**Introdução**

Concluído100 XP

* 2 minutos

Saiba como habilitar o acesso remoto em sua organização e publicar os aplicativos e sites da organização usando o WAP (proxy de aplicativo Web) do Windows Server.

**Cenário**

A Contoso Ltda. é uma empresa de serviços financeiros sediada em Seattle e com grandes escritórios pelo mundo. A maior parte de seu ambiente de computação é executado localmente no Windows Server. Isso inclui as cargas de trabalho virtualizadas nos hosts do Windows Server 2016.

A equipe de TI da Contoso está migrando os servidores Contoso locais para o Windows Server 2022. Como administrador de infraestrutura do Windows Server, você é responsável por gerenciar e manter a infraestrutura de rede do Windows Server que ajudará a Contoso a atingir suas metas de negócios.

Depois de concluir este módulo, você saberá como selecionar, usar e gerenciar os componentes de acesso remoto. Você também saberá como implementar o WAP como proxy reverso para os aplicativos Web internos.

**Objetivos de aprendizagem**

Depois de concluir este módulo, você poderá:

* Descrever as opções de acesso remoto disponíveis no Windows Server.
* Selecionar as opções de VPN e configurar os servidores VPN.
* Descrever a função de servidor NPS.
* Planejar e implementar o NPS.
* Determinar quando a PKI deve ser implantada para obter acesso remoto.
* Identificar as opções de autenticação para o proxy de aplicativo Web e explicar como usá-lo para publicar aplicativos.

**Pré-requisitos**

Para ter uma experiência melhor de aprendizagem do módulo, você precisará ter conhecimento e experiência em:

* Windows Server.
* Conceitos e tecnologias do AD DS (Active Directory Domain Services).
* Principais tecnologias de rede.
* Melhores práticas de segurança básica.

# Examinar as opções de acesso remoto no Windows Server

Concluído100 XP

* 7 minutos

A função de servidor Acesso Remoto no Windows Server fornece várias opções de acesso remoto. Cada opção representa uma tecnologia exclusiva que as organizações, como a Contoso, podem usar para acessar recursos internos nos escritórios de locais de site remoto ou na Internet. A tecnologia que a TI da Contoso decide usar depende das metas comerciais específicas.

## Recursos de acesso remoto com suporte

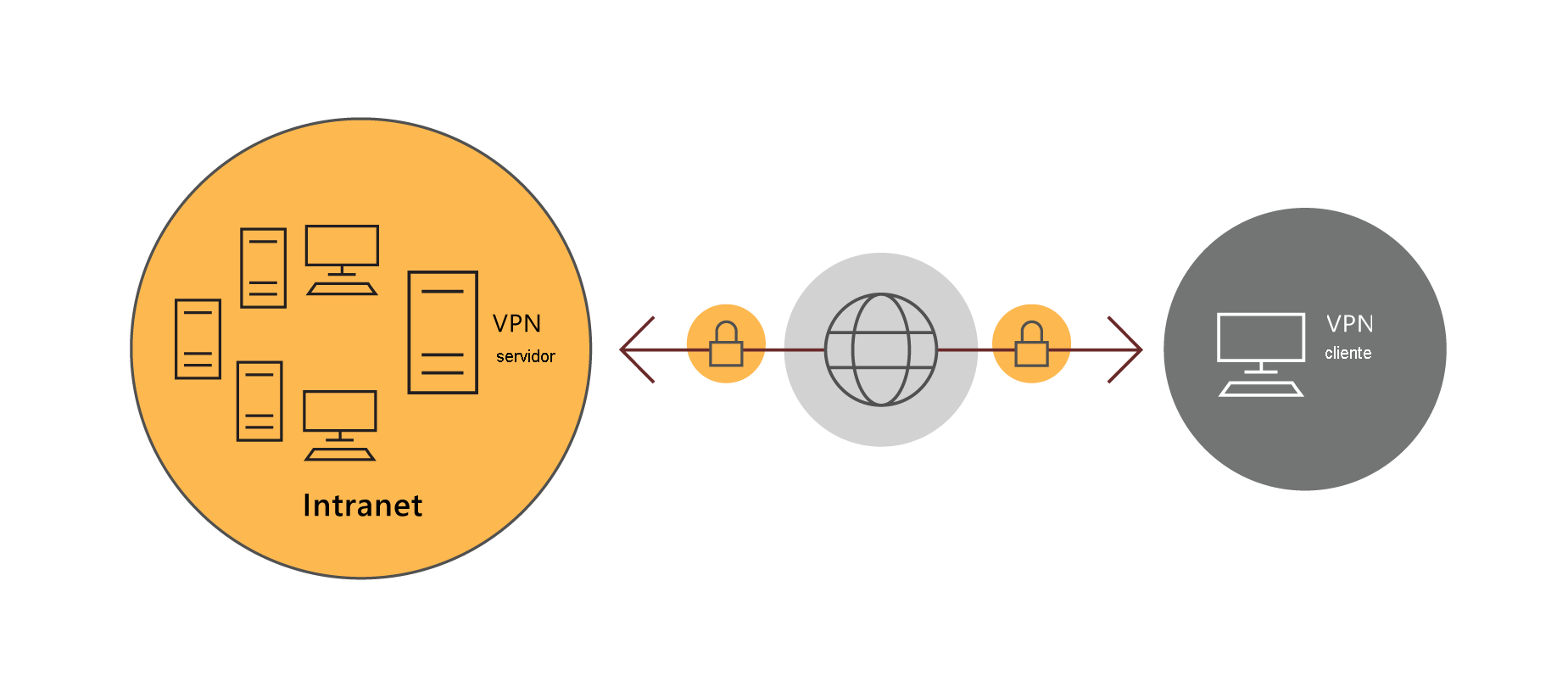
O Windows Server dá suporte a vários recursos de acesso remoto.

### VPN

As conexões VPN permitem que os usuários que trabalham externamente (por exemplo, em casa, em um site do cliente ou em um ponto de acesso sem fio público) acessem aplicativos e dados na rede privada de uma organização, usando a infraestrutura fornecida por uma rede pública, como a Internet.

Da perspectiva do usuário, a VPN é uma conexão ponto a ponto entre um computador, o cliente VPN e o servidor de uma organização. A infraestrutura exata da rede compartilhada ou pública não é relevante porque é exibida para o usuário como se os dados fossem enviados por um link privado dedicado.

O Windows Server dá suporte a várias configurações diferentes com VPNs, incluindo acesso remoto e site a site, exibidas no gráfico a seguir.



