Resumo da solução

Acesso seguro ao SAP para cadeia de suprimentos e terceiros com o Zscaler Private Access (ZPA)

Empresas globais com operações de cadeia de suprimentos e ativos de OT e IIoT exigem que usuários terceirizados, como prestadores de serviço e parceiros, tenham acesso ágil e conectado a aplicativos internos de gerenciamento de negócios da SAP. Para maximizar o tempo de atividade da produção e evitar interrupções por falhas de equipamentos e processos, as organizações precisam considerar uma abordagem moderna de acesso do usuário que forneça:

1. Acesso remoto seguro e sem agentes aos usuários da cadeia de suprimentos que acessam produtos SAP por meio de um navegador web a partir de dispositivos não confiáveis ou não gerenciados, como dispositivos pessoais, prestadores de serviço, trabalhadores de chão de fábrica, etc.
2. Uma redução nos riscos de exposição à superfície de ataque do aplicativo SAP ao conceder acesso à cadeia de suprimentos para aplicativos corporativos, ou seja, os usuários são conectados diretamente ao aplicativo SAP sem expor outros aplicativos ou a rede corporativa
3. Garantia de que as políticas de acesso global sejam aplicadas de forma consistente, mantendo a visibilidade do usuário e limitando permissões de acesso excessivas

No entanto, o risco de estender o acesso a terceiros é grande e as cadeias de suprimentos são alvos fáceis para ransomware e outros ataques sofisticados. Quando ocorrem interrupções, por menores que sejam, elas produzem efeitos em cascata que podem impactar a economia global. Para mitigar riscos, as empresas contam com VPNs para acessar os aplicativos SAP ERP necessários. Entretanto, em muitos casos, a implantação de um cliente de acesso remoto não é possível ou requer infraestrutura de TI adicional. Além disso, os parceiros podem não ter os privilégios necessários no nível do dispositivo para instalar esses clientes ou simplesmente não estarem dispostos a fazê-lo.

Apresentamos o Zscaler Private Access (ZPA)

Quando o acesso ao SAP é crucial para as operações da cadeia de suprimentos, o acesso por navegador sem agentes permite que você utilize um navegador web para autenticação de usuário e acesso a aplicativos pelo Zscaler Private Access (ZPA), sem exigir que os usuários se conectem a VPNs de site para site ou instalem o Zscaler Client Connector em seus dispositivos. Isso é pertinente para usuários terceirizados, como prestadores de serviço e parceiros, cuja organização de TI não permite clientes externos ou cujo sistema de BYOD (traga seu próprio dispositivo) não seja compatível com clientes.

Para muitos clientes, como a **Schmitz Cargobull**, uma fabricante inovadora, acessar aplicativos SAP internos usando VPNs não era mais viável após várias falhas de acesso que colocaram em risco operações sigilosas da cadeia de suprimentos. Após utilizar o ZPA para oferecer acesso seguro ao SAP ERP, Michael Schöller, chefe de infraestrutura, observou que "**os funcionários e terceiros podem acessar sistemas SAP de forma segura e confiável sem expor toda a rede**". Quando as políticas de zero trust são aplicadas por padrão em todos os dispositivos, locais e aplicativos, os parceiros nunca são inseridos na rede e o aplicativo nunca é exposto à internet. Ao limitar o uso não autorizado, os usuários são mais produtivos e as organizações são protegidas contra movimentações laterais injustificadas. Os administradores do ZPA podem contar com o serviço para visibilidade em tempo real das atividades dos usuários, identificar usuários que acessam aplicativos por meio do acesso por navegador e descobrir aplicativos anteriormente desconhecidos.

