SUMÁRIO EXECUTIVO

Como maximizar a proteção e o acesso, dentro ou fora do Campus

Mobilidade, aplicativos em nuvem e ameaças emergentes exigem mais do atual firewall de próxima geração

Resumo

Faculdades e universidades estão cada vez mais dependentes de aplicativos baseados em nuvem e conectividade móvel. Entretanto, os ataques cibernéticos crescem e os requisitos de conformidade e segurança estão mais rigorosos do que nunca. As universidades devem adotar uma abordagem de segurança de rede sem limites. Este sumário analisa as necessidades críticas de segurança de rede para as universidades atuais e explora as melhores práticas para selecionar uma plataforma efetiva de firewall de próxima geração.

Introdução

Aprendizagem à distância, teletrabalho e currículos baseados em nuvem abriram as redes de colégios e universidades para mais aplicativos baseados em nuvem e dispositivos móveis conectados. Os departamentos de TI estão sob pressão constante para proteger seus dados contra ataques de rede em constante evolução, mais evasivos e mais rápidos. O aumento exponencial no número de endpoints conectados, incluindo dispositivos IoT, criou mais vetores de ameaças que facilitam aos cibercriminosos introduzirem ataques avançados, tais como dia zero e ransomware, muitos dos quais são executados dentro da memória.

Adicionalmente, as universidades exigem continuidade tanto acadêmica quanto administrativa para assegurar o fluxo de informação e os serviços que oferecem por sua rede. Para atender as demandas atuais, os diretores de TI na universidade precisam de um firewall de próxima geração altamente confiável que não só possa ser dimensionado para apoiar simultaneamente um número imenso de dispositivos e conexões encriptadas, mas também examiná-los em busca de ameaças sem comprometer o desempenho.

Enquanto os riscos aumentam, mais se demanda de recursos restritos. O uso de um firewall de próxima geração de baixo custo e facilmente gerenciável que consiga lidar com a largura de banda disponível e suportar múltiplas redes e nuvens mostrou ser evasivo. Os custos se tornam inviáveis e a escassez de pessoal treinado mais grave.

As universidades precisam mudar dos modelos convencionais de segurança para uma abordagem de segurança de rede ilimitada que englobe tanto mobilidade quanto a nuvem. A segurança de rede, hoje em dia, precisa estar sempre ligada, sempre aprendendo e à frente de ameaças emergentes.

Complexidade de rede

As redes das universidades suportam diversos grupos de usuários, desde estudantes e professores até pesquisadores e administradores. Cada um deles pode solicitar acesso a uma sub-rede específica ou a ambientes em nuvem. A segurança deve funcionar em várias redes segmentadas, nuvens ou definições de serviços, cada qual com modelos e grupos de dispositivos exclusivos; muitas vezes com políticas diferentes.

Além disso, tal diversidade de rede pode incluir um legado inerente de soluções de segurança de rede de diversos fornecedores. Administradores de TI não querem gerenciar separadamente firewalls para cada uma dessas redes ou definições de serviço. Frequentemente eles têm que atender diversos grupos de usuários, cada qual exigindo configurações exclusivas e, em alguns casos, têm que fornecer clean pipe.

Com muitos dispositivos de segurança cobrindo várias redes, gerenciar o acesso e as políticas de segurança se torna complicado e oneroso. Muitas vezes a complexidade dificulta o monitoramento de segurança, o controle de acesso, a conformidade regulatória e a migração rápida. Gestão ineficiente gera um gargalo na segurança e diminui a agilidade do negócio. Isto também gera custos operacionais indiretos mais altos.

As melhores práticas recomendam que um firewall eficaz integre serviços de segurança que protegem os recursos SaaS e os baseados em nuvem e também mobilidade e endpoints IoT seguros. É necessária uma interface de política unificada para que as universidades criem de forma simples e intuitiva políticas de acesso e segurança globalmente em uma rede distribuída diversificada. Funções projetadas para simplificar a implementação e configuração facilitando a gestão podem ajudar as universidades a diminuir seu custo total de propriedade e ter um maior retorno de seu investimento em segurança.

A necessidade de rapidez

Como as universidades se desenvolvem e crescem, as conexões encriptadas, dispositivos endpoint, redes, carga de trabalho em nuvem, usuários e rapidez da internet também aumentam. Um firewall que não suporta nenhum desses fatores se torna um gargalo no cenário de TI. Firewall é considerado como uma checagem de segurança de alto desempenho — e não um ponto fraco. Como 70% de todas as sessões são encriptadas, é imprescindível para a produtividade e segurança de informação ter um firewall que consiga processar e examinar esse tráfego sem impactar a experiência de usuário final.