### Roteamento

O Windows Server pode funcionar como roteador ou dispositivo NAT (conversão de endereços de rede) entre duas redes internas ou entre a Internet e a rede interna. O roteamento funciona com tabelas de roteamento e dá suporte a protocolos de roteamento, incluindo:

* RIP (Routing Information Protocol) versão 2.
* Protocolo IGMP.
* Agente de retransmissão DHCP.

**Dica**

Embora você possa usar o Windows Server para essas tarefas de roteamento, não é comum fazer isso, pois a maioria das organizações tem dispositivos de hardware especializados para executar essas tarefas.

### Proxy de aplicativo Web

O proxy de aplicativo Web fornece a funcionalidade de proxy reverso para usuários que devem acessar os aplicativos Web internos da organização pela Internet. O proxy de aplicativo Web autentica os usuários usando as seguintes opções:

* Tecnologia AD FS, em que o proxy de aplicativo Web atua como proxy AD FS.
* A autenticação de passagem, em que o aplicativo publicado executa a autenticação, não o proxy de aplicativo Web.

### DirectAccess

O DirectAccess permite que os usuários remotos acessem com segurança recursos corporativos, como servidores de email, pastas compartilhadas e sites internos, sem se conectar a uma VPN (rede virtual privada). O DirectAccess aumenta a produtividade de uma força de trabalho móvel, oferecendo a mesma experiência de conectividade dentro e fora do escritório.

**Importante**

As edições do Windows 10 Enterprise e Education dão suporte ao DirectAccess.

## Visão geral do acesso a aplicativos remotos

O acesso a aplicativos remotos é uma parte importante do suporte a usuários móveis e usuários de escritórios remotos. A maneira como você fornece acesso remoto a aplicativos varia de acordo com a arquitetura do aplicativo. No entanto, para todos os aplicativos, você precisa garantir que o acesso remoto ao aplicativo seja seguro.

### Acesso remoto a arquivos de dados

Quando você usa uma VPN ou o DirectAccess para acessar arquivos de dados, como documentos do Microsoft Word ou planilhas do Microsoft Excel, pode levar mais tempo para abrir e fechar arquivos do que quando você está no escritório, mas o desempenho normalmente é aceitável. O desempenho mais lento ocorre principalmente porque as velocidades de rede são mais lentas em locais remotos e pela Internet.

### Acesso remoto a aplicativos da área de trabalho

Para aplicativos que usam armazenamento de dados compartilhado, como um banco de dado, o uso de uma VPN ou do DirectAccess geralmente causa desempenho lento. A maioria dos desenvolvedores não otimiza os aplicativos para que sejam executados em conexões mais lentas com alta latência. Portanto, os aplicativos têm muitas chamadas de comunicação com o armazenamento de dados de back-end. A latência adicional em cada chamada aumenta até resultar em um desempenho muito lento.

Para dar suporte a aplicativos com armazenamento de dados compartilhados, é comum implementar o RDS (Serviços de Área de Trabalho Remota). Quando você implementa o RDS, o aplicativo é instalado em um Host da Sessão da Área de Trabalho Remota localizado na rede interna compartilhada por vários usuários. O aplicativo permanece próximo aos dados, portanto, a latência de rede não causa problemas de desempenho.

**Dica**

Os usuários são conectados ao Host da Sessão da Área de Trabalho Remota que usa o protocolo RDP.

### Acesso remoto a aplicativos baseados na Web

Os aplicativos baseados na Web têm um bom desempenho em redes mais lentas e de latência mais alta. Isso ocorre porque a lógica do aplicativo é armazenada em um servidor Web próximo aos dados do aplicativo. Apenas um volume limitado de dados a serem exibidos na tela é enviado ao navegador da Web. Isso significa que os aplicativos baseados na Web são ideais para serem utilizados por usuários móveis e escritórios remotos.

O protocolo HTTPS que criptografa a comunicação normalmente é usado para aplicativos baseados na Web. Isso garante que os dados não possam ser interceptados em trânsito, mas a maioria das empresas também precisa que o aplicativo baseado na Web seja isolado da Internet por um proxy reverso. Os usuários remotos se comunicam com um proxy reverso em uma rede de perímetro e o proxy reverso se comunica com o aplicativo baseado na Web na rede interna.

**Importante**

O proxy de aplicativo Web funciona como proxy reverso para aplicativos baseados na Web.

## Gerenciar o acesso remoto no Windows Server

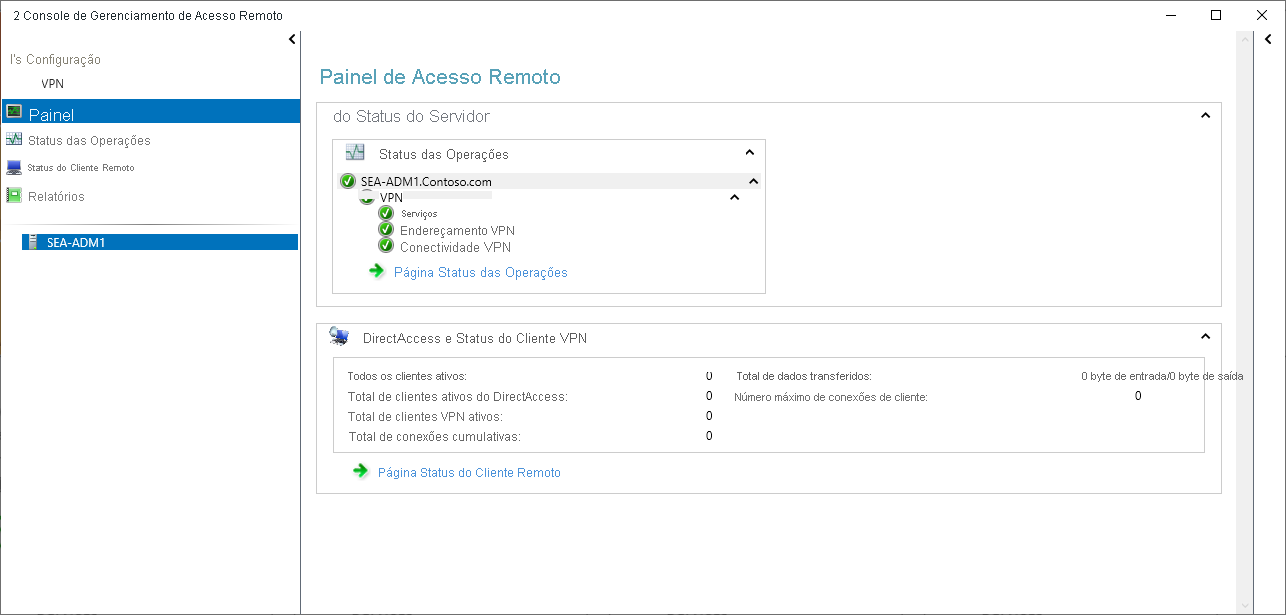
Depois de instalar a função Acesso Remoto em um servidor que executa o Windows Server, você pode gerenciar a função usando o console de gerenciamento de acesso remoto e o console de roteamento e acesso remoto ou o Windows PowerShell.