Benefícios da Zscaler para SAP

- **Proteja o acesso de usuários e dispositivos sem agentes ao SAP:** nunca coloque usuários de terceiros ou ferramentas da cadeia de suprimentos em sua rede corporativa, reduzindo a exposição a riscos e movimentação lateral.
- **Estenda o zero trust para aplicativos, cargas de trabalho e IoT:** aproveite um único mecanismo de política global para fornecer acesso rápido e direto a aplicativos SAP privados, cargas de trabalho e dispositivos de OT/IIoT.
- **Ofereça uma experiência de usuário do SAP superior:** aumente a produtividade das suas equipes híbridas e resolva proativamente problemas de experiência do usuário com o monitoramento e a visibilidade contínuos do ZDX.
- **Mitigue os riscos de violação de dados:** torne os aplicativos SAP invisíveis para usuários não autorizados e aplique o acesso de privilégio mínimo, minimizando a superfície de ataque do aplicativo SAP S/4HANA.
- **Reduza a complexidade operacional e os custos:** sem hardware ou software para gerenciar, as implantações de acesso à rede zero trust (ZTNA) fornecidas pela nuvem eliminam a sobrecarga de infraestrutura.

Como funciona o acesso sem agentes do ZPA

Design da cadeia de suprimentos do ZPA/SAP

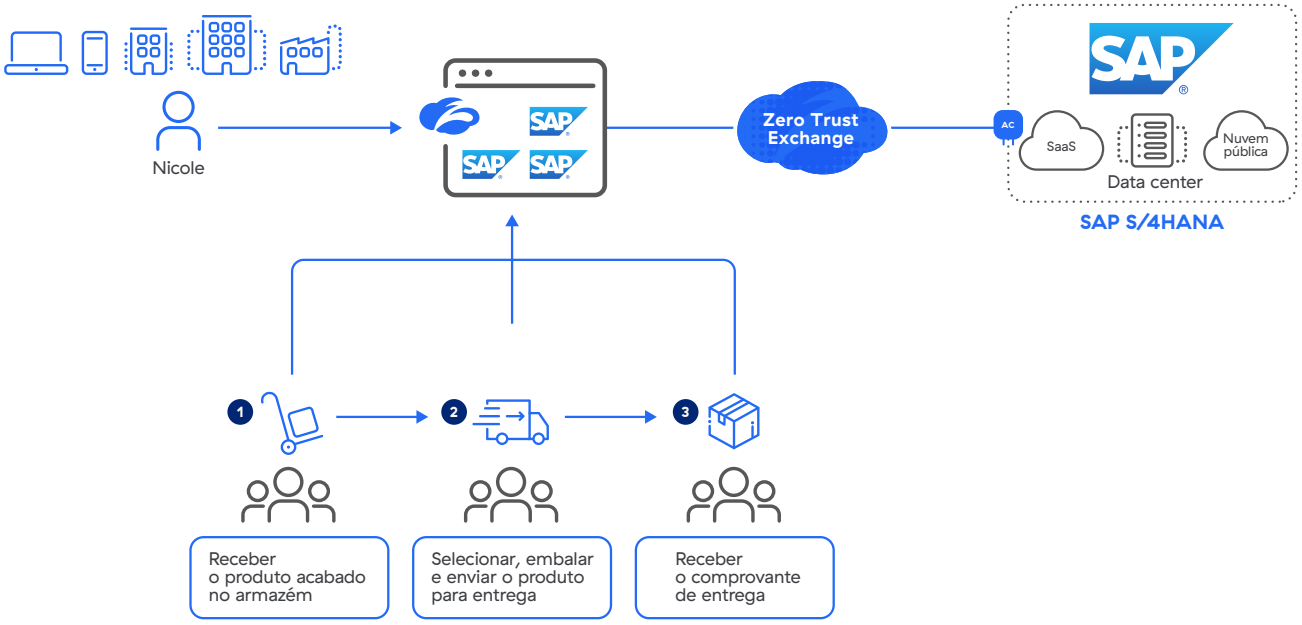


Figura 1: funcionários e usuários terceirizados na cadeia de suprimentos acessando aplicativos SAP com o ZPA Browser Access

