Arquitetura baseada em Confiança Zero
O que é, e como chegar lá

Alcatel·Lucent
Enterprise

e-Book
Arquitetura baseada em Confiança Zero

Índice

O que é arquitetura baseada em confiança zero?

O que significa arquitetura baseada em confiança zero (ZTA)? Significa que todos os usuários e dispositivos devem ser autenticados e autorizados antes que o acesso aos dados seja permitido. É uma estratégia de 'não confiar em ninguém, e autenticar tudo'.

Uma analogia pode ajudar a entender melhor.

Se pensarmos na segurança tradicional como uma fortaleza que protege um vilarejo, construiríamos a muralha da fortaleza (também conhecido como firewall) ao redor do vilarejo (também conhecido como empresa). Qualquer coisa que venha de fora da fortaleza não é confiável e é escrutinada, mas qualquer coisa dentro da fortaleza é implicitamente confiável e permitida. Esse limite de confiança é tanto físico quanto implícito, dependendo de qual lado da fortaleza você está. Enquanto você estiver no lado “certo” da parede, nenhuma verificação adicional é necessária. Se pensarmos nessa abordagem em termos de rede corporativa, pode haver alguma segmentação básica na forma de VLANs, SSIDs, sub-redes ou interfaces vinculadas a um firewall, mas essa segmentação é estática e tem mais a ver com escalabilidade e gerenciamento de rede do que com segurança.

Hoje, porém, a abordagem de firewall (fortaleza) está se tornando menos eficaz por conta própria, por vários motivos. A primeira é a mobilidade. Os usuários se conectam a outras redes fora da empresa e podem trazer ameaças com eles. Em segundo lugar, os visitantes na rede não são necessariamente confiáveis. Alguém poderia argumentar que mesmo os funcionários (aqueles dentro da fortaleza) não devem ser considerados totalmente confiáveis. Em terceiro lugar, mais e mais dispositivos IoT estão sendo adicionados à rede. Eles representam riscos de segurança mais altos porque podem não ser sancionados e gerenciados pela TI e geralmente não possuem recursos de segurança. Com a abordagem tradicional de 'fortaleza/vilarejo', 'firewall/empresa', se um usuário ou dispositivo for comprometido, há pouco ou nada impedindo que a ameaça se espalhe para outros usuários e dispositivos. Uma vez dentro, você está livre para se movimentar.

Na analogia da fortaleza, se a única coisa que protege o vilarejo de intrusos é a muralha, no dia em que os invasores aprenderem a escalar a muralha da fortaleza – e eles irão – será um desastre.

A questão é: o que podemos fazer? Vamos pensar sobre isso a partir da abordagem de 'não confiar em ninguém' ou 'confiança zero'.

Com confiança zero, nenhum usuário ou dispositivo é confiável. Quer estejam no local ou fora dele, eles passam pelas mesmas verificações. Não existe uma confiança pré-estabelecida nos usuários internos. Todo acesso é autenticado e autorizado.

Na analogia da fortaleza, isso significaria que, além da fortaleza que protege o vilarejo de ameaças externas, cada casa, cada edifício, tem sua própria segurança para proteger-se dos riscos vindos de habitantes nefastos que vivem dentro da fortaleza. Em termos empresariais, o que é conhecido como microssegmentação definida por software nos leva um passo à frente. Além da fortaleza e da segurança ao redor das construções, também temos seguranças pessoais que nos seguem por onde andarmos. E onde quer que formos, nos pedirão nosso passaporte. Na rede corporativa, esse limite de confiança é difuso, distribuído e móvel. Não está vinculado a um local específico, porta de switch ou VLAN. Depende da identidade, do dispositivo, da situação e da hora do dia, entre outras coisas. É definido por software e ajustado em tempo real. Nesta abordagem, os componentes precisam ser gerenciados e devem ser capazes de reagir e reconfigurar-se conforme necessário para responder a ameaças ou mudanças no fluxo de trabalho.