### Console de Gerenciamento de Acesso Remoto

O console de Gerenciamento de Acesso Remoto permite que você gerencie o DirectAccess, a VPN (rede virtual privada) e o proxy de aplicativo Web. Ao abrir esse console pela primeira vez, você usa uma interface baseada em assistente para definir as configurações de acesso remoto de acordo com os requisitos corporativos.

Depois de definir as configurações iniciais de acesso remoto, você pode gerenciar a solução de acesso remoto com as opções descritas na tabela a seguir.

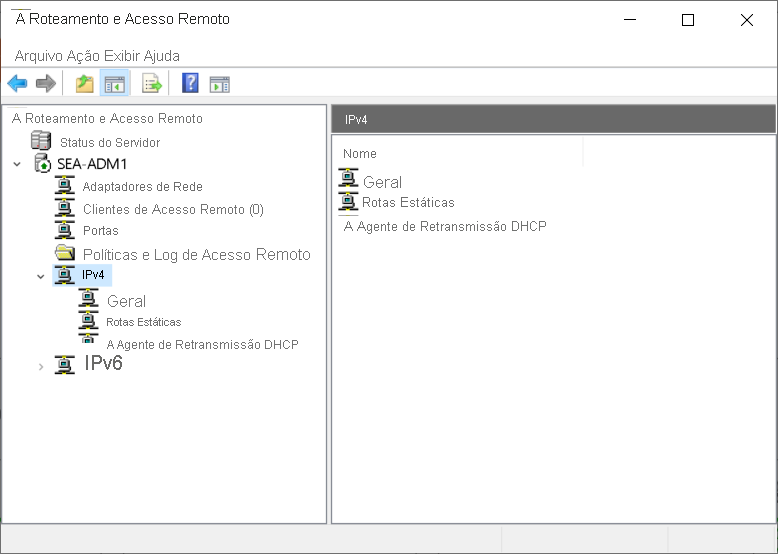
| **Opção** | **Descrição** |
| --- | --- |
| Configuração | Você pode editar as configurações de acesso remoto usando assistentes e a representação gráfica da configuração de rede atual no console. |
| Painel | Você pode monitorar o status geral de servidores e clientes que fazem parte da solução de acesso remoto. |
| Status das operações | Você pode acessar informações detalhadas sobre o status dos servidores que fazem parte da solução de acesso remoto. |
| Status do cliente remoto | Você pode acessar informações detalhadas sobre o status dos clientes conectados à solução de acesso remoto. |
| Relatórios | Você pode gerar relatórios históricos em diferentes parâmetros, como uso de acesso remoto, detalhes de acesso, detalhes de conexão e estatísticas de carga do servidor. |



### Console de acesso remoto e roteamento

Você pode usar o console de acesso remoto e roteamento para configurar um servidor que execute o Windows Server como dispositivo NAT, roteador dos protocolos IPv4 e IPv6, proxy DHCP e servidor VPN. Depois de concluir a configuração, você pode gerenciar a solução de acesso remoto usando as opções descritas na tabela a seguir.

| **Opção** | **Descrição** |
| --- | --- |
| Status do Servidor | Você pode monitorar o status do servidor de acesso remoto, as portas em uso e o tempo de operação do servidor. |
| Cliente de acesso remoto, portas, registro em log e políticas de acesso remoto | Você pode monitorar o status do cliente, o status da porta e as informações detalhadas de log sobre os clientes conectados ao servidor de Acesso Remoto. |
| IPv4 | Você pode definir as configurações IPv4, como NAT, roteamento IPv4 com rotas estáticas e estes protocolos de roteamento: RIP versão 2, IGMP e Agente de Retransmissão DHCP. |
| IPv6 | Você pode definir as configurações IPv6, como roteamento IPv6 com rotas estáticas e protocolo de roteamento do Agente de Retransmissão DHCP. |



**Selecionar e configurar as VPNs**

Concluído100 XP

* 8 minutos

Ao planejar as VPNs, a Contoso deve considerar vários fatores, incluindo o devido protocolo de túnel e método de autenticação. Ela também deve considerar a melhor maneira de configurar os servidores VPN para dar suporte às necessidades de acesso remoto dos usuários.

**Selecionar um protocolo de túnel**

A Contoso pode optar por implementar as VPNs usando um dos vários protocolos de túnel e métodos de autenticação. As conexões VPN podem usar um dos seguintes protocolos de túnel:

* Protocolo PPTP
* L2TP/IPsec
* SSTP (Secure Sockets Tunneling Protocol)
* IKEv2 (Internet Key Exchange versão 2)

Todos os protocolos de túnel VPN compartilham três recursos:

* Túnel. A tecnologia VPN encapsula os dados privados com um cabeçalho que contém informações de roteamento, o que permite que os dados percorram a rede de trânsito.
* Autenticação. Há três tipos de autenticação para conexões VPN, incluindo:
  + Autenticação de nível de usuário com a autenticação de protocolo PPP.
  + Autenticação de nível de computador com o protocolo IKE.
  + Autenticação de origem de dados e integridade dos dados.
* Criptografia de dados. Para garantir a confidencialidade dos dados à medida que atravessam a rede de trânsito compartilhada ou pública, o remetente criptografa os dados e o receptor os descriptografa.

A tabela a seguir descreve os protocolos de túnel compatíveis.

| **Protocolo** | **Descrição** |
| --- | --- |
| PPTP | Você pode usar o PPTP para acesso remoto e conexões VPN (rede virtual privada) site a site. Quando você usa a Internet como a rede pública de VPN, o servidor PPTP é um servidor VPN habilitado para PPTP com uma interface na Internet e outra na intranet. |
| L2TP/IPsec | O L2TP permite criptografar o tráfego de vários protocolos enviado por qualquer meio compatível com a entrega de datagrama ponto a ponto, como ATM (modo de transferência assíncrona) ou IP. O L2TP é uma combinação de PPTP e L2F. O L2TP representa os melhores recursos de PPTP e L2F. |
| SSTP | SSTP é um protocolo de túnel que usa o protocolo HTTPS sobre a porta TCP 443 para passar o tráfego por meio de firewalls e proxies da Web, o que poderia bloquear o tráfego PPTP e L2TP/IPsec. O SSTP proporciona um mecanismo para encapsular o tráfego PPP pelo canal SSL do protocolo HTTPS. O uso de PPP possibilita o suporte a métodos de autenticação fortes, como EAP-TLS. O protocolo SSL proporciona segurança no nível do transporte com melhor negociação de chave, criptografia e verificação de integridade. |
| IKEv2 | O IKEv2 usa o protocolo de modo de túnel IPsec sobre a porta UDP 500. O IKEv2 dá suporte à mobilidade, o que o torna uma boa opção de protocolo para uma força de trabalho móvel. As VPNs baseadas em IKEv2 permitem que os usuários migrem facilmente entre hotspots sem fio ou entre conexões sem fio e com fio. |

**Cuidado**

Você não deve usar o PPTP devido às vulnerabilidades de segurança. Em vez disso, use o IKEv2 sempre que possível, pois é mais seguro e oferece vantagens em relação ao L2TP.