Componentes do ZPA/SAP

- Os App Connectors fornecem uma interface segura e autenticada entre os servidores de aplicativos de uma organização e a nuvem do ZPA.
- A plataforma Zscaler Zero Trust Exchange (ZTE) oferece conexões rápidas e seguras e permite que seus funcionários trabalhem de qualquer lugar usando a internet como rede corporativa. A Zero Trust Exchange consiste em 150 data centers em todo o mundo, garantindo que o serviço esteja próximo de seus usuários, co-localizado com os provedores de nuvem e aplicativos que eles estão acessando, como Microsoft 365 e AWS. Ela garante a rota mais curta entre seus usuários e seus destinos, fornecendo segurança abrangente e uma experiência de usuário incrível.
- Os portais de usuário de acesso por navegador fornecem aos usuários e dispositivos sem agentes acesso a aplicativos autorizados para funcionários ou parceiros de uma organização.
- Os aplicativos são um nome de domínio totalmente qualificado (FQDN), nome de domínio local ou endereço IP que você define em um conjunto padrão de portas. Os aplicativos devem ser definidos dentro de um segmento de aplicativos.
- O segmento de aplicativos é um agrupamento de aplicativos definidos, com base no tipo de acesso ou privilégios do usuário.
- As políticas no ZPA controlam como os usuários acessam os aplicativos. Antes que um usuário possa acessar um aplicativo, uma política deve ser definida. Há muitos tipos de políticas. Consulte nosso link de recursos para obter mais informações sobre os tipos de políticas.

- **Um Zscaler Tunnel (Z-Tunnel)** é uma conexão ponto a ponto criptografada por TLS e mutuamente autenticada entre o Zscaler Client Connector e um ZPA Public Service Edge gerenciado pela Zscaler, ou entre um App Connector e um ZPA Private Service Edge gerenciado por uma organização. Um Z-Tunnel não contém nenhum dado de IP direto. Além disso, o Z-Tunnel pode transportar dentro dele vários canais de comunicação chamados Microtunnels.
- **Um Microtunnel (M-Tunnel)** é um canal de comunicação de ponta a ponta criado entre o Zscaler Client Connector e um aplicativo interno por meio de um ZPA Public Service Edge ou ZPA Private Service Edge e um App Connector mediante demanda.
- **Servidores de aplicativos SAP** são servidores que hospedam aplicativos SAP.

