Configurar o cliente Umbrella Roaming em uma rede corporativa

Contents

Introdução

Este documento descreve a configuração do cliente de roaming Umbrella na rede da sua empresa.

Overview

O cliente de roaming Umbrella é uma excelente ferramenta para proteger usuários remotos, mas também pode proteger usuários em sua rede corporativa, adicionando outra camada de segurança. Dependendo das necessidades da empresa, alguns administradores querem a proteção contínua do cliente de roaming Umbrella na rede corporativa, enquanto outros administradores preferem ter o cliente de roaming Umbrella 'recuando' em favor de outras políticas Umbrella.

A Umbrella oferece flexibilidade sobre como o cliente de roaming Umbrella opera quando ele entra em sua rede. Este artigo descreve essas diferentes abordagens.

Metas

P). Por que eu desabilitaria o cliente de roaming Umbrella na rede da minha empresa?

Normalmente, não há necessidade de desativar o cliente de roaming Umbrella para que o DNS interno e externo funcione. O cliente de roaming Umbrella usa o recurso Gerenciamento de Domínio para direcionar o tráfego de DNS interno para seus servidores DNS normais. Isso permite que você mantenha a proteção e a conectividade enquanto o cliente de roaming Umbrella é executado em seus endpoints na rede.

No entanto, às vezes há motivos para considerar desativar a proteção do cliente de roaming...

- Fornecer uma política '*na rede*' e '*fora da rede*' diferente para usuários móveis que deixam a rede.
- Usar um servidor DNS interno em uma rede corporativa oferece alguns benefícios em termos de cache e tráfego de DNS de saída reduzido.
- O cliente de roaming Umbrella envia periodicamente mensagens de sondagem para verificar a conexão com o Umbrella. Esse tráfego adicional pode ser indesejado quando você tem um número muito grande de clientes.

P) Por que eu gostaria que o cliente de roaming Umbrella permanecesse ativado na rede da minha empresa?

Por outro lado, há alguns bons motivos para manter o cliente de roaming habilitado o tempo todo:

- Verifique se o computador cliente de roaming Umbrella usa a mesma política o tempo todo.
- Sempre tendo o nome de host do cliente de roaming Umbrella identificável em relatórios (em vez da identidade da rede) - para relatórios granulares.
- O cliente de roaming usa o tráfego 'DNS criptografado' para melhorar a privacidade
- Para usuários de gateway da Web seguro (usando o AnyConnect), o cliente deve permanecer ativado para fornecer filtragem da Web SWG.

Modos de operação

Sempre ATIVADO

O cliente de roaming Umbrella pode permanecer ativado mesmo quando usado na rede da empresa. Nesse modo, as políticas são configuradas usando a Identidade do cliente de roaming Umbrella, e essa Identidade aparece nos relatórios.

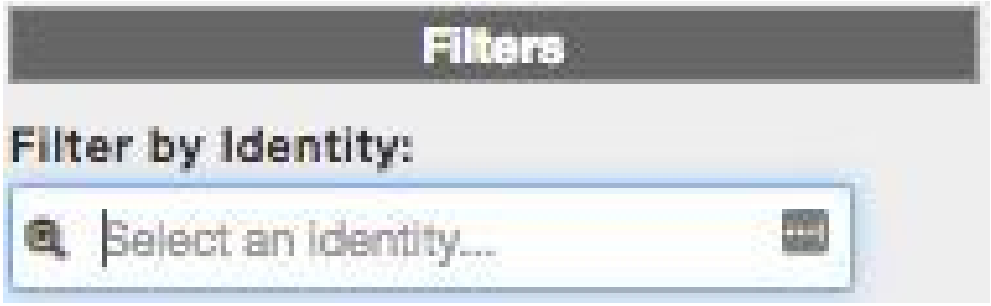
Política	A Identidade do cliente de roaming Umbrella é sempre usada.
Relatórios	A Identidade do cliente de roaming Umbrella sempre aparece em relatórios que oferecem granularidade por máquina
Tráfego DNS	• O cliente de roaming Umbrella continua a enviar consultas DNS diretamente ao Umbrella, mesmo quando em uma rede da empresa. • As consultas enviadas ao Umbrella são criptografadas, fornecendo segurança adicional. • As consultas de 'Domínios internos' são roteadas para seus servidores

	DNS normais e não enviadas para o Umbrella.
Mensagens de sondagem	O cliente de roaming Umbrella continua a enviar mensagens de sondagem para determinar a disponibilidade do Umbrella.

Como configurar o modo 'Always ON':

1. Navegue até Identities > Roaming Computers.
2. Clique no ícone (Roaming client settings).
3. Desmarque Desabilitar redirecionamento DNS em uma rede protegida por guarda-chuva e clique em Salvar.
4. Crie uma política separada para seus clientes de roaming Umbrella e certifique-se de que seja a prioridade mais alta (o topo da lista). Sua política de cliente de roaming Umbrella deve ter uma precedência maior do que qualquer política baseada em identidades de rede.