**Selecionar uma opção de autenticação**

A autenticação de clientes de acesso é uma preocupação de segurança importante. Os métodos de autenticação normalmente usam um protocolo de autenticação negociado durante o processo de estabelecimento da conexão. A função de servidor Acesso Remoto dá suporte aos métodos descritos na tabela a seguir.

| **Método** | **Descrição** |
| --- | --- |
| PAP | O Protocolo PAP usa senhas de texto não criptografado e é o protocolo de autenticação menos seguro. Normalmente, ele é negociado se o cliente de acesso remoto e o servidor de Acesso Remoto não puderem negociar uma forma mais segura de validação. O Windows Server inclui o PAP para dar suporte a sistemas operacionais cliente mais antigos que não são compatíveis com outros métodos de autenticação. |
| CHAP | O protocolo CHAP é um protocolo de autenticação de desafio/resposta que usa o esquema de hash MD5 padrão do setor para criptografar a resposta. Vários fornecedores de servidores de acesso à rede e clientes usam o CHAP. No entanto, como o CHAP requer que você use uma senha com criptografia reversível, você deve usar outro protocolo de autenticação, como o MS-CHAPv2. |
| MS-CHAPv2 | O protocolo MS-CHAPv2 é um protocolo de autenticação mútua com senha criptografada unidirecional e fornece melhorias em relação ao CHAP. |
| EAP | Se você usar o protocolo EAP, um mecanismo de autenticação arbitrária autenticará uma conexão de acesso remoto. O cliente de acesso remoto e o autenticador, que é o servidor de Acesso Remoto ou o servidor RADIUS, negociam o esquema de autenticação exato que será usado. O roteamento e o acesso remoto incluem suporte para EAP-TLS por padrão. Você pode conectar outros módulos EAP ao servidor que está executando o roteamento e o acesso remoto para fornecer outros métodos EAP. |

**Considerações adicionais**

Além do protocolo de túnel e do método de autenticação, antes de implantar a solução VPN da organização, você deve considerar o seguinte:

* Verifique se o servidor VPN tem duas interfaces de rede. Você deve determinar qual interface de rede será conectada à Internet e qual será conectada à rede privada. Durante a configuração, você deve escolher qual interface de rede será conectada à Internet. Se você especificar a interface de rede incorreta, o servidor VPN de acesso remoto não funcionará corretamente.
* Determine se os clientes remotos recebem endereços IP de um servidor DHCP na rede privada ou do servidor VPN de acesso remoto que você está configurando. Se você tiver um servidor DHCP na rede privada, o servidor VPN de acesso remoto pode conceder 10 endereços de cada vez no servidor DHCP e, em seguida, atribuir esses endereços a clientes remotos. Se você não tiver um servidor DHCP na rede privada, o servidor VPN de acesso remoto pode gerar e atribuir endereços IP automaticamente a clientes remotos. Se você quiser que o servidor VPN de acesso remoto atribua endereços IP de um intervalo especificado, deve determinar qual deve ser esse intervalo.
* Determine se você deseja um servidor RADIUS ou um servidor VPN de acesso remoto configurado para autenticar as solicitações de conexão de clientes VPN. A adição de um servidor RADIUS será útil se você planeja instalar vários servidores VPN de acesso remoto, pontos de acesso sem fio ou outros clientes RADIUS para a rede privada.

# Usar o NPS para criar e aplicar políticas de acesso à rede

Concluído100 XP

* 10 minutos

Para gerenciar usuários de acesso remoto com mais facilidade, organizações como a Contoso implantam e configuram a função de servidor NPS. O NPS permite que a Contoso crie e aplique políticas de acesso à rede em toda a organização para autenticação e autorização das solicitações de conexão. Elas podem usar o NPS para implementar a autenticação, autorização e contabilidade de acesso à rede com qualquer combinação das seguintes funções:

* Servidor RADIUS
* Proxy RADIUS
* Contabilização RADIUS

## ****Servidor RADIUS****

O RADIUS é um protocolo de autenticação padrão do setor que os fornecedores usam para dar suporte à troca de informações de autenticação entre os elementos de uma solução de acesso remoto. O NPS é a implementação da Microsoft de um servidor RADIUS. O NPS permite o uso de um conjunto heterogêneo de rede sem fio, comutador, acesso remoto ou equipamento VPN. Você pode usar o NPS com o serviço Roteamento e Acesso Remoto, que está disponível no sistema operacional Windows Server. Além disso, você pode usar o NPS com a função Acesso Remoto no Windows Server.

O NPS executa processos centralizados de autenticação, autorização e contabilização para conexões sem fio, servidores de Gateway de Área de Trabalho Remota, comutadores de autenticação, VPNs e conexões discadas. Ao usar o NPS como servidor RADIUS, você configura NASs (servidores de acesso à rede) como pontos de acesso sem fio e servidores VPN, que também são conhecidos como clientes RADIUS no NPS.

Você também configura as políticas de rede que o NPS usa para autorizar solicitações de conexão. Você pode configurar a contabilização RADIUS para que o NPS registre as informações de contabilização em arquivos de log no disco rígido local ou em um banco de dados do Microsoft SQL Server.

**Importante**

Não é possível instalar o NPS nas edições de Server Core do Windows Server.

Quando um servidor NPS é membro de um domínio AD DS (Active Directory Domain Services), o NPS usa o AD DS como banco de dados da conta de usuário e fornece a capacidade de SSO (logon único). Isso significa que o mesmo conjunto de credenciais de usuário habilita o controle de acesso à rede, como autenticação e autorização de acesso a uma rede e acesso a recursos no domínio AD DS.

