

Configurar Políticas SIG para Acesso Remoto para Usuários de Conexão Segura

Contents

[Introdução](#)

[Overview](#)

[Políticas DNS](#)

[Políticas de firewall](#)

[Políticas da Web](#)

[Identificação de usuário da Web](#)

[Políticas DLP](#)

[Identificação de usuário PPD](#)

Introdução

Este documento descreve como criar políticas SIG para usuários de Acesso Remoto para Conexão Segura.

Overview

Este artigo da Base de conhecimento aplica-se aos clientes que usam o pacote Secure Connect, que inclui a funcionalidade de Acesso Remoto (VPNaaS) no Umbrella.

Os administradores podem configurar o Umbrella Firewall, a Web e as políticas de perda de dados para aplicar a usuários móveis conectados ao acesso remoto via AnyConnect.

Políticas DNS

É possível enviar consultas DNS para resolvedores de Umbrella (por exemplo, 208.67.222.222) por meio da conexão VPN de acesso remoto do AnyConnect. No entanto, isso não permite a identificação, a política ou o relatório do tráfego DNS no painel do Umbrella.

- Isso fornece apenas resolução de DNS e, portanto, não é normalmente recomendado.
- O uso de resolvedores DNS externos na configuração DNS da VPN impede a resolução de Zonas DNS internas.

DNS Servers

Your organization's private DNS Servers. Up to 10 servers.

4410210378004

Para adicionar identidade, política e relatório para consultas DNS, um dos três métodos deve ser considerado:

- (Recomendado) - Implante o [módulo de roaming Umbrella AnyConnect](#) (em Implantações > Computadores em roaming). O tráfego de DNS externo é enviado diretamente para o Umbrella com a identidade "Roaming Computer" aplicada. Este módulo também oferece suporte à [identificação de usuário do AD](#) opcional.
- Encaminhe o tráfego do servidor DNS local para o Umbrella e identifique o tráfego usando uma identidade de [rede](#). Todos os usuários recebem a mesma política/identidade e não há relatórios de usuários granulares.
- Use um [Umbrella Virtual Appliance](#) em sua rede local para encaminhar o tráfego para o Umbrella. As consultas DNS podem ser identificadas por seu endereço interno (endereço IP do pool VPN). A [integração com o AD](#) pode ser adicionada - requer a instalação de componentes locais adicionais.

Este exemplo mostra como uma Política DNS pode ser configurada (Políticas > Políticas DNS) para um cliente AnyConnect individual - isso só é possível quando o Módulo de roaming do Umbrella AnyConnect é implantado:

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed, in descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you want. [Help](#).

Content Category Migration Incomplete.

You must migrate all legacy content categories. For more information, see [Umbrella's Help](#).

[MIGRATE CONTENT CATEGORIES](#)

What would you like to protect?

Select Identities

Search Identities

All Identities / Roaming Computers

☒ AC_W10

1 Selected

[REMOVE ALL](#)

☐ AC_W10

4410210455444



Note: Ao usar o módulo Umbrella para o AnyConnect, o tráfego DNS pode, opcionalmente, ser enviado para dentro ou para fora do túnel, dependendo de sua configuração de tunelamento dividido.

Políticas de firewall

As políticas de firewall se aplicam ao tráfego entre os clientes de acesso remoto (AnyConnect) e a Internet. Configure as regras em "Deployments > Firewall Policy" (Implantações > Política de firewall) conforme a documentação encontrada aqui: [Gerenciar firewall](#).

A regra de firewall padrão se aplica aos clientes de Acesso Remoto. Se estiver criando uma política específica para usuários de Acesso Remoto, você poderá optar por criar uma nova política de firewall e selecionar "Orgid de Acesso Remoto:<ID>" como a identidade do túnel de origem.

A mesma política de firewall se aplica a todos os usuários de acesso remoto.

- As políticas de firewall não são usadas para controlar o acesso entre clientes RA e redes

Privadas/de Filial. Isso deve ser controlado com firewalls no local.

- Como todas as regras de firewall Umbrella, essas regras controlam as conexões de saída para clientes de Acesso Remoto. Conexões de entrada nunca são permitidas.
- O endereço IP origem para clientes de Acesso Remoto é sempre atribuído dinamicamente a partir do pool VPN.
 - Não é recomendável criar regras para um computador específico usando o "IP de origem", pois o IP é reatribuído dinamicamente
 - A criação de regras que afetam os usuários de um data center de acesso remoto específico é possível usando um intervalo de "CIDR de origem". Cada data center fornece um intervalo de pool de VPN diferente que é configurado na página "Implantações > Acesso remoto".

