Estratégias de Segurança em Cibersegurança: Como Eliminar a Decisão do Usuário e Proteger sua Empresa

ÍNDICE

Filosofia de Segurança: Eliminar a Decisão do Usuário
Por que esse enfoque é crucial?
Proteção Contra Engenharia Social e Acessos Não Autorizados
1. Profundização em ACL (Listas de Controle de Acesso)
Sintaxe e Estratégia de Configuração
Localização na Configuração
2. Configuração do Cliente Personalizado (Custom Client)
Passos Críticos no Gerador (my.AnyDesk):
2.1. Gestão Avançada: Clientes Dinâmicos (Dynamic Configuration)
O que são e como funcionam?
Vantagens Críticas (Zero Redeploy)
Como Implementar Clientes Dinâmicos
3. O Addon “Namespace” (Espaço de Nomes)
Por que é a ferramenta definitiva contra a falsificação?
Custo e Implementação
Resumo da Arquitetura Proposta
Notas adicionais sobre a implementação

Filosofia de Segurança: Eliminar a Decisão do Usuário

O pilar fundamental dessa estratégia é **tirar a responsabilidade pela segurança dos ombros do colaborador**. Na cibersegurança moderna, sabemos que o “erro humano” é a via de ataque mais comum. A engenharia social (o engano) acontece porque explora a boa vontade, a urgência ou o medo do usuário.

Por que esse enfoque é crucial?

1. **O usuário não é um especialista:** Não podemos esperar que um colaborador do setor financeiro ou de recursos humanos diferencie tecnicamente entre uma janela de conexão legítima e uma ilegítima, especialmente sob pressão.
2. **A fadiga de decisão:** Diante de múltiplos alertas ou uma ligação urgente e agressiva de um suposto “suporte técnico”, o usuário tende a ceder para resolver a situação rapidamente.
3. **Bloqueio Técnico vs. Bloqueio Humano:** Se dependemos do usuário para dizer “Não”, existe uma margem de erro. Se configurarmos o software para que tecnicamente **não possa** dizer “Sim” (ainda que queira), eliminamos o risco.

Ao implementar as medidas desta guia, transformamos a segurança de **reativa** (esperar que o usuário detecte a fraude) para **preventiva** (o sistema rejeita a fraude automaticamente, sem intervenção humana).

Proteção Contra Engenharia Social e Acessos Não Autorizados

Esta guia detalha a configuração técnica avançada para ambientes corporativos utilizando a licença Standard (e o addon de Namespace), com o objetivo de prevenir que atacantes externos enganem os colaboradores para obter acesso remoto.

1. Profundização em ACL (Listas de Controle de Acesso)

A ACL é a barreira mais crítica. Funciona sob o princípio de “Negar tudo por padrão”. Se a lista estiver vazia, o AnyDesk permite conexões de qualquer um (com confirmação). Se houver **uma única entrada** na lista, o AnyDesk bloqueia automaticamente qualquer conexão que não corresponda àquela entrada.

Sintaxe e Estratégia de Configuração

Em vez de adicionar IDs numéricos individuais (o que é difícil de manter se houver rotatividade na equipe de TI), é recomendado o uso de **Wildcards (Comodines)** se você possuir um Namespace, ou

IDs específicos se não.

A. Filtragem por ID Numérica (Básico)

Se seus técnicos utilizam AnyDesk genérico ou se você não tem um Namespace próprio.

- **Formato:** 123456789 (Um ID por linha).
- **Vantagem:** Controle granular.
- **Desvantagem:** Você deve atualizar o cliente de todos os colaboradores se contratar um novo técnico.

B. Filtragem por Namespace e Wildcards (Avançado)

Se sua empresa adquiriu o addon de Namespace (ex. @minhaempresa).

- **Formato:** *@minhaempresa
- **Funcionamento:** O asterisco atua como comodim. Isso permite que **qualquer** técnico cujo usuário termine em @minhaempresa possa conectar, mas bloqueia instantaneamente:
  - Qualquer usuário @ad (a versão gratuita/pública).
  - Qualquer usuário de outra empresa.
  - Qualquer invasor utilizando contas roubadas de outros domínios.

Localização na Configuração

Para testes locais antes de implementar:

1. Ir a **Configurações** > **Segurança**.
2. Desbloquear o cadeado de segurança (requere admin).
3. Seção **Lista de Controle de Acesso**.
4. Ativar **Restringir acesso às seguintes IDs e aliases**.
5. Inserir os padrões (ex. *@minhaempresa ou os IDs).