As organizações que mantêm o acesso à rede, como os ISPs, têm o desafio de gerenciar uma variedade de métodos de acesso à rede em um único ponto de administração, independentemente do tipo de equipamento de acesso à rede usado. O padrão RADIUS atende a esse requisito. O RADIUS é um protocolo cliente-servidor que habilita o equipamento de acesso à rede, quando usado como clientes RADIUS, para enviar solicitações de autenticação e contabilização para um servidor RADIUS.

Um servidor RADIUS tem acesso às informações da conta do usuário e pode verificar as credenciais de autenticação de acesso à rede. Se as credenciais do usuário forem autênticas e o RADIUS autorizar a tentativa de conexão, o servidor RADIUS autoriza o acesso do usuário com base nas condições configuradas e registra a conexão de acesso à rede em um log de contabilização. O uso do RADIUS permite coletar e manter os dados de autenticação, autorização e contabilização do usuário de acesso à rede em um local central, e não em cada servidor de acesso.

## ****Proxy RADIUS****

Ao usar o NPS como proxy RADIUS, você configura políticas de solicitação de conexão que indicam quais solicitações de conexão o NPS irá encaminhar a outros servidores RADIUS e a quais servidores RADIUS você deseja encaminhar as solicitações de conexão. Também é possível configurar o NPS encaminhar os dados de contabilização para registro em log em um ou mais computadores de um grupo de servidores RADIUS remotos. Com o NPS, a organização também pode terceirizar a infraestrutura de acesso remoto para um provedor de serviços e, ao mesmo tempo, manter o controle sobre a autenticação, autorização e contabilização do usuário. Você pode criar configurações de NPS para as seguintes soluções:

* Servidores VPN.
* Pontos de acesso sem fio.
* Servidores de Gateway de Área de Trabalho Remota.
* VPN terceirizada, conexão discada ou acesso sem fio.
* Acesso à Internet.
* Acesso autenticado a recursos de extranet para parceiros de negócios.

### **Contabilização RADIUS**

Você pode configurar o NPS para realizar a contabilização RADIUS para solicitações de autenticação de usuário, mensagens de aceitação de acesso, mensagens de rejeição de acesso, solicitações e respostas de contabilização e atualizações de status periódicas. O NPS permite que você faça logon em um banco de dados do Microsoft SQL Server além de, ou em vez de, fazer logon em um arquivo local.

# Planejar e implementar o NPS

Concluído100 XP

* 7 minutos

O NPS executa processos centralizados de autenticação, autorização e contabilização para conexões sem fio, servidores de Gateway de Área de Trabalho Remota, comutadores de autenticação, VPNs e conexões discadas. Mas a Contoso deve primeiro configurar as políticas de rede que o NPS usa para autorizar solicitações de conexão. Ela também pode optar por configurar a contabilização RADIUS para que o NPS registre as informações de contabilização em arquivos de log no disco rígido local ou em um banco de dados do Microsoft SQL Server.

## Escolher um método de autenticação NPS

O NPS autentica e autoriza uma solicitação de conexão antes de permitir ou negar acesso, quando os usuários tentam se conectar à rede por meio de NASs. Ao implantar o NPS, você pode especificar o tipo necessário de método de autenticação para acesso à rede.

Os seguintes métodos de autenticação são compatíveis com o NPS:

* PAP
* Protocolo SPAP
* CHAP
* MS-CHAP
* MS-CHAP v2
* EAP

**Dica**

Quando você escolhe o EAP como o método de autenticação, a negociação do tipo de EAP ocorre entre o cliente de acesso e o servidor NPS.

**Cuidado**

Você não deve usar o PAP, SPAP, CHAP ou MS-CHAP em um ambiente de produção, pois eles são considerados altamente inseguros.

## Contabilização NPS

Você também precisa considerar como deve configurar o registro em log para o NPS. Você pode registrar as solicitações de autenticação de usuário e solicitações de contabilização para arquivos de log em formato de texto ou de banco de dados, ou pode fazer logon em um procedimento armazenado em um banco de dados do Microsoft SQL Server. Use o log de solicitações principalmente para fins de análise e cobrança de conexão e como ferramenta de investigação de segurança, pois ele permite que você identifique a atividade de um hacker.

## Configurar políticas no NPS

O NPS dá suporte a políticas de solicitação de conexão e políticas de rede. Elas são descritas na tabela a seguir.

| **Tipo** | **Descrição** |
| --- | --- |
| Política de solicitação de conexão | As políticas de solicitação de conexão permitem que você escolha se o servidor NPS local processa as solicitações de conexão ou as encaminha para outro servidor RADIUS processar |
| Política de rede | As políticas de rede permitem que você designe quais usuários estão autorizados a se conectar à rede e as circunstâncias em que eles podem se conectar. |

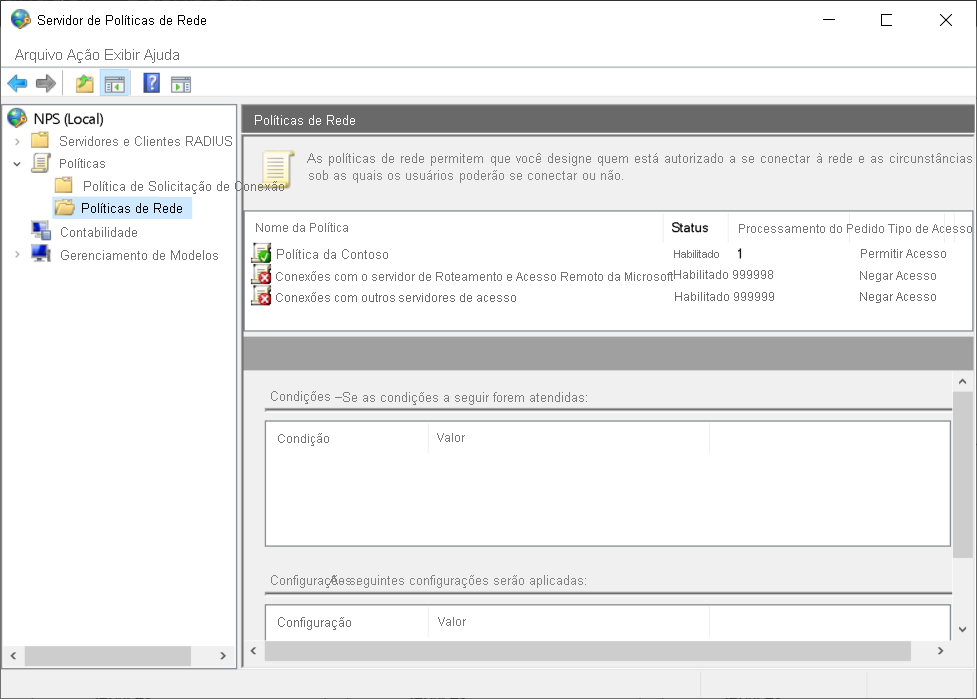
### Estabelecer as políticas de rede

Uma política de rede é um conjunto de condições, restrições e configurações que permitem designar quem está autorizado a se conectar à rede e as circunstâncias em que pode se conectar. Cada política de rede tem quatro categorias de propriedades.