Compreendendo a macro e microssegmentação

Em uma arquitetura de confiança zero, existem dois tipos de segmentação: macro e microssegmentação. Nos termos da nossa analogia, a muralha da fortaleza é a macrossegmentação, e os seguranças pessoais são a microssegmentação.

Na **macrossegmentação**, a rede física é dividida em diferentes segmentos lógicos. Esses segmentos podem ser uma VLAN, uma combinação de VLAN e VRF, também pode ser uma VPN quando se fala de Shortest Path Bridging, MPLS, ou mesmo túneis VXLAN ou GRE. Qualquer tráfego entre usuários ou dispositivos em diferentes segmentos é controlado por um firewall. Todas as empresas usam a segmentação de alguma forma, mas nem sempre por motivos de segurança. Muitas vezes, esse tipo de segmentação é usado por motivos de escalabilidade, administrativos ou organizacionais. Se dois dispositivos estiverem mapeados para VLANs diferentes, mas puderem se comunicar sem passar por um firewall, eles estarão no mesmo macrossegmento. Um exemplo típico desse tipo de segmentação é a telefonia IP em execução em VLANs e VRFs separados, logicamente isolados dos PCs.

A questão é: como você mapeia usuários ou dispositivos para esses segmentos? Embora possa ser feito estaticamente, por porta de switch ou SSID, por exemplo, é realmente uma maneira obsoleta de operar. É muito rígido, e não é uma boa escolha para usuários móveis. Idealmente, você teria um sistema de autenticação definido por software para que, quando um usuário ou dispositivo se conectar e autenticar, ele seja associado a um perfil. O perfil colocará o usuário ou dispositivo no segmento certo, independentemente da localização física, porta do switch ou SSID.

Embora a macrossegmentação tenha benefícios de segurança, em muitos casos ela é feita por motivos organizacionais ou administrativos. Por exemplo, câmeras e fechaduras estão sob o controle do grupo de segurança de acesso, enquanto os termostatos estão sob o controle do grupo de manutenção predial.

A microssegmentação nos leva um passo à frente. Nem todos os usuários são iguais e nem todos os usuários têm uma necessidade legítima de acessar todos os recursos. O mesmo perfil que mapeia usuários para um segmento também inclui um conjunto de políticas que adicionam controle refinado sobre privilégios de usuário/dispositivo que são diferentes para diferentes funções, como RH versus Finanças. Isso é conhecido como **acesso baseado em função** e está diretamente relacionado ao **princípio de privilégios mínimos**. E assim, embora as câmeras e as fechaduras estejam no mesmo segmento, elas não precisam usar os mesmos recursos. A câmera precisa se comunicar com o gravador de vídeo e a fechadura da porta com seu servidor. Não há necessidade de uma câmera se comunicar com a fechadura, da mesma forma que não há necessidade de que uma fechadura se comunique com outra fechadura. Essas permissões refinadas são implementadas por meio de políticas que fazem parte do perfil, e são aplicadas dinamicamente ao dispositivo após a autenticação.

A microssegmentação precisa ser definida por software por vários motivos. Nem os usuários nem os dispositivos IoT são estáticos. Eles se movem, conectam e desconectam, e as políticas não podem ser vinculadas a um local ou uma porta. Na verdade, as configurações de microssegmentação precisam ser dinâmicas com base na combinação de vários fatores, incluindo, entre outros, a identidade do usuário ou dispositivo, a hora do dia e o local.

Em resumo, quando a comunicação entre diferentes segmentos é controlada por um firewall, trata-se de macrossegmentação. Quando a comunicação dentro do mesmo segmento é controlada por políticas de controle de acesso à rede (NAC) associadas ao dispositivo ou à função do usuário, trata-se de microssegmentação.

Por que você precisa de ambas

O que acontece se você usar apenas um tipo de segmentação?