Rule Criteria

Specify the protocols, IPs, network tunnels, and ports to be allowed or blocked.

Protocol

Any Protocol

Applications

Any

Source Tunnels

Specify Tunnels

Q Remote Access orgId:5372429 X

CLEAR

Source IPs/CIDRs

Any

4409322341524



Note: A identificação por usuário não está disponível para políticas de firewall.

Políticas da Web

As políticas da Web se aplicam ao tráfego entre os clientes de acesso remoto (AnyConnect) e a Internet. Configure as regras em "Deployments > Web Policies" conforme a documentação encontrada aqui: [Gerenciar Políticas da Web](#).

- As políticas da Web não são usadas para controlar o acesso entre clientes RA e servidores Web Privados/de Filial. As políticas da Web aplicam-se somente a sites externos.

A política da Web padrão se aplica aos clientes de Acesso Remoto. No entanto, recomendamos [criar um novo conjunto de regras](#) para definir configurações de segurança especificamente para clientes de Acesso Remoto. Ao definir as identidades do conjunto de regras, escolha Remote Access orgid:<ID> na lista de túneis. A mesma política da Web se aplica a todos os usuários de acesso remoto.

Depois de criar um conjunto de regras, é possível [adicionar uma regra da Web](#) à qual define a Filtragem de categoria de conteúdo e as configurações do aplicativo.

Ruleset Identities

You must select ruleset identities for them to be added to this ruleset and have this ruleset enabled. Identities matching the ruleset can then be evaluated against the rules within the ruleset. This has the effect of a logical AND between the ruleset identity and the rule identity. Identities are first added to Umbrella through the Identities page. For more information, see Umbrella's [Help](#).

☐ AD Groups

☐ AD Users 4 >

☒ Tunnels 12 >

☐ Networks 1 >

☐ Roaming Computers

☐ Internal Networks (All Tunnels)

1 Selected REMOVE ALL

Remote Access orgId:5372429

CANCEL

SAVE

4409322363924

Identificação de usuário da Web

Por padrão, o tráfego de acesso remoto não pode ser controlado por usuário ou grupo. A mesma política se aplica a todo o tráfego de RA com base na identidade "orgid de acesso remoto". Para adicionar a identificação de usuário/grupo, você tem duas opções:

- Instale nosso módulo [AnyConnect Umbrella Roaming Security](#) e habilite o [recurso de agente SWG](#). O agente envia o tráfego da Web diretamente para o Umbrella SWG com a identidade "Computador em roaming" aplicada. Este módulo também oferece suporte à [identificação de usuário do AD](#) opcional.
- Habilite o [SAML](#) no conjunto de regras da Web que afeta sua identidade de "orgid de acesso remoto". Depois de se conectar ao acesso remoto, os usuários do RA são solicitados a se autenticar via SAML uma segunda vez ao gerar o tráfego do navegador da Web.

Note: Ao usar o módulo Umbrella para o AnyConnect, o tráfego SWG pode, opcionalmente, ser enviado para dentro ou para fora do túnel, dependendo de sua configuração de tunelamento dividido.