| **Propriedade** | **Descrição** |
| --- | --- |
| Visão geral | As propriedades de visão geral permitem que você especifique se a política está habilitada, se a política concede ou nega acesso e se as solicitações de conexão exigem um método de conexão de rede ou tipo de servidor de acesso de rede específico. As propriedades de visão geral também permitem que você especifique se deseja ignorar as propriedades de discagem das contas de usuário no AD DS. Se você selecionar essa opção, o NPS usará apenas as configurações da política de rede para determinar se deve autorizar a conexão. |
| Condições | Essas propriedades permitem que você especifique as condições que a solicitação de conexão deve ter para corresponder à política de rede. Se as condições configuradas na política corresponderem à solicitação de conexão, o NPS aplicará as configurações de política de rede à conexão. Por exemplo, se você especificar o endereço IPv4 do servidor de acesso à rede (endereço IPv4 do NAS) como condição da política de rede e o NPS receber uma solicitação de conexão de um NAS que tem o endereço IP especificado, a condição na política corresponderá à solicitação de conexão. |
| Restrições | Restrições são parâmetros adicionais da política de rede necessários para corresponder à solicitação de conexão. Se a solicitação de conexão não corresponder a uma restrição, o NPS rejeita a solicitação automaticamente. Ao contrário da resposta do NPS a condições incompatíveis na rede, se uma restrição não corresponder, o NPS não avalia as políticas de rede adicionais e nega a solicitação de conexão. |
| Settings | As propriedades de configurações permitem que você especifique as configurações que o NPS aplica à solicitação de conexão, contanto que todas as condições da política de rede sejam compatíveis e a solicitação seja aceita. |

**Importante**

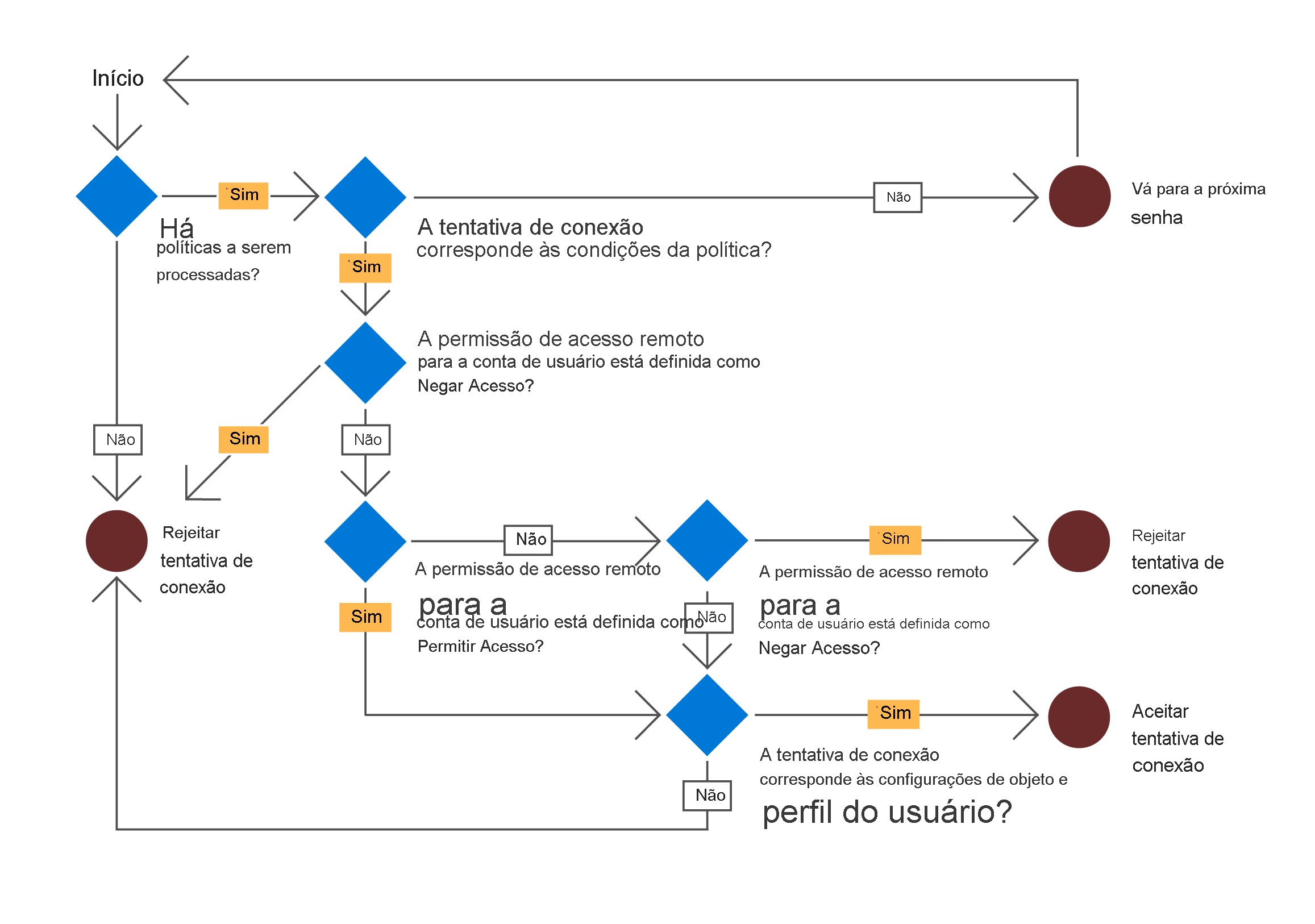
Quando você implanta a função NPS pela primeira vez, as duas políticas de rede padrão negam o acesso remoto a todas as tentativas de conexão. Você pode configurar políticas de rede adicionais para gerenciar as tentativas de conexão.