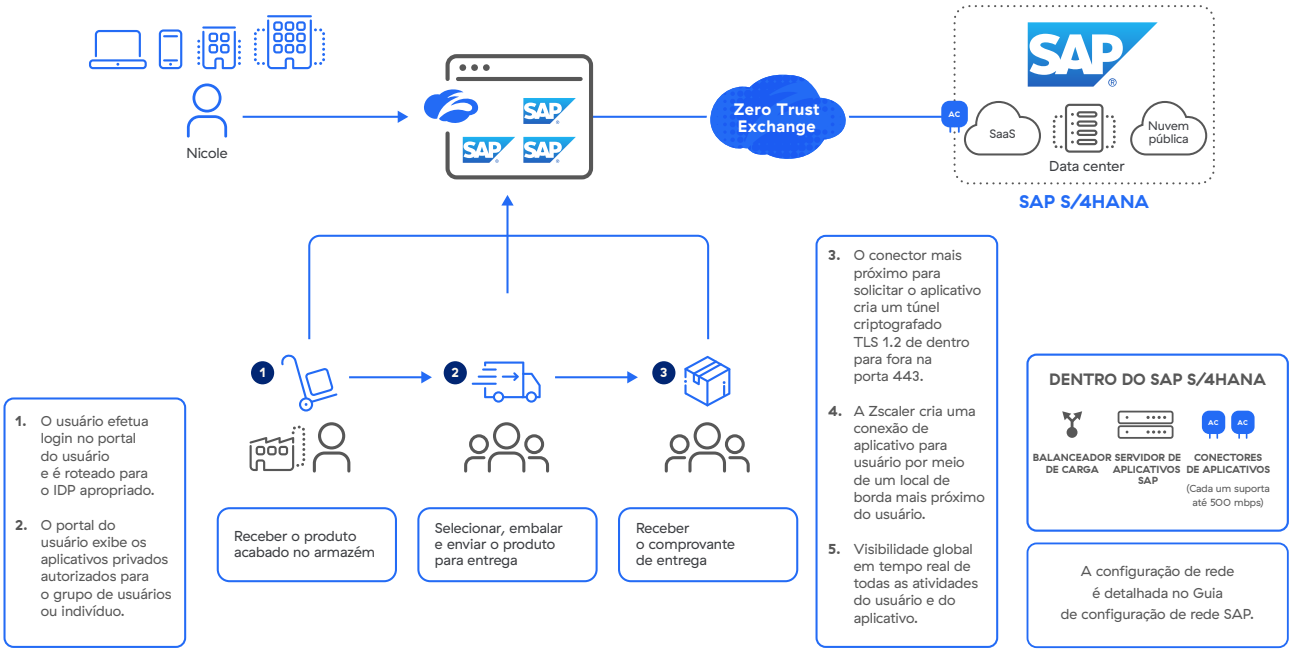
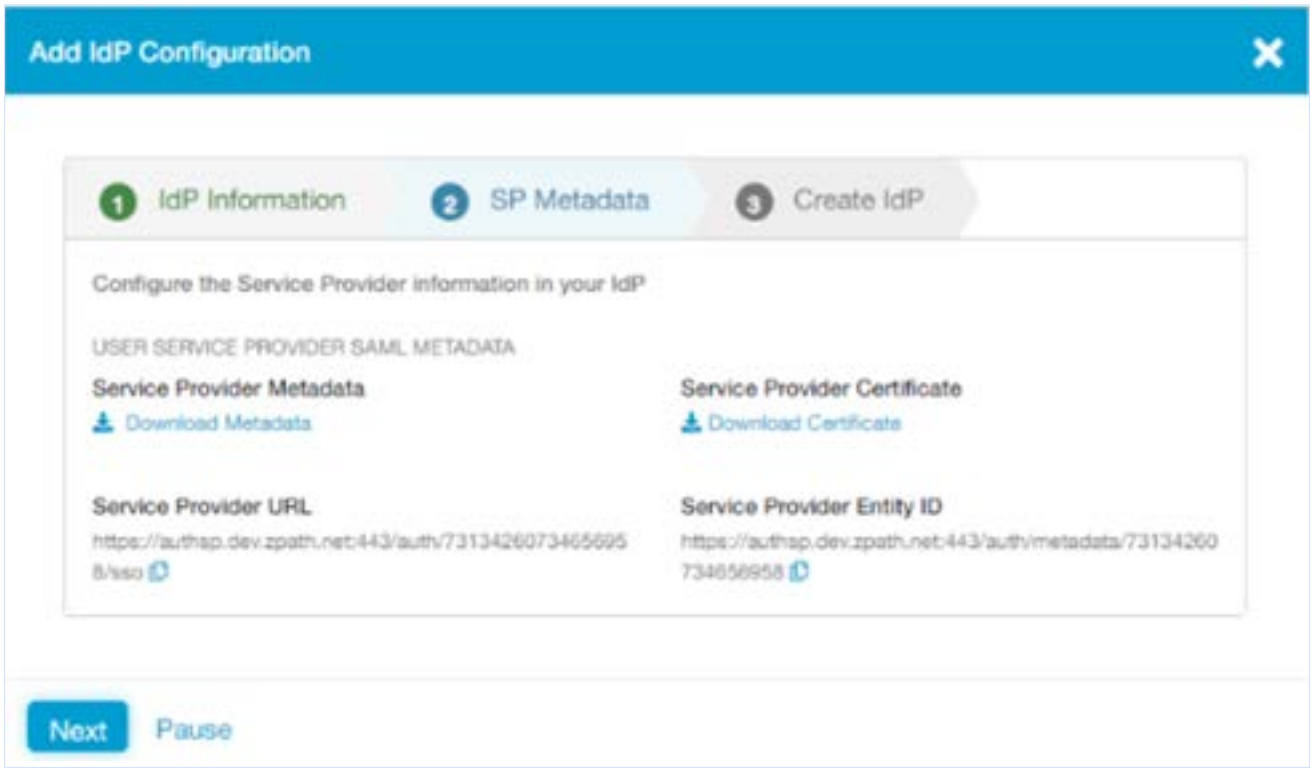


