RESUMO DA SOLUÇÃO

Aruba ESP com segurança zero-trust

Segurança para o Edge

Os desafios da segurança de rede evoluíram consideravelmente ao longo dos anos, à medida que os usuários se tornaram cada vez mais descentralizados e os ataques mais sofisticados e persistentes. As abordagens tradicionais de segurança, com foco principalmente no perímetro da rede, tornaram-se ineficazes como estratégias de segurança independentes. A segurança de rede moderna deve acomodar um conjunto diversificado de usuários e dispositivos em constante mudança, bem como ameaças muito mais predominantes, que visam partes anteriormente "confiáveis" da infraestrutura de rede.

O zero-trust surgiu como um modelo eficaz para atender melhor às mudanças nos requisitos de segurança da empresa moderna, supondo que todos os usuários, dispositivos, servidores e segmentos de rede são inerentemente inseguros e possivelmente hostis. O Aruba ESP com segurança zero-trust aprimora a postura geral da segurança de rede, aplicando um conjunto mais rigoroso de práticas recomendadas e controles de segurança aos recursos de rede anteriormente confiáveis.

ARUBA ESP: PRINCIPAIS CONCEITOS DO ZERO-TRUST

O zero-trust varia significativamente, dependendo de qual domínio de segurança está sendo considerado. Embora os controles no nível de aplicativo tenham sido um ponto focal no zero-trust, uma estratégia abrangente também deve envolver a segurança de rede e o crescente número de dispositivos conectados, incluindo o trabalho em casa. O Aruba ESP com segurança zero-trust incorpora visibilidade abrangente, menos acesso à microssegmentação e controle, além de monitoramento e aplicação contínuos. Até as soluções VPN tradicionais são aprimoradas, garantindo que os mesmos controles aplicados às redes de campus ou filial também sejam estendidas ao trabalho em casa ou remoto.

Na era da IoT, os princípios básicos de boa segurança de rede costumam ser difíceis de implementar. Quando possível, todos os dispositivos e usuários devem ser identificados e autenticados corretamente antes de terem acesso à rede. Além da autenticação, os usuários

e dispositivos devem receber a menor quantidade de acesso necessária para realizar as atividades críticas para os negócios, uma vez que estejam na rede. Isso significa autorizar quais recursos e aplicativos de rede determinados usuários ou dispositivos podem acessar. Por fim, todas as comunicações entre usuários finais e aplicativos devem ser criptografadas.

A NECESSIDADE DE VISIBILIDADE ABRANGENTE

Com o aumento da adoção da IoT, a visibilidade total do espectro de todos os dispositivos e usuários na rede tornou-se uma tarefa cada vez mais desafiadora. Sem visibilidade, é difícil aplicar controles críticos de segurança que são compatíveis com o modelo zero-trust. A automação, o aprendizado de máquina baseado em IA e a capacidade de identificar rapidamente os tipos de dispositivos são essenciais.

O Aruba ClearPass Device Insight usa uma combinação de técnicas ativas e passivas de descoberta e perfil para detectar todo o espectro de dispositivos conectados ou que tentam se conectar à rede. Isso inclui dispositivos comuns

baseados no usuário, como laptops e tablets. A diferença em relação às ferramentas tradicionais é a capacidade de ver o conjunto cada vez mais diversificado de dispositivos de IoT que se tornaram cada vez mais difundidos nas redes de hoje.

ADOÇÃO DE "MENOS ACESSO" E MICROSSEGMENTAÇÃO

Depois que a visibilidade é estabelecida, a aplicação das práticas recomendadas do Zero-Trust relacionadas a "Menos Acesso" e microssegmentação consiste nas próximas etapas essenciais. Isso significa usar o melhor método de autenticação possível para cada endpoint na rede (ou seja, autenticação 802.1X completa e multifator para dispositivos do usuário) e aplicar uma política de controle de acesso que autorize o acesso apenas a recursos absolutamente necessários para esse dispositivo ou usuário.

O Aruba ClearPass Policy Manager viabiliza a criação de políticas de acesso baseadas em funções, que permitem que as equipes de TI e segurança operacionalizem essas práticas recomendadas, usando uma única função e privilégios de acesso associados, que são aplicados em qualquer lugar da rede - infraestrutura com ou sem fio, na filial ou no campus. Após o perfil, os dispositivos recebem automaticamente a política de controle de acesso adequada e são segmentados de outros dispositivos por meio dos recursos de Segmentação dinâmica da Aruba. A aplicação é fornecida pelo Policy Enforcement Firewall (PEF) da Aruba, um firewall de aplicativo completo incorporado à infraestrutura de rede da Aruba. A infraestrutura da Aruba também utiliza os protocolos de criptografia mais seguros, como o padrão WPA3, através de conexões de rede sem fio.

O ClearPass Policy Manager também é integrado a uma ampla variedade de soluções de autenticação, permitindo o uso da autenticação multifator e a capacidade de forçar a reautenticação nos principais pontos da rede. Por meio do ecossistema ClearPass, os clientes também podem incorporar facilmente outras soluções para atender aos requisitos Zero-Trust relacionados a informações contextuais e outra telemetria de segurança.

Isso significa que o ClearPass pode ser integrado a uma ampla gama de soluções, como as ferramentas de segurança de endpoint, para tomar decisões mais inteligentes de controle de acesso com base na postura de um dispositivo. As políticas de controle de acesso também podem ser alteradas com base no tipo de dispositivo que está sendo usado, de onde o usuário está se conectando e em outros critérios baseados em contexto.