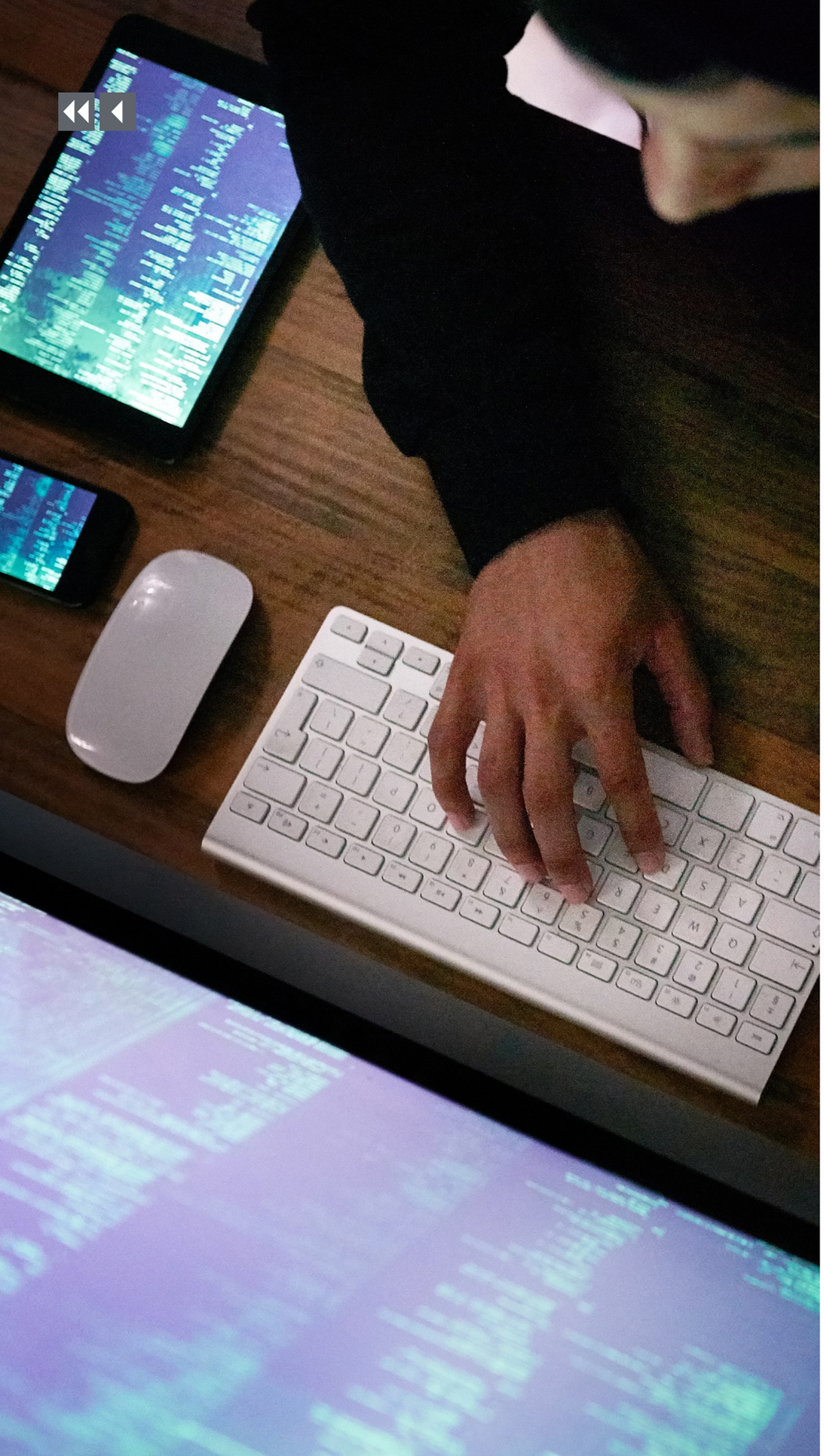
Vejamos a macrossegmentação. O problema de usar apenas essa abordagem é que o firewall se torna um gargalo, pois todo o tráfego precisa passar pelo firewall para autenticação e autorização. Isso pode levar a problemas de desempenho. Você pode implantar mais firewalls na camada de distribuição, mas isso pode ser bastante caro e não necessariamente melhorar o desempenho, pois os firewalls não têm taxa de transmissão. Além disso, agora existem vários pontos de aplicação de políticas e vários locais para manter as políticas atualizadas, tornando o gerenciamento mais complicado.

