Quando o link principal fica indisponível, a conectividade com a Internet é transferida para LANs remotas e equipamentos de redes 4G LTE.

• Oferta de Zero Touch Provisioning (ZTP). O ZTP permite que os administradores automatizem o processo de implantação. Por sua vez, isso permite automatizar tarefas repetitivas, reduzir pontos de contato humanos, reduzir erros e dimensionar o processo de implantação para qualquer tamanho.

• Envie alertas automáticos por e-mail ou SMS para notificar qualquer problema de rede.

• Identifique qualquer inconsistência ou atividade incomum com condições de temperatura, posições de "cage door" e disponibilidade da rede.

• Permite que você instale e opere remotamente a rede sem uma visita no local a partir de uma única tela.



"Você poderá continuar seu trabalho sem problemas após uma interrupção. É assim que projetamos nossos locais, para que qualquer pessoa possa entrar e reiniciá-lo. A Opengear nos salvou muitas e muitas vezes. "

Landon Orr
Engenheiro de Redes de Produção

RETORNO SOBRE SEU INVESTIMENTO OOB

Os consoles de OOB podem se pagar rapidamente, reduzindo os custos operacionais e as perdas de tempo de inatividade potencialmente catastróficas. Em termos de custos operacionais, considere diminuir o custo de um único local de ponta.

Uma visita de instalação pode custar 500 dólares. Um console OOB avançado pode custar 1500 dólares. Apenas três interrupções compensaram o custo. Uma viagem de avião para resolver o problema poderia ser ainda mais cara, equilibrando os custos em um incidente. E esta é apenas uma das localidades.

As perdas operacionais também são menores, pois, de acordo com o Gartner, o custo médio de 1 minuto de inatividade é de US$5.600. Considere uma rede com 10 locais físicos.

Agora, para equipar sua rede com uma implantação típica de administração fora-de-banda com 10 locais e um sistema centralizado de administração terá um custo aproximado US$25 mil. Em média, você atinge um equilíbrio após apenas cinco minutos de inatividade.

CONCLUSÃO

A administração fora-de-banda elimina a necessidade devisitas técnicas por engenheiros de rede a Data Centers, filiais, quiosques, escritórios dispersos ou locais de varejo de POS. Você pode carregar remotamente configurações e imagens do sistema operacional, simplificar as funções de backup e restauração, ligar e desligar os roteadores para reiniciar o equipamento e reduzir os tempos de reparo. A OOB aumenta muito o tempo e produtividade da sua empresa. E para seus clientes, a administração fora-de-banda pode significar a diferença entre operações tranquilas e falhas catastróficas. Se seus clientes não conseguem acessar seus negócios, a confiança e a lealdade vão sofrer e você terminará com uma alta rotatividade de clientes.