Figura 2: funcionários e usuários terceirizados na cadeia de suprimentos acessando aplicativos SAP com o ZPA Browser Access (detalhes adicionais)

As figuras 1 e 2 descrevem uma implantação do ZPA para um ambiente SAP híbrido. Nicole é uma funcionária da ACME que precisa rastrear produtos conforme eles passam pela cadeia de suprimentos. Paul é funcionário de um depósito que armazena produtos da ACME antes de serem enviados aos clientes. Quando Paul recebe uma remessa, ele alerta a ACME e Nicole por meio de um portal de acesso por navegador do ZPA. Paul navega até o portal do usuário da ACME em seu tablet e é redirecionado para seu Provedor de Identidade (IDP). Após a autenticação de Paul, o portal do usuário exibirá os aplicativos apropriados para Paul. Paul seleciona o aplicativo SAP de que precisa e, nos bastidores, o App Connector mais próximo do aplicativo SAP solicitado cria um Z-Tunnel, uma conexão criptografada em TLS, com a nuvem da Zscaler. A nuvem da Zscaler então costura a conexão do portal do usuário ao aplicativo SAP. Paul agora tem acesso e pode atualizar a ACME e Nicole sobre a localização de seus produtos. É importante observar que Paul não precisa de um dispositivo específico da ACME, o dispositivo não tem agentes e pode ser não gerenciado ou não confiável, e só precisa de um navegador web para acessar a porta de acesso por navegador do ZPA para se conectar aos aplicativos SAP.

Introdução ao acesso sem agentes do ZPA para SAP

Etapa 1: configurar autenticação de logon único (SSO) e IDP

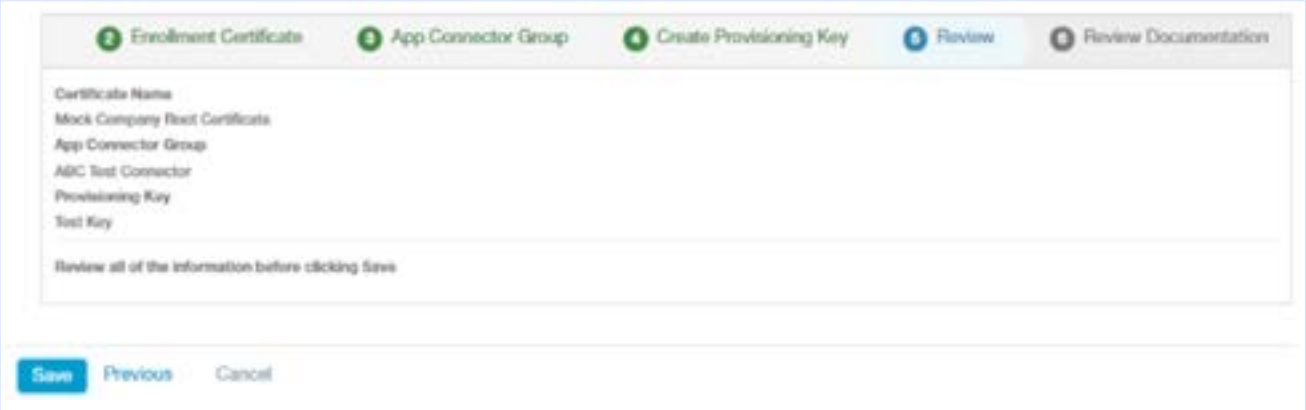


O ZPA aproveita as identidades de usuários do Provedor de Identidade (IdP) existente de uma organização e pode ser configurado para oferecer suporte a uma ou várias soluções de IdP. O ZPA oferece suporte ao logon único (SSO) via SAML para que seus usuários remotos possam acessar aplicativos corporativos sem precisar fazer login separadamente no ZPA.