Usar Política de Rede Regular
O cliente de roaming Umbrella está habilitado e continua a falar diretamente com o Umbrella, no entanto, a Identidade de Rede é usada para fins de política e relatórios. Esse modo é ativado simplesmente colocando a política de rede em uma precedência mais alta do que a política de cliente de roaming Umbrella.

Política	A política de rede é usada na rede protegida. Isso permite diferentes políticas de entrada/saída da rede.
Relatórios	• O relatório é associado à identidade de rede como a identidade principal. • Os relatórios ainda permitem que você pesquise por meio do nome de host do cliente de roaming Umbrella para filtrar os resultados apenas para esse cliente. 

Tráfego DNS	• O cliente de roaming Umbrella continua a enviar consultas DNS diretamente ao Umbrella, mesmo quando em uma rede da empresa. • As consultas enviadas ao Umbrella são criptografadas, fornecendo segurança adicional. • As consultas de 'Domínios internos' são roteadas para seus servidores DNS normais e não enviadas para o Umbrella.
Mensagens de sondagem	O cliente de roaming Umbrella continua a enviar mensagens de sondagem para determinar a disponibilidade do Umbrella.

Como "Usar Política de Rede Regular":

1. Navegue até Identities > Roaming Computers.
2. Clique no ícone (Roaming client settings).
3. Desmarque Desabilitar redirecionamento DNS em uma rede protegida por guarda-chuva e clique em Salvar.
4. Crie uma política separada para sua(s) rede(s). Certifique-se de que a política para a(s) sua(s) rede(s) tenha uma precedência mais alta do que qualquer política baseada no cliente de roaming.

Desabilitar atrás de redes protegidas (ideal para redes menores)
O cliente de roaming Umbrella pode "recuar" quando detecta que está em uma rede protegida. Isso significa que a Identidade de rede é usada para fins de política e relatório.

Este modo tem um comportamento semelhante ao do modo 'Usar Política de Rede Regular', exceto pelo fato de que o cliente de roaming Umbrella realmente se desativa e não interfere no tráfego DNS.

Política	A política de rede é usada na rede protegida. Isso permite diferentes políticas de entrada/saída da rede.
Relatórios	Quando na rede protegida, não há granularidade por máquina para os relatórios. Os relatórios são associados somente à Identidade de rede.
Tráfego DNS	Quando na rede protegida, o cliente de roaming Umbrella não interfere nas consultas DNS e elas vão para o servidor DNS interno normal.

Mensagens de sondagem	O cliente de roaming Umbrella continua a enviar mensagens de sondagem para determinar se está em uma rede protegida.

Como configurar Desabilitar atrás de redes protegidas:

1. Navegue até Identities > Roaming Computers.
2. Clique no ícone (Roaming client settings).
3. Selecione Disable DNS redirection while on an Umbrella Protected Network e clique em Save.
4. Navegue até Policies > Policies List.
5. Crie uma política separada para sua(s) rede(s). Verifique se a política para a(s) sua(s) rede(s) tem precedência sobre qualquer política baseada no cliente de roaming Umbrella.
6. Os servidores DNS locais devem estar encaminhando para os resolvedores do Umbrella e devem ser registrados corretamente no painel do Umbrella.
7. Para que esse recurso funcione, o IP de saída usado pela estação de trabalho cliente deve ser registrado com a mesma identidade de rede do IP de saída usado pelos servidores DNS internos. Para obter mais detalhes, consulte este artigo.

Desabilitar atrás de domínio de rede confiável (ideal para redes maiores)

Agora é possível escolher um 'Domínio de rede confiável' configurado pelo cliente. O cliente tenta resolver esse domínio DNS (registro A) e desabilitar a proteção quando o domínio é resolvido com êxito. Esse é um registro DNS somente interno que só é resolvido quando o cliente está na rede da empresa.

Política	O cliente faz back-off sempre que o Domínio Confiável é detectado e não necessariamente recebe a política ou filtragem Umbrella. Recomendamos adicionar outros recursos do Umbrella (por exemplo, Proteção de rede) para garantir que a política ainda seja aplicada na rede da empresa.
Relatórios	O cliente faz back-off sempre que o Domínio Confiável é detectado e não necessariamente recebe a política ou filtragem Umbrella. Se a rede estiver protegida por outros recursos do Umbrella (por exemplo, Proteção de rede), o tráfego aparecerá nos relatórios sob a identidade da rede.
Tráfego DNS	Quando na rede confiável, o cliente de roaming Umbrella não interfere nas consultas DNS e elas vão para o servidor DNS interno normal.