2. Configuração do Cliente Personalizado (Custom Client)

Não deve permitir que os colaboradores instalem o AnyDesk público. Você deve gerar um executável MSI/EXE a partir de my.anydesk.com que contenha as regras de segurança “incorporadas”.

Passos Críticos no Gerador (my.AnyDesk):

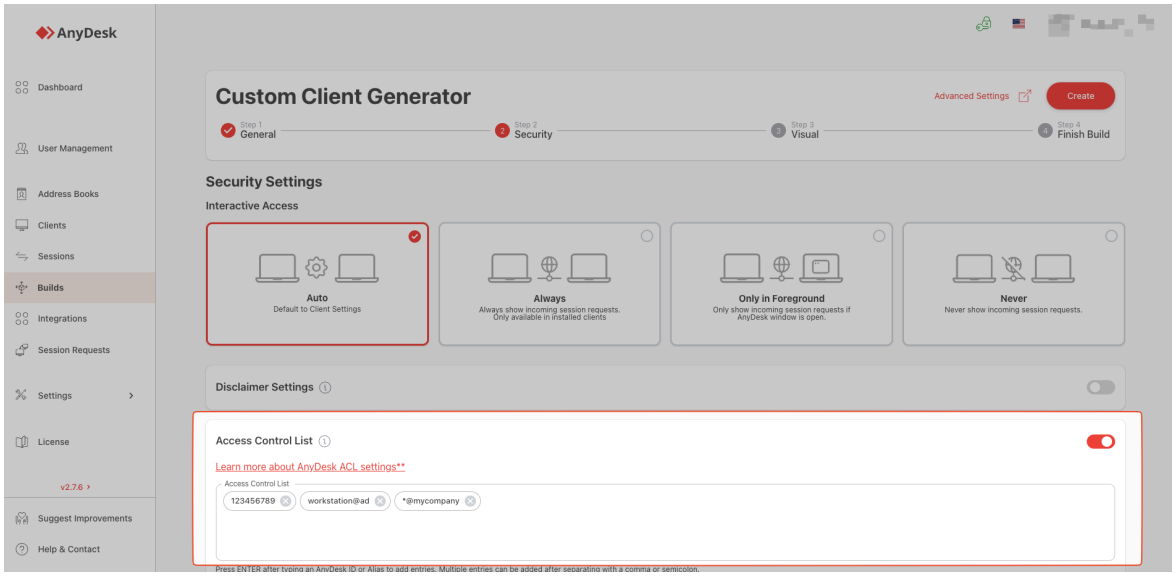
Ao criar um novo cliente na aba **Clientes**, configure o seguinte:

A. Seção “Options” (Opções)

- **Disable Settings (Desabilitar configuração): RADICAL**. Normalmente, essa configuração não é necessária se a empresa gerencia bem os privilégios dos seus usuários (administradores e usuários regulares separados), mas se você deseja que o acesso remoto esteja protegido mesmo diante do mau uso de uma conta de administrador, deve marcar essa caixa. Isso elimina a aba de configurações no menu do usuário.
    - *Por que:* Impede que um atacante, usando engenharia social (“Senhora, por favor vá a configurações e apague a lista para que eu possa ajudar”), consiga eludir a segurança.
- **Request Elevation at Startup:** Recomendado habilitar. Essa opção solicita elevação de privilégios (UAC) ao iniciar, evitando que o Windows bloqueie o técnico ao executar tarefas administrativas. **Importante**: Isso se aplica apenas a versões portáteis ou que não requerem instalação, já que a instalação do AnyDesk, por si só, necessita de privilégios de administrador.

B. Seção “Security” (Segurança)

- **Access Control List (ACL):** Aqui é onde “queimamos” a lista branca no instalador.
    - Introduza os IDs dos seus técnicos ou o comodim *@minhaempresa.
    - Ao ser instalado, este cliente na PC do colaborador, a lista já estará ativa e bloqueada.
- **Interactive Access:** Mantenha em “Always Show Incoming Session Requests” (Sempre mostrar solicitações). Nunca permita acesso sem supervisão a menos que seja um servidor.



Ativar ACL

C. Seção “Program Name & Icon” (Identidade Visual)

- Carregue o logotipo da sua empresa.

- Altere o nome de “AnyDesk” para “Suporte Remoto [SuaEmpresa]”.
- *Efeito Psicológico:* Treine os usuários: “Se o programa não tem o logotipo azul da nossa empresa, é um vírus/estelionato”.