MONITORAMENTO E APLICAÇÃO CONTÍNUOS

Com o controle de acesso baseado em função para aplicar a segmentação granular, o monitoramento contínuo de usuários e dispositivos na rede constitui outra prática recomendada do Zero-Trust. Aborda os riscos relacionados a ameaças internas, malware avançado ou ameaças persistentes que contornam as defesas de perímetro tradicionais.

Defesa contra ameaças com IDS/IPS

Os recursos de defesa contra ameaças da Aruba defendem contra uma infinidade de ameaças, incluindo phishing, negação de serviço (DoS) e ataques de ransomware cada vez mais disseminados. Os gateways de SD-WAN 9000 da Aruba realizam a detecção e prevenção de invasão com base em identidade (IDS/IPS), trabalhando em conjunto com o Aruba Central, o ClearPass Policy Manager e o Policy

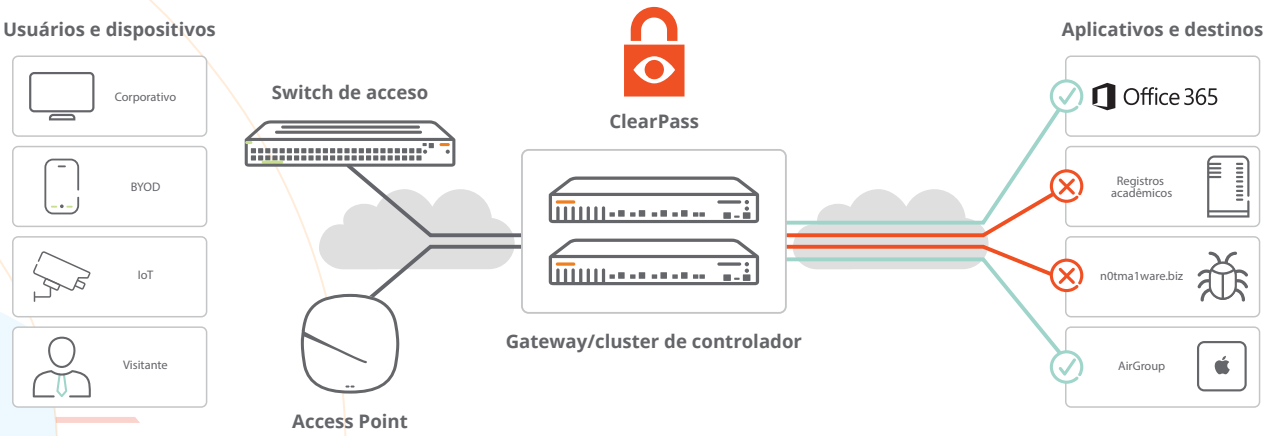

Figura 1: O Aruba ClearPass atribui automaticamente políticas de controle de acesso baseadas em função, que são aplicadas usando a Segmentação dinâmica

Figura 2: A segurança zero-trust é um pilar fundamental do Aruba ESP

Enforcement Firewall. O IDS/IPS com base em identidade realiza a inspeção de tráfego com base em padrões e assinaturas, tanto no tráfego de LAN da filial (leste-oeste) quanto no tráfego de SD-WAN (norte-sul) que flui através do gateway para fornecer segurança de rede da filial integrada. Um painel de segurança avançado no Aruba Central fornece às equipes de TI visibilidade em toda a rede, métricas multidimensionais de ameaças, dados de inteligência de ameaças, bem como correlação e gerenciamento de incidentes. Os eventos de ameaça são enviados aos sistemas SIEM e ClearPass para correção.

360 Security Exchange

Com mais de 150 integrações compostas pelas melhores soluções de segurança, que incluem conjuntos de ferramentas SOAR (Security Operations and Response), o ClearPass Policy Manager pode aplicar dinamicamente o acesso com base na telemetria de ameaças em tempo real proveniente de várias fontes. É possível criar políticas para tomar decisões de controle de acesso em tempo real com base nos alertas de firewalls de próxima geração (NGFWs), ferramentas de gerenciamento de informações e eventos de segurança (SIEM) e muitas outras fontes. As ações do ClearPass são totalmente configuráveis, desde a limitação do acesso (ou seja, apenas à Internet) até a remoção total de um dispositivo da rede para correção.

ARUBA ESP (PLATAFORMA DE SERVIÇOS EDGE)

Para ajudar nossos clientes a aproveitar as oportunidades no Edge, desenvolvemos o Aruba ESP, a primeira plataforma baseada em IA do setor, criada para unificar, automatizar e proteger o Edge. A segurança zero-trust é um componente essencial do Aruba ESP e, quando combinada com a AIOps e uma infraestrutura unificada, permite que as empresas reduzam os custos, simplifiquem as operações e mantenham a segurança.

RESUMO

O ambiente de rede e o cenário de ameaças de hoje exigem uma abordagem diferente. A segurança de rede centralizada no perímetro do passado não foi criada para a força de trabalho móvel ou os dispositivos de IoT emergentes da atualidade. O Aruba ESP com segurança zero-trust fornece um conjunto abrangente de recursos que abrangem visibilidade, controle e aplicação para atender aos requisitos de uma infraestrutura de rede descentralizada e orientada para a IoT.

SO_ZeroTrustSecurity_051120 a00097694enw