A outra opção, usando apenas a microssegmentação, também é problemática. Se a única aplicação da política for feita por meio de políticas NAC, essas listas de políticas se tornarão muito longas e complexas, e você poderá esgotar os limites de capacidade do dispositivo.

A conclusão é que é melhor ter um equilíbrio entre essas duas formas de segmentação. Deixe o firewall controlar qualquer tráfego entre diferentes segmentos (vertical) e deixe que as políticas NAC controlem o tráfego dentro de um determinado segmento (lateral).

Ao combinar esses dois, você pode agir sobre as ameaças de segurança que se espalham de um segmento de segurança para outro, assim como aquelas que se movem lateralmente no mesmo segmento. Em termos mais tangíveis, a microssegmentação é o que impede um invasor que conseguiu comprometer uma câmera de usar a violação como um pivô para comprometer outros recursos, como uma fechadura de porta.

O objetivo é autenticar cada conexão e atribuir permissões a cada usuário ou dispositivo. Isso significa usar segmentação para evitar a propagação de ameaças por meio de movimento lateral e monitoramento contínuo e quarentena de qualquer usuário ou dispositivo que se torne incompatível.



Como chegar lá

Em uma situação de "greenfield", seria relativamente fácil construir uma arquitetura de confiança zero usando microssegmentação desde o início. Mas, em situações "brownfield", a adaptação da rede com microssegmentação pode resultar no bloqueio de usuários, dispositivos e aplicativos da rede devido a falhas de autenticação ou políticas incompletas. Seria difícil ou mesmo improvável que uma empresa pudesse migrar de uma só vez — em um único ciclo de atualização.

Em ambientes brownfield, haverá um período durante o qual as arquiteturas de confiança não zero e confiança zero coexistirão, e a migração ocorrerá em uma camada ou um local por vez. O importante é garantir que os elementos de infraestrutura implantados e a maneira como são implantados sejam flexíveis e capazes de operar em modo confiança zero ou microssegmentado quando outros elementos de infraestrutura estiverem prontos. Isso significa que a infraestrutura precisará interoperar com componentes existentes e futuros.

A metodologia

Há cinco etapas em direção a uma arquitetura de confiança zero – monitorar, validar e avaliar, planejar, simular e aplicar.

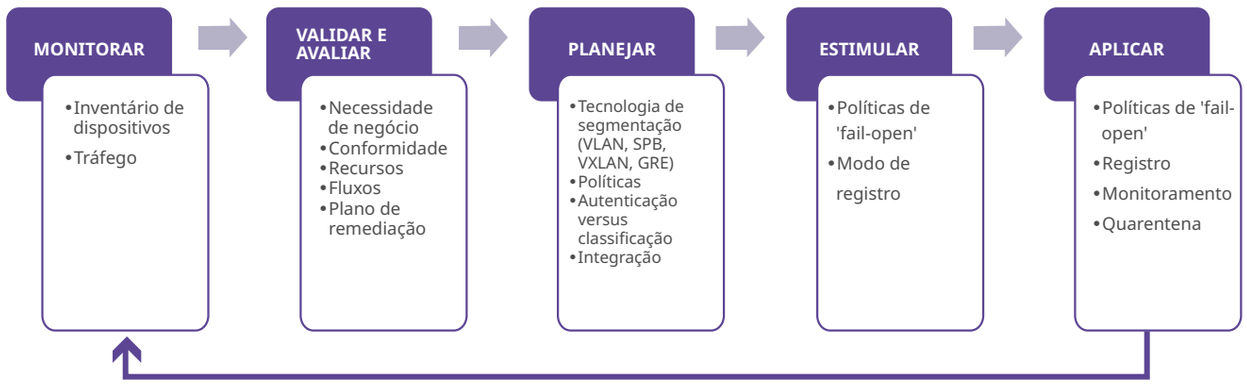


Figura 1 - A metodologia

Etapa 1: Monitorar

Antes de qualquer outra coisa, você precisa começar a monitorar, e construir um mapa e inventário do que você tem em sua rede.

