RESUMO EXECUTIVO

IDENTIFIQUE, CONECTE E PROTEJA A MOBILIDADE E A IOT NA BORDA

INTRODUÇÃO

O número gigantesco de dispositivos IoT que se conecta a redes empresariais gera desafios para a TI, visto que eles equilibram os benefícios de edifícios inteligentes com o risco de integração de milhares de dispositivos desconhecidos ao seu ambiente, sem precisar do conjunto certo de ferramentas para automaticamente identificar, definir o perfil, autenticar e aplicar políticas a esses dispositivos.

O anúncio mais recente da Aruba lida com esses desafios com uma abordagem em quatro etapas para a conectividade de IoT na borda: A identificação do que está na rede, conexão de dispositivos móveis e de IoT com switches inteligentes, proteção da rede com gerenciamento de política líder de setor e inovação por meio de nosso ecossistema de parceiros para fornecer segurança de ponta a ponta.

A IOT APRESENTA DESAFIOS.

A explosão de dispositivos móveis e a migração para edifícios inteligentes apresentam desafios significativos para a TI e os líderes de negócios.

Falta de visibilidade: você realmente sabe o que está na sua rede?

A segurança começa com o entendimento do que está na rede: smartphones não gerenciados, pontos de extremidade não autorizados, dispositivos de IoT. Tudo isso aumenta a superfície de ataque e ameaça a segurança empresarial. A capacidade de ver o que está em uma rede dá à TI um entendimento melhor de como e pelo que sua rede está sendo usada. A TI deve estar preparada para identificar e definir o perfil de cada dispositivo que está se conectando à rede, independentemente de onde está se conectando. Isso se torna mais desafiador conforme dispositivos de IoT com e sem fio desconhecidos ocupam nossas redes. O perfil de todos os dispositivos precisa ser definido e avaliado na conectividade, atribuído a uma categoria, com acesso automaticamente concedido ou negado com base no tipo de dispositivo, no status da propriedade ou no sistema operacional.

A conexão com fio é a nova preocupação.

Para organizações no espaço empresarial e industrial, o número esperado de dispositivos de IoT com fio pode variar de 35% a mais de 50% dependendo da vertical: detectores de movimento, equipamentos médicos, controladores de processos no chão de fábrica, para citar alguns. No passado, as discussões sobre o controle de acesso à rede (NAC) eram principalmente centradas em como proteger a rede sem fio, porque é assim que a maioria dos dispositivos estava se conectando. As conexões seguras por sessão se tornaram um requisito, visto que a interceptação sem fio e os usuários sem fio poderiam estabelecer acesso de qualquer lugar dentro da faixa de um ponto de acesso e SSID não seguro.

O enorme foco na proteção das redes de segurança significava que as redes com fio eram deixadas desprotegidas, visto que os switches ficavam atrás de portas trancadas, e a percepção era de que eles não mostravam as mesmas vulnerabilidades da conexão sem fio. Infelizmente, conforme as redes com fio cresciam, a consistência entre vários switches diminuíam, deixando as portas bem abertas e acessíveis a qualquer pessoa. As portas em salas de conferência e áreas de impressoras são um exemplo clássico em que existe uma segurança "incerta". Com vários dispositivos de IoT se conectando com fio, chegou a hora de dar o mesmo nível de atenção para proteger a infraestrutura com fio.

As infraestruturas com fio tradicionais não foram otimizadas para IoT

Nos ambientes de comutação legados, a força de trabalho não era móvel e a IoT ainda não existia. Os ativos residiam atrás do firewall, e a TI precisava garantir que o perímetro permanecesse forte. Agora, entre na IoT — a infraestrutura com fio precisa ser tão inteligente quanto a sem fio — os switches de hoje precisam ter a segurança e o gerenciamento de rede inteligente integrados para que todos esses dispositivos possam ser conectados com segurança e perfeitamente.

A proteção da rede requer fluxos de trabalho automatizados

Com os milhares de dispositivos móveis e de IoT desconhecidos se conectando a uma rede empresarial diariamente, é impossível atribuir manualmente e aplicar políticas que respondam por cada dispositivo. Todo o processo deve ser automatizado para reduzir o risco com esforço manual mínimo da TI. Os dispositivos estáticos e a própria infraestrutura deverão também o perfil criado e ser verificados automaticamente em busca de alterações suspeitas. Se um dispositivo estiver agindo de forma suspeita, ele deverá ser colocado automaticamente em quarentena até a ameaça ser avaliada.

Custa caro se antecipar aos hackers

Parece que ouvimos falar sobre grandes violações de dados quase diariamente. É caro e demorado para as empresas investirem em segurança e é quase impossível se antecipar aos hackers inovando sozinho. O ecossistema de parceiros da Aruba foi projetado para reunir os melhores parceiros de segurança a fim de oferecer uma solução de segurança de ponta a ponta.