Mensagens de sondagem	O cliente de roaming Umbrella desabilita a maioria de seus testes 'probe' DNS nesse estado, reduzindo significativamente a quantidade de tráfego gerado por Clientes de Roaming.

Como configurar o Domínio de rede confiável:

1. Crie um registro DNS A em seus servidores DNS internos (por exemplo, magic.mydomain.tld) (em inglês).
    1. O registro deve ser um "subdomínio" (mínimo de 3 rótulos DNS)
    2. O registro deve ser resolvido para um endereço RFC-1918 interno
    3. Certifique-se de que o registro não exista publicamente
2. Navegue até Identities > Roaming Computers.
3. Clique no ícone (Roaming client settings).
4. Selecione a opção Trusted Network Domain e insira o nome do domínio (por exemplo, magic.mydomain.tld) (em inglês). Click Save.

Usando o cliente de roaming Umbrella com um dispositivo virtual Umbrella

Como parte do produto "Insights" da Umbrella (nos pacotes Platform and Insights), fornecemos um Virtual Appliance (VA) que atua como um encaminhador DNS dentro da sua rede. Essa VA é a chave para obter visibilidade sobre a origem das solicitações DNS na rede e também é necessária para a integração com o Ative Diretory.

Por padrão, o cliente de roaming Umbrella desabilita-se se detectar que um VA está sendo usado para encaminhamento DNS. Se o VA tiver sido atribuído como servidor DNS (usando as configurações estáticas ou DHCP), o cliente de roaming Umbrella detectará isso e desabilitará a si mesmo.

Retorno de VA

Política	Com a Retorno de VA habilitada, a Identidade de VA é usada para decidir a política escolhida. As políticas podem ser criadas com base nestas identidades: • Usuário do AD (somente se a integração com o AD estiver habilitada) • Computador do AD (somente se a integração com o AD estiver habilitada) • Rede interna • Nome do site principal. Clique aqui para obter mais informações sobre a precedência da política.

Relatórios	Com o recurso de recuo de VA habilitado, o cliente de roaming Umbrella é desabilitado quando está atrás de um VA e não é mostrado em relatórios. Os relatórios são registrados como: • Usuário do AD (somente se a integração com o AD estiver habilitada) • Computador do AD (somente se a integração com o AD estiver habilitada) • Rede interna • Nome do site principal. Além disso, o endereço IP do cliente interno é registrado para cada solicitação. 
Tráfego DNS	• O cliente de roaming Umbrella não interfere nas consultas DNS e elas vão para o dispositivo virtual. • O VA encaminha consultas externas de DNS para o Umbrella (criptografado). • O VA roteia consultas de DNS interno conforme apropriado e as encaminha para os servidores DNS internos configurados.
Mensagens de sondagem	O cliente de roaming Umbrella ainda envia mensagens de sondagem ao Umbrella, mas faz isso a uma taxa reduzida.

Como configurar a retirada de VA:

1. Este recurso está ativado por padrão, mas você pode verificar seu status (e, opcionalmente, desativá-lo)
2. Navegue até Identities > Roaming Computers.
3. Clique no ícone (Roaming client settings).
4. Selecione a opção VA Backoff

Módulo de segurança de roaming Cisco Umbrella AnyConnect

O módulo Umbrella para Cisco AnyConnect suporta todos os mesmos modos de operação, conforme descrito acima. Dois modos adicionais específicos do AnyConnect também estão disponíveis. Esses dois modos podem ser ativados no Umbrella Dashboard na página Identities > Roaming Computers, no entanto, é necessária uma configuração adicional no perfil do AnyConnect VPN.

- Respeite a detecção de rede confiável do AnyConnect.
  Esse recurso faz com que o módulo de segurança Umbrella seja desabilitado quando o

Cisco AnyConnect determinar que ele está em uma rede confiável. Isso depende do recurso de detecção de rede confiável do AnyConnect para identificar a rede. Domínios confiáveis, servidores DNS e URLs podem ser usados para identificar a rede da sua empresa. Para obter mais informações, consulte a documentação do AnyConnect.

- Desabilitar o cliente de roaming enquanto sessões VPN de túnel completo estão ativas
  Com esse recurso habilitado, o módulo Umbrella é desabilitado quando o AnyConnect está conectado a uma VPN de túnel completo (ou Túnel All DNS).

Quando desativado, o cliente de roaming não filtra o tráfego DNS, portanto, é importante garantir que sua rede esteja coberta por outra segurança, como nosso recurso de proteção de rede.

Mais informações

Se você quiser desativar o cliente de roaming na rede da sua empresa, mas precisar de mais controle, ou quiser discutir outras opções, entre em contato com o suporte do Cisco Umbrella.

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.