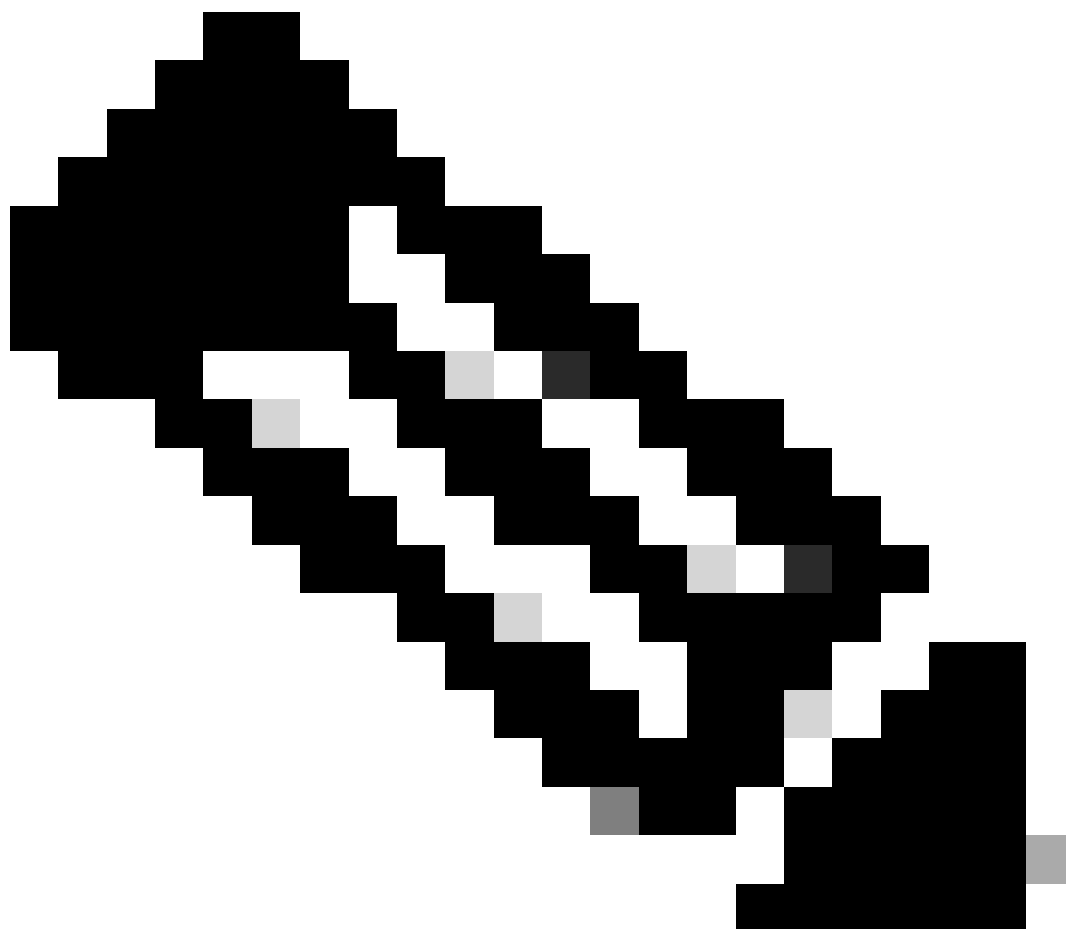
Este exemplo mostra como uma Política DNS pode ser configurada (Políticas > Políticas DNS) para um cliente AnyConnect individual - isso só é possível quando o Módulo de roaming do Umbrella AnyConnect é implantado:

The screenshot displays the 'Ruleset 3' configuration page in the Umbrella console. At the top, a status bar indicates 'Contains 0 Identity', 'Applied To', and 'Last Modified Nov 11, 2021'. A prominent orange warning banner states: 'Ruleset disabled. You must select at least one ruleset identity to enable this ruleset so that its settings and rules are evaluated and enforced.' Below this, the 'Ruleset Rules' section features an 'ADD RULE' button and a table with columns for Priority, Rule Name, Rule Action, and Identities. The table contains one entry: 'Rule 1' with a 'Block' action. To the right of the table, a search bar for identities is shown, and a dropdown menu is open, displaying '1 Anyconnect Client' and 'AC_W10' (which is selected). A '1 Selected' indicator is visible. On the far right, a 'SAVE' button and a trash icon are present.

Políticas DLP

As políticas de perda de dados aplicam-se ao tráfego entre os clientes de acesso remoto (AnyConnect) e a Internet. Configure as regras em 'Implantações > Políticas de prevenção de perda de dados' conforme a documentação encontrada aqui: [Gerenciar Políticas de Proteção de Dados](#).

- As políticas DLP não são usadas para controlar o acesso entre clientes RA e servidores Web Privados/Filiais. As políticas DLP aplicam-se somente a sites externos de tráfego.
-



Note: Para que as políticas DLP sejam aplicadas, você deve primeiro ter criado um conjunto de regras da Web para usuários de acesso remoto. O conjunto de regras da Web deve ter Descriptografia HTTPS Habilitada.

Ao selecionar identidades para uma regra de proteção de Dados, escolha Orgid de Acesso Remoto:<ID>. A mesma política de proteção de dados se aplica a todos os usuários. Para concluir a regra PPD, você também precisa selecionar ou definir [Classificadores PPD](#).

Identities

Select identities to add them to this rule.

All Identities

☐	AD Groups	
☐	AD Users	4 >
☒	Tunnels	12 >
☐	Networks	1 >
☐	Roaming Computers	
☐	Internal Networks (All Tunnels)	

1 Selected [REMOVE ALL](#)

☒ Remote Access orgId:5372429

4409322428820

Identificação de usuário PPD

O DLP obtém a identidade do usuário do gateway da Web seguro (políticas da Web). Consulte a seção de políticas da Web para obter instruções sobre como adicionar a identificação do usuário.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.