Para que os usuários acessem seus aplicativos via ZPA, eles devem primeiro se autenticar no Zscaler Client Connector usando qualquer provedor de identidade (IdP) compatível com SAML 2.0 usando o modelo iniciado pelo provedor de serviços (iniciado pelo SP). O SSO do usuário do ZPA é iniciado pelo SP, mas o SSO do administrador do ZPA pode ser iniciado pelo SP ou pelo IdP.

1. Configure seu IdP e especifique o ZPA como SP. Antes de adicionar uma configuração de IdP usando o portal de administração do ZPA, você precisa ter o IdP em vigor para sua organização.
2. Adicione uma configuração de IDP por meio do portal de administração do ZPA.

Etapa 2: implantar App Connectors



Os App Connectors fornecem uma interface autenticada segura entre os aplicativos SAP e a nuvem do ZPA. Os App Connectors geralmente são implantados em pares para oferecer alta disponibilidade, e são normalmente implantados adjacentes ao servidor de aplicativos SAP. Os App Connectors podem ser implantados de várias formas. A Zscaler distribui uma imagem de máquina virtual (VM) padrão para implantação em data centers corporativos, ambientes de nuvem local privada, como VMware, ou ambientes de nuvem pública, como Amazon Web Services (AWS) EC2. Além disso, a Zscaler fornece pacotes que podem ser instalados em distribuições Linux compatíveis.

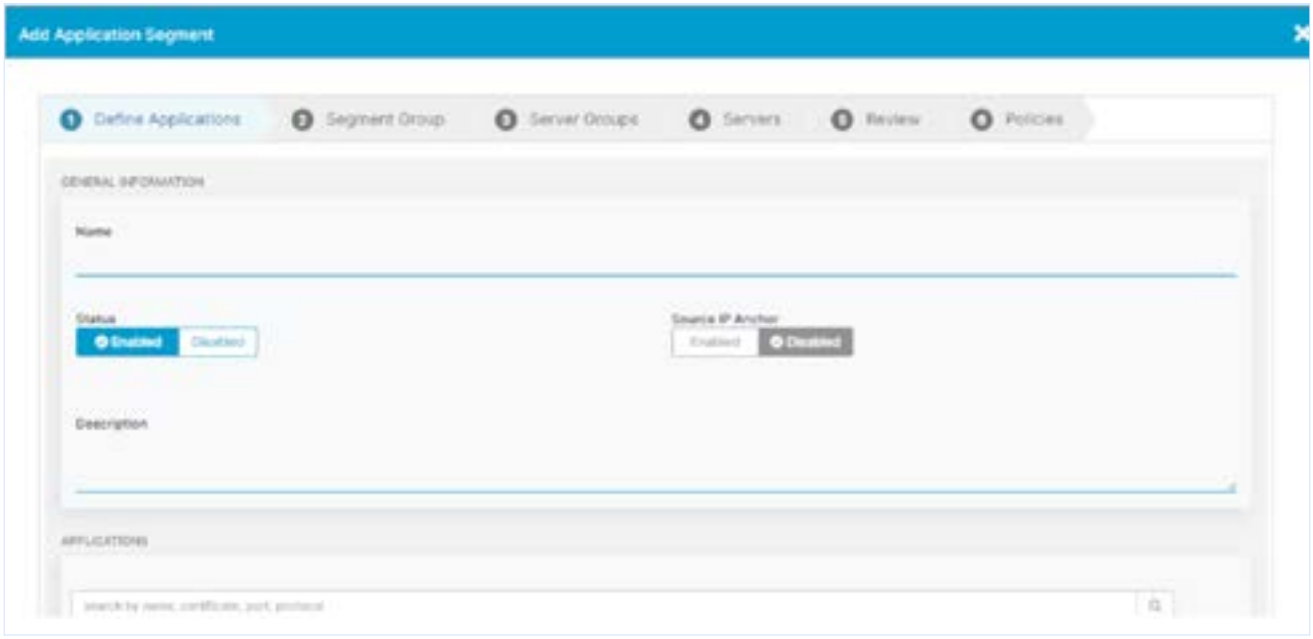
A configuração padrão do App Connector consiste em duas etapas principais:

1. Adicione um App Connector por meio do portal de administração do ZPA.
2. Implante os App Connectors na plataforma compatível de sua escolha.