PLANO DA ARUBA PARA CONECTIVIDADE DE IOT SEGURA NA BORDA

1. Identifique e defina o perfil de dispositivos desconhecidos em redes com e sem fio de vários fornecedores

Considerando que a segurança de rede começa por saber o que está na rede, é essencial que as organizações consigam identificar

e definir o perfil de todos os dispositivos. A família ClearPass da Aruba oferece uma vantagem exclusiva em relação à concorrência, visto que a geração de perfil em tempo real e sem agentes pode ser adquirida como um dispositivo independente ou em uma solução de aplicação de política abrangente.

Ambas as soluções permitem identificar continuamente os pontos de extremidade e dispositivos de rede em redes com e sem fio habilitadas para AAA ou não AAA, por meio de endereços IP dinâmicos ou estáticos. O visual abrangente do painel facilita a visualização do número total de pontos de extremidade e o número por categoria, família e tipo de dispositivo.

O novo Aruba ClearPass Universal Profiler é um dispositivo virtual independente que pode ser implantado e funcionar em minutos e foi projetado para essas organizações que não estão prontas para uma solução de NAC completa ou para áreas remotas ou restritas em que NAC não foi implantado. O Universal Profiler é uma simples e econômica de identificar e definir o perfil do que está na rede.

O Aruba ClearPass Policy Manager é um dispositivo virtual ou físico que contém geração de perfil abrangente, aplicação de política com e sem fio não AAA e AAA, acesso de convidado, integração de BYOD, recursos de avaliação de ponto de extremidade, geração de relatórios e integração de solução orientada com base na experiência do usuário e de segurança de terceiros integrada.

2. Conecte dispositivos de IoT com inteligência automatizada

A migração para edifícios inteligentes significa que as empresas de hoje precisam de uma infraestrutura com fio mais inteligente. Os avanços mais recentes no ArubaOS-Switch foram projetados para solidificar e proteger a borda inteligente, otimizando para dispositivos móveis e de IoT. Esses avanços permitem o acesso baseado em função unificado entre redes sem e com fio, com a capacidade de identificar e atribuir funções a dispositivos de IoT conectados a fim de priorizar os aplicativos críticos para os negócios e proteger a rede.

Os switches de camada 3 Aruba podem também realizar o encapsulamento de tráfego com fio baseado em porta e baseado em usuário para uma controladora de mobilidade, de forma que as políticas possam ser aplicadas, os serviços avançados possam ser estendidos e o tráfego possa ser criptografado para proteger a LAN. Para atender à demanda do rápido crescimento em dispositivos de IoT e conectados em empresas distribuídas, o Aruba 2540 de bom custo-benefício (assim como os outros switches Aruba) oferecem suporte a Zero Touch Provisioning e ao gerenciamento baseado em nuvem opcional para permitir que as empresas simplifiquem e reduzam os custos de gerenciamento e implantação de rede.

3. Proteja a rede com políticas inteligentes

Quando você tiver a visibilidade de dispositivo, a aplicação automática de política entrará em cena. O Aruba ClearPass Policy Manager pode ajudá-lo a ver o que está na sua rede e aplicar políticas e fluxos de trabalho automatizados em infraestruturas com e sem fio de vários fornecedores. O ClearPass fornece definição de perfil, aplicação de política, acesso de convidado, integração de BYOD e muito mais para oferecer descarga de TI, proteção avançada contra ameaças e uma experiência avançada ao usuário. E com um novo foco na proteção da infraestrutura com fio, o recurso OnConnect usa os protocolos de switch existentes, ajudando-o a bloquear as portas com fio em lugares vulneráveis, como salas de conferência, telefones IP e em áreas de impressoras.

4. Agilize a inovação para melhorar a segurança na borda

O ecossistema de tecnologia da Aruba inclui soluções de segurança líderes de setor que se integram ao ClearPass Exchange para garantir segurança de ponta a ponta na borda e no núcleo. Nossas parcerias mais recentes se concentram na segurança de IoT:

- Niara usa padrões de tráfego conhecidos associados a tipos de dispositivos para identificar comportamento suspeito e solicita que o ClearPass remova o dispositivo da rede.
- Attivo permite que a TI crie dispositivos de IoT "virtuais falsos" em que as pessoas tentam usar os dispositivos falsos para atacar uma rede. Quando o dispositivo virtual for visto apresentando um comportamento indesejado, será solicitado que o ClearPass retire os dispositivos da rede.

CONCLUSÃO

À medida que as organizações integram a IoT às operações habituais, a integração e o gerenciamento de dispositivos de IoT se torna fundamental para o sucesso. As empresas precisam de uma estratégia para conectar dispositivos móveis e de IoT com segurança na borda, para extrair as eficiências e o valor associados aos edifícios inteligentes enquanto mantêm a rede e os ativos corporativos protegidos. A abordagem da conectividade de IoT em quatro etapas da Aruba lida com os desafios de identificar o que está na rede, conectando dispositivos por meio de infraestruturas com e sem fio inteligentes, protegendo a rede com gerenciamento de políticas automatizado e usando nosso ecossistema de parceiros para aumentar a segurança de ponta a ponta a fim de se antecipar aos riscos potenciais.

a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089 USA
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com