RESUMO EXECUTIVO: PROTEGENDO A PRÓXIMA ONDA WIRELESS

Resumo

A conectividade wireless está em toda parte na economia móvel global dos dias atuais. Os dispositivos wireless incluem desde smartphones e notebooks até câmeras de segurança e headsets de realidade virtual. As empresas precisam reconhecer e suprir a necessidade de alta qualidade, desempenho e segurança de redes wireless e endpoints.

Negócios da atualidade em um mundo wireless

A conectividade wireless de alta velocidade deixou de ser opcional no panorama atual das redes. Ela se tornou uma necessidade, pois as empresas procuram aumentar o valor do cliente e melhorar a produtividade dos funcionários com iniciativas de BYOD (bring your own device) e com o uso cada vez maior de aplicações que consomem muita largura de banda. Outras organizações, como escolas e universidades, usam a conectividade wireless para proporcionar aos alunos um ambiente educacional mais conectado. O usuário espera ter conectividade wireless independentemente da localização ou do tipo de dispositivo. Além disso, existe uma tendência cada vez maior de uso de dispositivos apenas com conectividade wireless no local de trabalho, na sala de aula, em hospitais e na vida diária.

IoT Wireless

Tudo isso é motivado por vários fatores importantes. O primeiro é a proliferação constante de dispositivos que utilizam Wi-Fi, tanto pessoais quanto corporativos. Segundo a ABI Research, a expectativa é que mais de 20 bilhões de Wi-Fi chipsets sejam entregues entre 2016 e 2021. Além disso, mais de 95% dos dispositivos entregues em 2021 terão capacidade para 5 GHz. O segundo é a Internet das Coisas (IoT), que também se expandiu enquanto os dispositivos tradicionalmente não compatíveis com a funcionalidade wireless, como carros, aparelhos domésticos inteligentes (por exemplo, geladeiras, câmeras de segurança,

etc.), entre outros, passaram a conectar-se à Internet por meio da conectividade wireless. Várias empresas de análise previram que haverá 50 bilhões de dispositivos da IoT até 2020.

Em terceiro lugar, juntamente com o aumento dos dispositivos habilitados para Wi-Fi, está o uso de aplicações que consomem bastante largura de banda, como aplicações de multimídia em HD, de nuvem e de dispositivos móveis, com um número crescente de hospedagens na rede. E, finalmente, o mais novo padrão wireless, 802.11ac Wave 2, tornou-se mainstream com os usuários que procuram aproveitar a promessa das velocidades wireless multi-gigabit. Essa combinação exige que as organizações ofereçam aos clientes, funcionários e estudantes uma solução wireless de alta velocidade que aprimore consideravelmente a experiência do usuário.

Rede doméstica na empresa

De acordo com a Wi-Fi Alliance, a rede doméstica está se tornando uma rede corporativa. Isso se deve principalmente ao surgimento de coisas conectadas no dia a dia, assistentes pessoais e aparelhos de realidade virtual sem fio. O impacto do Wi-Fi também pode ser sentido no cotidiano não apenas dos usuários, como também de empresas, como Amazon, Facebook, Netflix e grandes companhias aéreas. Elas dependem do Wi-Fi para realizar operações diárias, como entrega no mesmo dia, acesso móvel a mídias sociais, serviços de streaming de mídia e até partidas pontuais nas companhias aéreas. O Wi-Fi deverá evoluir e melhorar ainda mais com a introdução de novos padrões e protocolos.

Garantia da qualidade wireless do serviço

A velocidade é sempre importante em todo ambiente de rede, assim como a qualidade da conexão wireless em ambientes de alta densidade, incluindo locais externos nos quais as condições podem ser difíceis. Em muitos casos, vários dispositivos conectam-se ao mesmo access point e competem por uma parte da largura de banda. Esse "congestionamento de dispositivos" causa interferência que pode prejudicar o sinal, consequentemente produzindo um desempenho insatisfatório. Fatores adicionais, como objetos físicos (por exemplo, edifícios, paredes e árvores) e outros dispositivos que compartilham a mesma frequência ou canal (fornos de micro-ondas ou telefones sem fio), podem interferir no sinal wireless, obstruindo o caminho de transmissão da frequência de rádio. Tudo isso tem o potencial de afetar aplicações, como o streaming de vídeo, que pode ser prejudicado quando há atraso nos pacotes e a qualidade da imagem é ruim, ou o vídeo é lento devido ao buffering.

Aumento da ameaça à segurança

Por trás de tudo isso está a necessidade de proteger o tráfego wireless contra as ameaças e vulnerabilidades na Internet. Muitos dos produtos de rede wireless de hoje oferecem proteção contra atividades de access point invasores ou de mapeamento de access point para impedir que os invasores obtenham acesso à rede e, consequentemente, a recursos importantes. No entanto, muitas vezes eles não têm a capacidade de fazer uma varredura de inspeção profunda de pacotes do tráfego criptografado na LAN wireless, colocando as organizações em risco. Esses produtos nem sempre contam com recursos de segurança adicionais, como detecção de access point invasores e capacidade de distinguir o acesso de usuário externo do interno. Além dos riscos de segurança, a implantação, o monitoramento e o gerenciamento dos produtos podem levar muito tempo. Talvez não tenham também recursos de suporte para configuração automática e gerenciamento centralizado, que são especialmente importantes na criação e manutenção de uma infraestrutura de rede wireless de grande porte.

Conclusões

As organizações exigem atualmente das redes wireless mais do que apenas uma conectividade mais veloz. Elas precisam de uma solução que ofereça maior taxa de transferência, melhor qualidade de sinal e experiência de usuário aprimorada, em uma grande variedade de clientes wireless em ambientes de alta densidade. Não apenas isso, mas ela deve ser capaz de detectar e remover ameaças do tráfego wireless, criptografado ou não criptografado, para proteger a rede e ao mesmo tempo simplificar a implantação e o gerenciamento constante.

Saiba mais. Visite www.sonicwall.com/en-us/products/firewalls/wireless-security.

Quem Somos

A SonicWall vem lutando contra a indústria do crime cibernético há mais de 25 anos, defendendo empresas de pequeno e médio porte e empresas no mundo todo. Nossa combinação de produtos e parceiros viabilizou uma solução de defesa cibernética de tempo real sintonizada às necessidades específicas de mais de 500 mil empresas em mais de 150 países, para que você possa fazer mais negócios com menos relutâncias.

Em caso de dúvidas sobre o possível uso deste material, escreva para:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consulte nosso website para obter informações adicionais.
www.sonicwall.com/pt-br/