A migração para ZTA requer conhecimento detalhado dos ativos (físicos e virtuais), assuntos (incluindo privilégios de usuário) e processos de negócios que circulam na rede. O conhecimento incompleto na maioria das vezes leva a falhas onde o acesso é negado devido a informações insuficientes. Isso é especialmente um problema se houver equipamentos “shadow IT” (TI invisível) ou “shadow IoT” (IoT invisível) desconhecidos dentro da organização.

Comece a monitorar dispositivos e fluxos de tráfego. Crie um relatório de inventário com todos os dispositivos vistos na rede, categorizados por tipo de dispositivo, fabricante, modelo, sistema operacional, entre outros. O relatório também deve mostrar onde e em qual porta do switch ou SSID o dispositivo foi visto pela última vez. Essas informações podem ser obtidas a partir de elementos como endereço MAC, assinatura DHCP e agente de usuário HTTP.

A maioria das ferramentas de terceiros fornecerá apenas um endereço IP e não o tipo de equipamento. Seria ideal ter uma ferramenta para criar um inventário de IoT/dispositivo para facilitar a criação rápida e fácil do perfil NAC para cada tipo de dispositivo.

A outra informação necessária para a criação de políticas são os fluxos de tráfego. Dependendo do equipamento que você possui, você pode obter essas informações de ferramentas de monitoramento de fluxo, como sFlow, Netflow ou Deep Packet Inspection (DPI).

Este processo será frequente. Na primeira vez que você ativar o monitoramento, os relatórios podem não ser tão significativos, mas conforme você avança para as outras etapas, eles se tornarão mais específicos e úteis. As informações coletadas nesta etapa serão fundamentais para as próximas etapas.

Etapa 2: Validar e avaliar

O próximo passo é validar esses achados. Avalie as necessidades de negócio. Qualquer shadow IoT que não possa ser justificado deve ser eliminado, pois aumenta desnecessariamente a superfície de ataque. Para o resto, você precisa identificar os assuntos (usuários e dispositivos), os fluxos de tráfego e os fluxos de trabalho, pois eles precisarão ser refletidos em suas políticas. Por exemplo, quem terá acesso a ativos específicos e o que eles poderão fazer com esses ativos. Aplique o princípio do privilégio mínimo.

A microssegmentação não significa relaxar outras políticas de segurança, como políticas de senha ou atualizações de firmware. As capacidades individuais precisam ser avaliadas. Esses dispositivos podem suportar autenticação baseada em certificado? Existe uma ferramenta de gerenciamento que permita a emissão e aplicação desses certificados? Quais são os fluxos de tráfego necessários? Você pode precisar obter essas informações do fabricante, mas também deve compará-las com seus próprios relatórios de análise de tráfego. Se você encontrar ativos que não estejam em conformidade com a política da empresa, precisará de um plano de correção para torná-los compatíveis ou precisará de controles adicionais em operação.

Etapa 3: Planejar

Neste estágio você já conhece os ativos, os assuntos (usuários), o tráfego e os fluxos de trabalho. Agora você precisa transformar esse conhecimento em políticas de autenticação e segurança para implementar a arquitetura de microssegmentação necessária. Como mencionado anteriormente, para obter melhores resultados, você deve incluir uma combinação de macro e microssegmentação. Lembrando que na maioria dos cenários "brownfield" você estará limitado pela arquitetura que já está em vigor.

Para macrossegmentação, existem várias opções, como VLANs, VRFs, SPB VPNs, VXLAN ou túneis GRE e recursos especiais, como VLAN privada. Cada um deles tem seus prós e contras e pode ser útil em diferentes situações. Para microssegmentação, você precisará saber quais políticas incluir no perfil para cada usuário ou tipo de dispositivo. Por fim, você precisará definir como mapear usuários e dispositivos para seus segmentos e políticas. Isso se resume à autenticação ou classificação, que pode incluir a impressão digital do dispositivo.