No entanto, configurar os App Connectors para SAP HEC/PCE requer etapas especiais:

1. O cliente SAP solicita o Zscaler Endpoint Service ao seu representante de conta SAP ou gerente de entrega ao cliente.
2. A SAP instala App Connectors de alta disponibilidade no SAP HEC/PCE em nome do cliente.
3. O cliente fornece à SAP a licença do ZPA para aplicar aos App Connectors.

Etapa 3: configurar segmentos de aplicativos para acesso por navegador



Um segmento de aplicativos é uma coleção de instâncias de aplicativos. Os aplicativos são descobertos automaticamente e podem ser agrupados automaticamente com base em critérios de correspondência. Um segmento de aplicativos pode estar ancorado a um ou mais hosts ou segmentos de host. Segmentos de aplicativos são usados para acomodar políticas que incluem ou abrangem vários outros segmentos.

A Zscaler recomenda as seguintes práticas para configurar segmentos de aplicativos SAP:

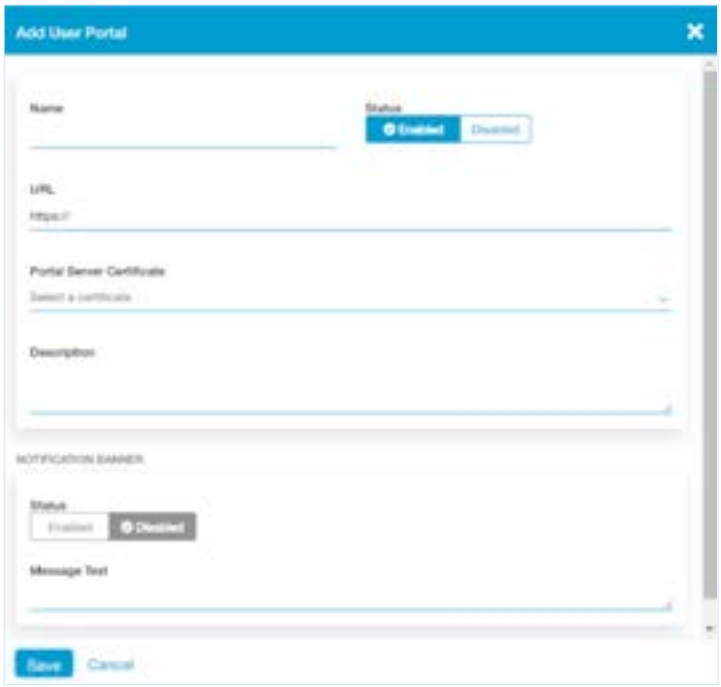
- Crie um único segmento de aplicativos para todos os aplicativos SAP. Isso permitirá que o serviço ZPA faça o balanceamento de carga das solicitações dos usuários para esses aplicativos. Entretanto, se a segmentação for necessária, crie vários segmentos de aplicativos para os aplicativos SAP.
- Crie segmentos de aplicativos para aplicativos SAP usando FQDNs. Se o cliente SAP não conseguir resolver o FQDN do host, ele tentará se conectar ao endereço IP. Embora o serviço seja compatível com endereços IP, é mais seguro que modelos zero trust se conectem com FQDNs.
- Se o nome do host SAP não for um FQDN, um domínio de pesquisa DNS será necessário. Se o cliente não tiver um sufixo de pesquisa, ele não poderá preencher o FQDN para se conectar ao SAP. O cliente retornará ao endereço IP fornecido pelo servidor de mensagens SAP, o que pode não ser desejável ou roteável pelo serviço ZPA.
- Use o rastreamento do Wireshark ou as configurações do SAP para identificar os endereços IP de todos os servidores SAP e crie um segmento de aplicativos que inclua apenas esses endereços IP e as portas TCP apropriadas. Não anuncie todo o intervalo de sub-rede (por exemplo, 192.168.1.0/24).
- Se houver uma lista de controle de acesso (ACL) configurada no servidor de mensagens SAP ou no servidor de aplicativos, adicione os endereços IP do App Connector a ela. Como o serviço ZPA executa um NAT de origem para o cliente, todo o tráfego é visto do endereço IP do App Connector. Para o grupo App Connector associado aos segmentos de aplicativos, o ZPA balanceará a carga das solicitações do usuário entre os App Connectors neste grupo App Connector.

