

Solucionar problemas de entradas do log de atividades do DNS com decisão bloqueada

Contents

Problema

Um ou mais destes sintomas são relatados:

- A pesquisa de atividade (Monitorar > Pesquisa de atividade, filtrada para eventos DNS) mostra Decisão/Ação = Bloqueada para um domínio, mas a revisão das regras de acesso à Internet não revela uma regra que obviamente a bloqueie.
- O domínio não está presente em nenhuma lista de destino de bloqueio mantida pelo administrador.

Ambiente

- As informações neste documento são baseadas em:
 - Plataforma de nuvem Cisco Secure Access (SSE)
 - Cisco Secure Client 5.x com o módulo de segurança de roaming implantado e registrado em uma organização de acesso seguro

Resolução

Etapa 1. Verificar a identidade que foi avaliada

- Confirme a identidade contra a qual a decisão foi tomada. Se o evento mostrar uma identidade de rede, site ou túnel em vez do usuário ou computador móvel esperado, a consulta correspondeu a um conjunto de regras diferente do analisado.
- Para usuários em roaming, verifique se o dispositivo está registrado e reportando como protegido

Incompatibilidade de identidade: Corrija a implantação para que a identidade desejada seja aplicada — registre o dispositivo de roaming, corrija o mapeamento do AD/grupo de usuários ou ajuste o conjunto de regras de identidade de rede — em vez de soltar a regra que correspondeu incorretamente.

Etapa 2: Verificar uma correspondência de categoria de segurança

- Se o evento transportar uma categoria de segurança (malware, C2, phishing, domínios vistos recentemente, tunelamento DNS etc.), o bloqueio veio das configurações de segurança do conjunto de regras correspondente — nenhuma regra de conteúdo ou lista de destino precisa fazer referência ao domínio.
- Pesquise a reputação atual e a categorização do domínio no portal Cisco Talos Intelligence em <https://talosintelligence.com/> (pesquisa no Reputation Center).
- Se a categorização ou reputação mostrada no Talos estiver incorreta, envie uma solicitação de contestação/reclassificação (abra um caso) com o Talos diretamente através de <https://talosintelligence.com/> para que o domínio seja reavaliado. Depois que o Talos atualizar a classificação, a alteração será propagada para a aplicação de acesso seguro.

Etapa 3: Inspeccionar a cadeia CNAME

- Resolva o domínio de um ponto de vista não filtrado e inspecione toda a cadeia de respostas (por exemplo, `dig +noall +answer <domain>` OU `nslookup -debug <domain>`).
- Verificar cada alvo CNAME na cadeia em relação às listas de destino e à categorização do Talos; um destino CNAME bloqueado explica uma decisão Bloqueada em um domínio aparentemente limpo consultado

Etapa 4: Reavaliar a política de cima para baixo para a identidade real

- Percorra as regras de acesso à Internet em ordem como a identidade da Etapa 1, verificando o escopo de identidade de cada regra, programação, estado habilitado e configurações de segurança/conteúdo/aplicativo, até e incluindo a regra padrão.
- Use o Policy Tester (por exemplo, policy.test.sse.cisco.com/?=cisco.com) com a identidade e o destino exatos para ver qual regra o Secure Access relata como a correspondência e compare-a com a regra nomeada no evento.

Caso especial: Domínios Vistos Recentemente

Se a categoria de segurança no evento for Domínios recentemente vistos (NSD)

Opções de correção, por ordem de preferência:

Se o domínio for crítico para os negócios, adicione-o a uma Lista de destinos de permissão referenciada pela regra aplicável; uma entrada de permissão tem precedência sobre o bloco de segurança do NSD para esse destino.

Desabilitar DNS criptografado (DoH) e QUIC

O DNS criptografado e o QUIC podem causar lacunas de visibilidade na camada DNS que contribuem para confundir os resultados da pesquisa de atividades: As consultas resolvidas pelo DoH do navegador nunca alcançam os resolvedores de Acesso Seguro (portanto, estão totalmente ausentes do log), enquanto os domínios do provedor do DoH podem aparecer como eventos Bloqueados.

Desabilitar esses transportes em pontos de extremidade gerenciados garante que todo o DNS permaneça inspecionável e o Registro de atividades reflita o comportamento real do ponto de extremidade.

DNS sobre HTTPS (DoH) por navegador

Google Chrome

- Manual: navegue até `chrome://settings/security` e desative Usar DNS seguro.