Quando o NPS autoriza uma solicitação de conexão, ele compara a solicitação a cada política de rede na lista ordenada de políticas, começando pela primeira política e passando para o próximo item na lista. Se o NPS encontrar uma política em que as condições correspondem à solicitação de conexão, ele usa a política correspondente e as propriedades de discagem da conta de usuário para autorizar a solicitação. Se você configurar as propriedades de discagem da conta de usuário para conceder ou controlar o acesso por meio da política de rede de rede, e a solicitação de conexão for autorizada, o NPS aplica as configurações definidas na política de rede para a conexão:

* Se o NPS não encontrar uma política de rede que corresponda à solicitação de conexão, o NPS rejeita a conexão.
* Se as propriedades de discagem da conta de usuário estiverem definidas para negar acesso, o NPS rejeita a solicitação de conexão mesmo assim.

Isso é resumido no diagrama a seguir.



## Unidade seguinte: Implantar uma PKI para acesso remoto

**Implantar uma PKI para acesso remoto**

Concluído100 XP

* 7 minutos

A Contoso pode usar certificados digitais para verificar e autenticar a identidade de cada parte envolvida em uma transação eletrônica. Os certificados digitais também ajudam a estabelecer a confiança entre os computadores e os aplicativos correspondentes hospedados nos servidores de aplicativos. O acesso remoto usa certificados para verificar a identidade dos servidores e fornecer criptografia. A Contoso também pode usar certificados para verificar a identidade de usuários ou computadores que se conectam para acesso remoto.

**Métodos para obter certificados**

Na maioria dos casos, você obtém certificados de uma autoridade de certificação. A consideração mais importante de uma autoridade de certificação é a confiança. Se um certificado for emitido por uma autoridade de certificação confiável, ele será confiável e poderá ser usado para autenticação. Se uma autoridade de certificação não for confiável, os certificados emitidos por ela não poderão ser usados para autenticação.

Para obter certificados, você pode:

* Criar sua própria autoridade de certificação privada usando o Windows Server. Os certificados emitidos por uma autoridade de certificação privada são automaticamente confiáveis para clientes e servidores Windows ingressados no domínio. No entanto, os certificados emitidos por uma autoridade de certificação interna não são automaticamente confiáveis para os dispositivos que não ingressaram no domínio.
* Compre certificados de uma autoridade de certificação pública. Os certificados emitidos por uma autoridade de certificação pública são automaticamente confiáveis para quase todos os dispositivos, independentemente de terem ingressado no domínio. O Windows não inclui ferramentas para implantar automaticamente os certificados de uma autoridade de certificação pública para usuários ou computadores.
* Gerar certificados autoassinados em alguns aplicativos. Por padrão, esses certificados são confiáveis apenas para o servidor emissor e não para outros computadores na organização.
* Gerar certificados autoassinados usando o PowerShell. Você pode usar o cmdlet New-SelfSignedCertificate para gerar um novo certificado autoassinado.

**Observação**

Você usa certificados autoassinados em organizações de pequeno e médio porte que usam o DirectAccess configurado com o assistente de introdução de fácil instalação e configuração.

**Considerações ao planejar a PKI**

Para determinar se você deve implementar uma PKI interna para acesso remoto, será necessário planejar como você usará os certificados. Se você estiver usando certificados somente em alguns servidores, o custo de usar uma autoridade de certificação pública será baixo. Os certificados de uma autoridade de certificação pública também são úteis, se você espera que dispositivos que não ingressaram no domínio acessem os servidores.

Uma autoridade de certificação privada é útil principalmente para acesso remoto, quando você está emitindo certificados para dispositivos cliente e usuários individuais para autenticação. Por exemplo, é comum exigir um certificado de computador válido para permitir o acesso VPN como segundo nível de autenticação, além de um nome de usuário e uma senha. Se você estiver emitindo certificados para muitos computadores, o registro automático fornecido por uma autoridade de certificação privada é importante. Também ocorre uma economia de custo significativa, pois você não precisa pagar por certificados emitidos por uma autoridade de certificação privada.

A tabela a seguir resume as vantagens e desvantagens dos certificados emitidos por autoridades de certificação privadas e públicas.

| **Tipo de autoridade de certificação** | **Vantagens** | **Desvantagens** |
| --- | --- | --- |
| Autoridade de certificação privada | Uma autoridade de certificação privada oferece maior controle sobre o gerenciamento de certificados e tem um custo menor em comparação com uma autoridade de certificação pública. Não há custo por certificado. Você também tem a opção de usar modelos personalizados e inscrição automática. | Por padrão, os certificados de autoridades de certificação privadas não são confiáveis para clientes externos (navegadores da Web e sistemas operacionais) e exigem mais administração. |
| CA Pública | Um certificado emitido por uma autoridade de certificação pública é confiável para muitos clientes externos (navegadores da Web e sistemas operacionais) e requer administração mínima. | O custo é maior em comparação a uma autoridade de certificação privada. O custo é baseado no certificado. A aquisição do certificado também é mais lenta. |

**Unidade seguinte: Usar o WAP como proxy da Web reverso**

# Usar o WAP como proxy da Web reverso

Concluído100 XP

* 10 minutos

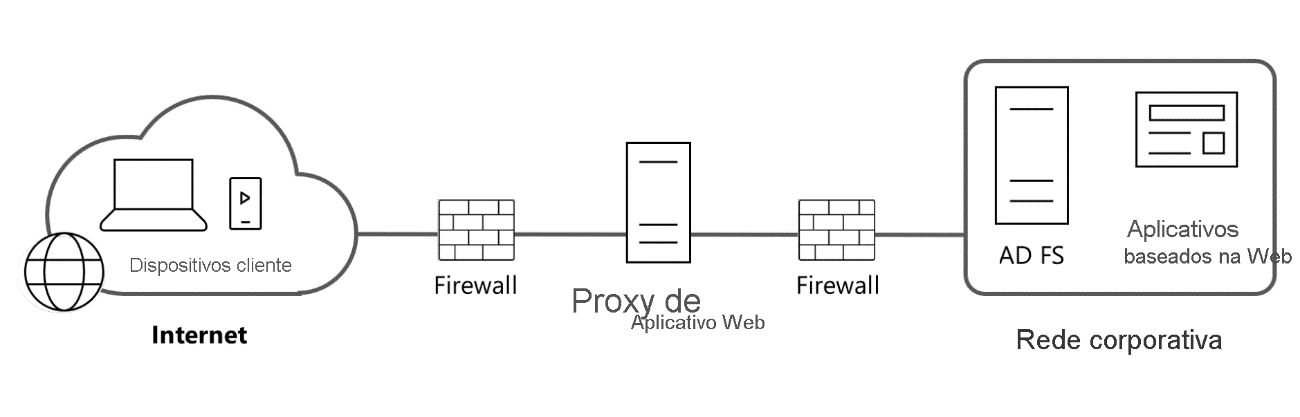
O Proxy de Aplicativo Web é um serviço de função Acesso Remoto. Esse serviço de função funciona como proxy da Web reverso e fornece aos usuários localizados na Internet o acesso a aplicativos Web corporativos internos ou servidores de Gateway de Área de Trabalho Remota. O proxy de aplicativo Web pode usar o AD FS para autenticar os usuários da Internet e atua como proxy AD FS para publicar aplicativos baseados em declarações.