Idealmente, você deve investir em tecnologia (segmentação definida por software) que permita criar políticas de autenticação flexíveis, para que você possa atualizar facilmente os perfis da rede.

Sugerimos que você crie o fluxo de autenticação nesta ordem:

1. Autenticação por meio de certificados 802.1x usando o servidor RADIUS. A autenticação gera um registro de autenticação. Essas são informações que podem ser compartilhadas com um firewall.
2. Se você não conseguir autenticar o dispositivo por meio de certificados 802.1x, tente a autenticação MAC em seguida. A autenticação MAC não é tão segura quanto 802.1x, mas é melhor do que nenhuma autenticação. Use-a até que esteja pronto para progredir para 802.1x.
3. Se nenhum perfil for retornado, você pode tentar a impressão digital, que também pode ser usada para mapear para um segmento de perfil e regras. Isso não gera um registro de autenticação ou contabilidade, mas é registrado no banco de dados de inventário de IoT.
4. Por último, você pode ter um padrão “pegar tudo” caso os perfis não sejam retornados, ou se tudo mais falhar. Nos estágios iniciais, você ainda precisará mapear o dispositivo para um perfil que levará ao mesmo segmento e regras e registrará o dispositivo no banco de dados de inventário.

Esse fluxo deve ser estruturado de maneira flexível para que você possa ajustá-lo à medida que avança. Por exemplo, você pode querer eliminar a autenticação MAC primeiro e adicioná-la mais tarde, depois de obter a lista de endereços MAC contida no relatório de inventário. E à medida que você refina o processo, você pode, por exemplo, alterar o segmento e as regras associadas ao perfil padrão para regras muito restritivas, permitindo acesso apenas a um 'bastion host'.

Você também pode compartilhar a função do dispositivo com o firewall para que as regras do firewall possam ser baseadas na função do dispositivo e não apenas no endereço IP/sub-rede. A vantagem desta integração é dupla. Em primeiro lugar, o firewall pode aplicar políticas refinadas a esses dispositivos IoT. Em segundo lugar, as políticas de firewall agora são baseadas em usuário ou função e, portanto, não estão mais vinculadas a uma sub-rede ou endereço IP, o que permite um novo projeto e nova segmentação futuros da rede.

O processo será constante e você precisará ajustar e refinar à medida que se tornar mais maduro no uso de autenticação e segmentação.

Passo 4: Simular

Não importa o quanto você planeje, é improvável que você acerte na primeira vez. Qualquer erro no projeto do esquema de autenticação, qualquer omissão que você fizer na 'lista de permissões' da política de segurança resultará em um processo de negócios interrompido. Você precisará aplicar as políticas de autenticação e acesso em um modo 'fail-open'. O que isso significa é que os dispositivos e usuários que falharem na autenticação ainda serão permitidos na rede e fluxos de tráfego inesperados ainda serão permitidos. Mas tudo isso será registrado, e com esses logs você pode refinar os esquemas de autenticação e políticas.

Etapa 5: Aplicar

Após alguns ajustes, você não observará mais falhas de autenticação ou negação de fluxos legítimos. Você pode então mover essas políticas de 'fail-open' para 'fail-close', o que significa que os dispositivos não autorizados serão bloqueados e os fluxos inesperados serão descartados.

Desnecessário dizer que você precisará continuar monitorando quaisquer dispositivos e fluxos de tráfego inesperados – repetindo todo o ciclo conforme necessário.

E mais

Como parte do monitoramento contínuo, registro e quarentena, recomendamos que você também invista em um Sistema de Detecção de Intrusão (IDS) externo. Embora haja uma variedade de ataques Distributed Denial of Service (DDoS) que podem ser identificados diretamente pelo próprio switch, um IDS externo também pode detectar uma variedade mais ampla de ataques, como vírus ou outras anomalias. Você deve se lembrar de alguns anos atrás quando várias câmeras de vigilância por vídeo foram infectadas com o malware Mirai, ou o dia em que esses dispositivos lançaram um ataque coordenado em servidores DNS globais que afetaram serviços como Twitter, Spotify ou PayPal. Esses ataques podem não ser detectados por seus switches, mas por um IDS dedicado certamente será.