Microsoft Edge

- Manual: navegue até `edge://settings/privacy` e desative Usar DNS seguro.

Mozilla Firefox

- Manual: Menu > Configurações > Privacidade e segurança > DNS sobre HTTPS (ou Configurações de rede em versões mais antigas) e selecione Off / desmarque Enable DNS over HTTPS.
- Note: Os resolvedores do Umbrella/Secure Access respondem ao domínio canário Mozilla (use-application-dns.net) de uma forma que sinaliza ao Firefox para manter o DoH desativado por padrão; configurações explícitas de GPO ainda são recomendadas porque a configuração DoH definida pelo usuário substitui a verificação canary. Caution: não adicione os domínios kill-switch/canary do Mozilla a uma lista de destinos de bloqueio — uma resposta de registro A de página de bloqueio é tratada como válida e pode fazer com que o Firefox mantenha ou atualize seu uso do DoH.

QUIC (HTTP/3)

O QUIC é executado em UDP/443 e pode transportar tráfego geral da Web e DoH3 (DNS sobre HTTP/3), ignorando caminhos de inspeção que esperam TCP.

Desabilitar o QUIC força os navegadores a retornar para HTTP/2 ou HTTP/1.1 baseado em TCP, que restaura a visibilidade total:

- Cromado/borda: Manual (não persistente, alterável pelo usuário): defina `chrome://flags/#enable-quic` / `edge://flags/#enable-quic` como Disabled.
- Firefox defina a preferência `network.http.http3.enable = false` (`about:config` ou `policy/AutoConfig`).

Se, após essas etapas, a regra correspondente relatada no evento ainda não puder ser reconciliada com a configuração, abra um caso no TAC da Cisco e forneça a exportação do evento Activity Search (carimbo de data/hora com fuso horário, identidades, regra correspondente, categorias, tipo de registro e domínio) junto com capturas de tela das regras relevantes e listas de destino.

Causa

Correspondência de categoria de segurança (inteligência do Talos) - O domínio é bloqueado por uma configuração de segurança — por exemplo, malware, comando e controle, phishing, criptografia, encapsulamento DNS ou domínios vistos recentemente — com base na reputação e na categorização do Cisco Talos, e não por qualquer lista de destino ou regra de conteúdo configurada explicitamente pelo administrador. Essa é a causa mais frequente de blocos de "correspondência não óbvia".

Incompatibilidade de atribuição de identidade - A consulta foi atribuída a uma identidade diferente da esperada (identidade de rede/site em vez do computador em roaming, um usuário/grupo do AD diferente ou um dispositivo não registrado que retorne a uma política de nível de rede), portanto uma regra diferente (geralmente mais estrita ou padrão) foi correspondida.

Ordem das regras e regra padrão - uma regra mais ampla no topo da política (ou a regra padrão/abrangente na parte inferior) correspondida antes da regra Permitir pretendida; a regra desejada também pode ser desabilitada, agendada ou definida para identidades que não incluem a origem afetada.

Herança da lista de destino - Uma lista de destino de bloqueio contém um domínio pai (example.com), que cobre implicitamente todos os subdomínios (app.example.com), ou contém um IP/CIDR que o domínio resolve. Pesquisar nas listas o FQDN exato sozinho não revela isso.

Bloqueio de cadeia CNAME - O domínio consultado é permitido, mas sua cadeia de resolução contém um CNAME para um domínio (geralmente um CDN, rastreador ou host estacionado/bloqueado) que está bloqueado; a decisão é aplicada à cadeia e o registro mostra o domínio originalmente consultado como Bloqueado.

Correspondência de categoria de aplicativo ou conteúdo - O domínio pertence a um aplicativo bloqueado (controle de aplicativo) ou categoria de conteúdo que o administrador não associou a ele; a categorização pode diferir da intuição (por exemplo, uma ferramenta de negócios categorizada como Compartilhamento de arquivos ou Proxy/Anonymizer).

Mudança recente de política ou categorização - A política ou a categorização do Talos mudou recentemente; o evento em revisão antecede (ou antecede) a alteração ou a propagação de política/sincronização do cliente não foi concluída no momento da consulta.

Conteúdo relacionado

- [Configurar Servidores DNS Internos para Umbrella](#)
- [Configurar DNS sobre HTTPS \(DoH\) com Umbrella](#)
- [Adicionar um controlador de domínio no acesso seguro](#)
- [Informações da página Bloco de acesso seguro da Cisco](#)
- [Suporte técnico e downloads da Cisco](#)

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.