2.1. Gestão Avançada: Clientes Dinâmicos (Dynamic Configuration)

Existe uma limitação operacional com os clientes personalizados tradicionais (Estáticos): a configuração fica “queimada” dentro do arquivo .exe ou .msi no momento do download. Se precisar alterar a lista de acesso (ACL) porque um técnico saiu ou mudou uma política de segurança, **deverá gerar um novo instalador e redeployá-lo em toda a empresa**, o que é custoso e lento.

Para resolver isso, o AnyDesk (versão 8.0.3 ou superior) oferece a **Configuração de Cliente Dinâmica**.

O que são e como funcionam?

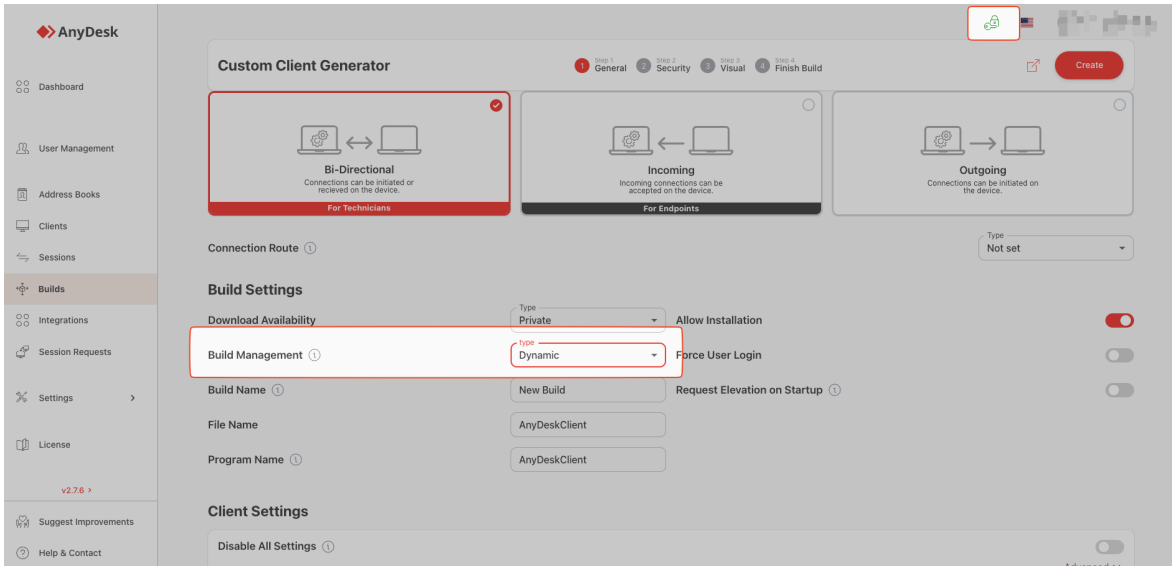
Diferente do cliente estático, o cliente dinâmico não tem a configuração incorporada de forma permanente. Em vez disso, o cliente instalado consulta periodicamente os servidores do AnyDesk (my.anydesk.com) para baixar sua configuração mais recente.

Vantagens Críticas (Zero Redeploy)

1. **Atualização de ACL em Tempo Real:**
    - **Cenário:** Você despede um técnico com acesso crítico ou detecta que um ID foi comprometido.
    - **Solução:** Você acessa o console web, remove aquele ID da ACL do perfil e salva.
    - **Resultado:** Todos os computadores da empresa atualizam sua lista automaticamente e bloqueiam o técnico. Não é necessário mexer nos PCs dos usuários nem enviar atualizações por GPO.
2. **Flexibilidade em Políticas:**
    - Você pode endurecer a segurança de forma ágil (ex. desativar a área de transferência globalmente diante de uma ameaça de vazamento de dados) sem reinstalar o software.
3. **Facilidade de Gestão:**
    - Você mantém uma “fonte única de verdade” na nuvem. Sabe que todos os clientes têm a mesma configuração de segurança, independentemente de quando foram instalados.

Como Implementar Clientes Dinâmicos

1. No my.anydesk.com, vá para a aba **Files** ou **Clients** (dependendo da sua versão).
2. Certifique-se de ativar a opção “**Private key**”; caso contrário, não poderá selecionar o tipo de cliente.
3. Crie uma nova configuração de cliente.
4. Certifique-se de que a opção de **Dynamic Configuration** (ou atribuir a um perfil centralizado) esteja ativa.
5. Ao instalar este cliente nos equipamentos, ele se vinculará a esse perfil na nuvem. Quaisquer alterações futuras que você fizer no perfil web serão replicadas nos agentes instalados.
6. **Importante**: Um cliente estático não pode se tornar dinâmico. Se você já implementou um estático, terá que reinstalar o AnyDesk utilizando o cliente dinâmico que gerou anteriormente.