Um firewall eficaz para a universidade deve oferecer escalabilidade, confiabilidade e segurança profunda para milhões de conexões simultâneas a velocidades de vários gigabits. Um firewall com várias instâncias de melhores práticas garante altos níveis de qualidade de serviço, com disponibilidade ininterrupta da rede e conectividade de mais de 100 Gbps de infraestrutura.

Riscos crescentes

O cenário de ameaças continua a crescer e as ameaças se tornam cada vez mais evasivas. Todos os dias úteis, a SonicWall descobre e classifica mais de 140.000 formas novas e atualizadas de malware. Estas variantes são frequentemente atualizadas para contornar filtros estáticos em numerosos dispositivos e serviços. Além disso, muitos atacantes terceirizam componentes, tais como táticas de evasão, boot lockers ou runners, de modo que seja mais difícil detectar seus malware.

O risco frequente para as universidades é de ataques via dispositivos IoT no campus. Gartner estima que há mais de 20 bilhões de dispositivos IoT ativos hoje. Em 2025, IDC prevê que mais de 41 bilhões de dispositivos IoT vão gerar quase que 80 de zettabytes de dados, muitos deles atrás de firewalls. E o pior, muitos destes serão dispositivos IoT não gerenciados. Sem acesso controlado a dispositivos não gerenciados, as vulnerabilidades comuns podem ser exploradas e não podem ser corrigidas ou gerenciadas por TI.

Aplicações SaaS não gerenciadas apresentam outro risco. As universidades usam muitas aplicações de software para melhorar a produtividade e aumentar a colaboração. A organização adquire muitas destas aplicações com licença, tais como Office 365, Teams ou Jira. Todas são aplicações licenciadas, gerenciadas e autorizadas.

No entanto, estudantes, faculdades e funcionários usam cada vez mais aplicações sem licença e não gerenciadas que os departamentos de TI não conhecem ou não aprovam. Isto é conhecido como TI invisível e como exemplos podemos incluir Dropbox ou Google Drive. Raramente as universidades têm conhecimento sobre as preocupações quanto à conformidade ou de ameaças envolvidas quando essas aplicações não autorizadas são usadas. Consequentemente, como elas têm vulnerabilidades que a TI não conhece ou que não são monitoradas suficientemente ou ainda não são controladas pela TI, estas aplicações se tornam um caminho para vazamento e violação de dados por meio de credenciais roubadas e malware.

Para enfrentar estes riscos, um firewall eficaz de próxima geração deve assegurar que cada byte de cada um dos pacotes seja inspecionado e, ao mesmo tempo, manter o alto desempenho e a baixa latência exigidos pelas redes ocupadas. O ideal é oferecer varredura simultânea de ameaças diversas e aplicações bem como a análise de arquivos de qualquer tamanho, sem remontagem de pacotes. Também deve fornecer resposta rápida e proteção contínua contra ameaças zero-day de atualizações de inteligência em tempo real que coletam, analisam e vetam informações sobre ameaças entre vetores cruzados a partir de uma infinidade de fontes globais.

Conclusão

As universidades de hoje precisam de segurança ilimitada sem compromissos. Isto demanda proteção avançada contra ameaças e alta velocidade com custo total de propriedade mínimo. As melhores práticas incluem arquiteturas de várias instâncias e criação de política unificada a fim de defender as redes de forma mais simples e eficaz.

SonicWall pode ajudar. A plataforma Network Security Services da SonicWall (NS*sp*) 15700 é um firewall de próxima geração com alta densidade de portas multi-gig e taxa de transferência acima de 100 Gbps, que processa vários milhões de conexões e, ao mesmo tempo, inspeciona ameaças zero-day e avançadas. Criada para a segurança de rede do ensino superior, ela elimina ataques em tempo real sem diminuir o desempenho. Foi especialmente construída para ser altamente confiável e fornecer constantemente serviços.

Saiba mais. Visite www.sonicwall.com/products/firewalls/high-end

Sobre SonicWall

A SonicWall fornece o modelo Boundless Cybersecurity na era da computação hiper distribuída e uma realidade de trabalho onde todos estão remotos, móveis e inseguros. Ao revelar ameaças ainda desconhecidas, fornecendo visibilidade em tempo real e possibilitando a contínua inovação da economia, a SonicWall resolve as falhas na segurança cibernética para empresas, governos e SMBs em nível mundial. Para obter mais informações, visite www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Faça referência ao nosso website para informação adicional.
www.sonicwall.com