**Observação**

Um aplicativo baseado em declarações pode usar as informações sobre um usuário, como associação de grupo, endereço de email, departamento ou empresa, como parte da autorização do usuário.

Antes de instalar o proxy de aplicativo Web, você deve implantar o AD FS como pré-requisito. O proxy de aplicativo Web usa o AD FS para serviços de autenticação. O AD FS fornece a funcionalidade de SSO, o que significa que, se os usuários inserirem as credenciais para acessar um aplicativo Web corporativo uma vez, eles não serão solicitados a inserir as credenciais novamente para acesso posterior ao aplicativo Web corporativo. Você também pode usar o AD FS para autenticar os usuários no proxy de aplicativo Web, antes que eles se comuniquem com o aplicativo.

Colocar o servidor proxy de aplicativo Web na rede de perímetro entre dois dispositivos de firewall é uma configuração típica. O servidor AD FS e os aplicativos publicados estão localizados na rede corporativa e, juntamente com os controladores de domínio e outros servidores internos, são protegidos pelo segundo firewall. Esse cenário fornece acesso seguro aos aplicativos corporativos para os usuários localizados na Internet e, ao mesmo tempo, protege a infraestrutura corporativa de TI contra ameaças à segurança na Internet.



## Opções de autenticação para o proxy de aplicativo Web

Ao configurar um aplicativo no proxy de aplicativo Web, você precisa selecionar o tipo de pré-autenticação. Você pode escolher pré-autenticação de AD FS ou pré-autenticação de passagem. A pré-autenticação de AD FS fornece mais recursos e benefícios, mas a pré-autenticação de passagem é compatível com todos os aplicativos Web.

### Pré-autenticação de AD FS

A pré-autenticação de AD FS usa o AD FS para aplicativos Web que utilizam a autenticação baseada em declarações. Quando um usuário inicia uma conexão com o aplicativo Web corporativo, o primeiro ponto de entrada a que o usuário se conecta é o proxy de aplicativo Web. O proxy de aplicativo Web autentica o usuário no servidor AD FS. Se a autenticação for realizada com sucesso, o proxy de aplicativo Web estabelece uma conexão com o servidor Web na rede corporativa em que o aplicativo está hospedado.

Ao usar a pré-autenticação de AD FS, você garante que somente os usuários autorizados possam enviar pacotes de dados para o aplicativo Web. Isso impede que hackers aproveitem as falhas do aplicativo Web antes da autenticação. A pré-autenticação de AD FS reduz significativamente a superfície de ataque de um aplicativo Web.

### Pré-autenticação de passagem

A pré-autenticação de passagem não usa o AD FS para autenticação e o proxy de aplicativo Web não autentica o usuário. Em vez disso, o usuário é conectado ao aplicativo Web por meio do proxy de aplicativo Web. O proxy de aplicativo Web recria os pacotes de dados conforme são entregues ao aplicativo Web, que fornece proteção contra falhas, como pacotes malformados. No entanto, a parte de dados do pacote passa para o aplicativo Web. O aplicativo Web é responsável por autenticar os usuários.

### Benefícios da pré-autenticação de AD FS

A pré-autenticação de AD FS fornece os seguintes benefícios em relação à pré-autenticação de passagem:

* SSO. Permite que os usuários pré-autenticados pelo AD FS insiram as credenciais somente uma vez. Se os usuários acessarem posteriormente outros aplicativos que usam o AD FS para autenticação, eles não serão solicitados a inserir novamente as credenciais.
* MFA (autenticação multifator). A MFA permite que você configure vários tipos de credenciais para reforçar a segurança. Por exemplo, você pode configurar o sistema para que os usuários insiram o nome de usuário e a senha juntamente com um cartão inteligente.
* Controle de acesso multifator. Controles de acesso multifator são usados em organizações que desejam fortalecer a segurança ao publicar aplicativos Web, implementando regras de declaração de autorização. As regras são configuradas para emitir uma permissão ou declaração de negação, que determina se o acesso de um usuário ou um grupo é permitido ou negado a um aplicativo Web que está usando a pré-autenticação de AD FS.

## Publicar os aplicativos com o proxy de aplicativo Web

Após a instalação do serviço de função Proxy de Aplicativo Web, você o configura usando o Assistente de Configuração de Proxy de Aplicativo Web no console de Gerenciamento de Acesso Remoto. Quando o Assistente de Configuração de Proxy de Aplicativo Web é concluído, ele cria o console de Proxy de Aplicativo Web, que pode ser usado para gerenciamento e configuração adicionais do Proxy de Aplicativo Web.

O Assistente de Configuração de Proxy de Aplicativo Web exige que você insira as seguintes informações durante o processo de configuração inicial:

* Nome do AD FS. Para localizar esse nome, abra o console de Gerenciamento do AD FS e, em Editar Propriedades do Serviço de Federação, encontre o valor na caixa Nome do Serviço de Federação.
* Credenciais da conta de administrador local para AD FS.
* Certificado de proxy do AD FS. Este é um certificado usado pelo Proxy de Aplicativo Web para a funcionalidade de proxy do AD FS.

**Dica**

O certificado de proxy do AD FS deve conter o nome do AD FS no campo de entidade do certificado, conforme exigido pelo Assistente de Configuração de Proxy de Aplicativo Web. Além disso, o campo de nomes alternativos da entidade do certificado deve incluir o nome do AD FS.

Depois de concluir o Assistente de Configuração de Proxy de Aplicativo Web, você pode publicar o aplicativo Web usando os cmdlets do console de Proxy de Aplicativo Web ou do Windows PowerShell. Os cmdlets do Windows PowerShell para gerenciar os aplicativos publicados são:

* Add-WebApplicationProxyApplication
* Get-WebApplicationProxyApplication
* Set-WebApplicationProxyApplication

Ao publicar o aplicativo Web, você deve fornecer as seguintes informações:

* O tipo de pré-autenticação, por exemplo, de passagem.
* O aplicativo a ser publicado.
* A URL externa do aplicativo, por exemplo, https://lon-svr1.adatum.com.
* Um certificado cujo nome da entidade cobre a URL externa, por exemplo, lon-svr1.adatum.com.
* A URL do servidor de back-end, que é inserida automaticamente quando você insere a URL externa.