Por isso, é recomendável que os endereços IP de todos os App Connectors no grupo App Connector sejam adicionados à ACL.

Para oferecer suporte a aplicativos SAP no ZPA, você precisa configurar segmentos de aplicativos e domínios de pesquisa de DNS.

1. Adicione um segmento de aplicativos por meio do portal de administração do ZPA.
   - Na janela Adicionar aplicativo, em Definir aplicativos, insira um nome de domínio totalmente qualificado (FQDN) que corresponda aos aplicativos SAP. Embora seja possível inserir um endereço IP, a Zscaler recomenda que você use FQDNs sempre que possível, pois é mais seguro. Se o cliente não tiver um sufixo de pesquisa, ele não poderá preencher o FQDN para se conectar ao SAP. O cliente retornará ao endereço IP fornecido pelo SAP Message Server.
   - Selecione Acesso ao navegador para habilitar o segmento de aplicativo para acesso por navegador.
2. Navegue até a página Acesso por navegador no portal de administração do ZPA e expanda o segmento de aplicativo que acabou de ser configurado para acesso por navegador. Copie o Nome Canônico (CNAME).
3. Adicione as informações de CNAME que você acabou de copiar ao seu DNS público e verifique se o FQDN do portal do usuário resolve para o registro.
4. Adicione um domínio de pesquisa de DNS. Para o SAP, você pode configurar domínios de pesquisa de DNS para FQDNs no portal de administração do ZPA. Isso permite que o cliente SAP anexe o sufixo de pesquisa e crie o FQDN. No entanto, você também pode configurar o SAP para fornecer um FQDN em vez de um nome curto. Isso elimina a necessidade de configurar um domínio de pesquisa de DNS.

Etapa 4: configurar o portal de acesso por navegador



1. Configure um portal de acesso por navegador por meio do portal de administração do ZPA. Ao adicionar um novo portal, você será solicitado a adicionar o nome do portal, o URL, o certificado do servidor do portal, uma descrição e a opção de adicionar um banner de exibição para os usuários.

2. Na página Portais do usuário no portal de administração do ZPA, expanda a linha para visualizar os detalhes do portal na tabela e clique no ícone Copiar ao lado do nome canônico (CNAME). Você precisará deste registro CNAME para seu DNS público.

3. Adicione as informações de CNAME que você acabou de copiar ao seu DNS público e verifique se o FQDN do portal do usuário resolve para o registro.

4. Em seguida, adicione links do portal, que são os links dos aplicativos habilitados para acesso por navegador que serão exibidos no portal do usuário de acesso por navegador.

5. Navegue até a página Links do portal no portal de administração do ZPA. A partir daqui, você pode configurar o nome, o protocolo (HTTPs/HTTP), a descrição e o ícone/imagem para cada aplicativo que será exibido no portal.

Recursos

ZPA: acesso por navegador
ZPA: suporte a aplicativos SAP
RISE com SAP S/4HANA Cloud, edição privada e SAP ERP, PCE

+1 408.533.0288 Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134 zscaler.com/br