Assim que o ataque for detectado, o IDS informará ao seu sistema de gerenciamento de rede (NMS) os endereços IP dos dispositivos afetados. Idealmente, seu NMS seria capaz de localizar esses dispositivos em seu banco de dados e alteraria seus perfis para uma 'função de quarentena'.

A 'função de quarentena' é uma função muito restritiva, e normalmente só permitiria a comunicação com um 'bastion host' para que o dispositivo pudesse ser remediado, por exemplo, definindo uma senha forte ou atualizando seu firmware, entre outros.

Por que a ALE?

As soluções Digital Age Networking da Alcatel-Lucent Enterprise incorporam segmentação definida por software robusta e flexível com políticas DPI NAC dinâmicas que permitem evolução passo-a-passo para uma arquitetura de confiança zero.

A Digital Age Network é o modelo da Alcatel-Lucent Enterprise que permite que empresas e organizações entrem na era digital e expandam seus negócios digitais. Baseia-se em três pilares:

- Uma Rede Autônoma que conecta pessoas, processos, aplicações e objetos de forma fácil, automática e segura. A Rede Autônoma da ALE baseia-se em um portfólio simplificado e completo com uma verdadeira plataforma de gerenciamento unificada, fornecendo políticas de segurança comuns em nossa LAN e WLAN. A Rede Autônoma também oferece flexibilidade de implantação em ambientes internos, externos e industriais. O gerenciamento da rede pode ser realizado no local, na nuvem ou em uma implantação híbrida, dependendo da preferência do cliente.
- Integração segura e eficiente de dispositivos IoT: A segmentação mantém os dispositivos em seus segmentos dedicados e minimiza o risco de ter o dispositivo e a rede comprometidos. A segmentação de IoT pode ajudar a empresa a entender, de maneira fácil e automática, se o dispositivo está se comportando adequadamente ou não, e ajuda a manter a rede segura.
- Inovação nos Negócios por meio da automação do fluxo de trabalho: a integração de usuários, aplicativos e métricas de IoT em tempo real, com dados de geolocalização, em plataformas de colaboração, simplifica a criação e a implantação de novos processos e serviços de negócios digitais automatizados, incluindo a notificação de segurança e administradores de rede sobre quaisquer violações à medida que elas acontecem.

Você tem uma ferramenta para criar um inventário de dispositivos/IoT? Você tem uma ferramenta que permite monitorar os fluxos de aplicativos? Seus switches e access points atuais estão preparados para segmentação definida por software? Se atualmente você não conta com essas ferramentas, entre em contato conosco e podemos ajudá-lo a obtê-las.

O que sabemos com certeza

Vamos encerrar com algumas dicas importantes:

- Para ter uma ZTA (Arquitetura baseada em Confiança Zero) realmente eficiente, você deve usar macro e microssegmentação
- Existem cinco etapas para uma ZTA: monitorar, validar e avaliar, planejar, simular e aplicar
- A ZTA baseada em microssegmentação se apoia em três pilares: Autenticação, com 802.1x EAP-TLS como padrão ouro; políticas diferenciadas associadas à função de usuário ou dispositivo que remontam ao princípio de privilégio mínimo; e monitoramento contínuo e quarentena
- Em ambientes híbridos e móveis, a microssegmentação deve ser definida por software, ou seja, deve ser dinâmica e baseada em políticas, não definida estaticamente, caso contrário seria impraticável

Migrar para uma ZTA por meio de microssegmentação é um processo, e é improvável que uma empresa de tamanho significativo chegue lá em um único ciclo de atualização. Mas em cada atualização, redesenho ou ciclo de melhoria contínua, você pode se aproximar desse objetivo se implementar a infraestrutura e o design certos.

A Alcatel-Lucent Enterprise está empenhada em desenvolver tecnologia e soluções de rede que ajudem as organizações a concretizar o seu potencial de negócios através da transformação digital.

Alcatel·Lucent
Enterprise