Gerar cliente dinâmico

3. O Addon “Namespace” (Espaço de Nomes)

No AnyDesk, todos os usuários públicos têm o alias nome@ad. O Namespace permite que você tenha seu próprio sufixo, ex. nome@minhaempresa.

Por que é a ferramenta definitiva contra a falsificação?

1. Verificação de Identidade (Anti-Spoofing)

Ninguém no mundo pode criar um alias que termine em @suaempresa, exceto você (o administrador da licença). O AnyDesk verifica a propriedade do domínio/nome.

- **Cenário de ataque:** Um hacker liga dizendo ser do “Suporte TI”. Seu ID será hacker@ad ou um número 332-112-445.
- **Defesa:** Se sua ACL estiver configurada como *@suaempresa, a conexão do hacker será automaticamente rejeitada. Nem mesmo a alerta soará na PC do colaborador.

2. Gestão Escalável

Sem Namespace, sempre que um novo técnico entra, você precisa atualizar a ACL de 500 colaboradores para adicionar o ID do novo técnico.
Com Namespace:

1. Você cria o alias do novo técnico no seu console (novo.tecnico@minhaempresa).
2. Como a ACL dos colaboradores diz *@suaempresa, o novo técnico tem acesso imediato sem mexer nas configurações dos usuários.

3. Auditoria Forense

Nos logs de conexão (my.anydesk.com > Sessions), você verá claramente juan@minhaempresa conectou a recepcion@minhaempresa. Isso é muito mais fácil de auditar do que ver o ID 445212 conectou ao ID 998212.

Custo e Implementação

O Namespace é um “Add-on” (custo adicional) sobre a licença Standard ou Advanced, embora algumas vezes venha incluído em licenças Enterprise. É comprado uma única vez por nome.

Resumo da Arquitetura Proposta

Para uma segurança estilo “Fortaleza”:

1. **Adquirir Namespace:** Comprar @minhaempresa.
2. **Atribuir Alias:** Dar a cada técnico seu alias corporativo (tecnico1@minhaempresa).
3. **Criar Cliente Personalizado Dinâmico:**
    - Logo corporativo.
    - Configuração desabilitada para o usuário.
    - Vinculado a perfil dinâmico na nuvem.
    - **ACL Centralizada:** *@minhaempresa.
4. **Implementação:** Instalar este MSI via GPO (Políticas de Grupo) ou MDM (Intune/ManageEngine) em todos os equipamentos.

5. **Resultado:** Somente os técnicos com alias @minhaempresa podem iniciar uma conexão. O restante da internet está bloqueado e você pode revogar acessos em segundos a partir do console web.

Notas adicionais sobre a implementação

1. Implementação via GPO (Políticas de Grupo):
   Uma vez que você baixe o arquivo .msi do seu cliente personalizado, não precisa ir PC por PC. Você pode usar um comando de instalação silenciosa no seu Diretório Ativo ou ferramenta de gestão:
   AnyDesk_Custom_Client.msi /qn

   Por ser um cliente personalizado com a configuração "incorporada", não precisa de scripts adicionais para configurar a senha ou a ACL; o MSI já contém isso.

2. Se não comprar o Namespace:
   Você ainda pode usar a estratégia, mas a ACL do cliente personalizado precisará ser uma lista estática de IDs:
   111222333, 444555666, 777888999
   O risco é operacional: se o técnico 111222333 deixar a empresa e levar seu laptop, você precisará atualizar urgentemente os clientes dos colaboradores para revogar seu acesso (a não ser que use Clientes Dinâmicos para atualizar a lista remotamente).

3. Segurança Física do Técnico:
   Lembre-se de que com essa configuração, a "chave mestra" são os laptops dos seus técnicos. Assegure-se de que seus técnicos tenham:

   - Autenticação de Duplo Fator (2FA) ativada no acesso ao AnyDesk.
   - Senha forte em sua própria sessão do Windows.

Experimente gratuitamente o AnyDesk e aproveite todos os seus benefícios! Para mais informações sobre a compra do AnyDesk no Brasil, entre em contato conosco.