A Pesquisa de atividade do Secure Access exibe nomes de regra DESCONHECIDOS

Contents

Problema

Durante uma migração do Umbrella para SSE, os eventos de Pesquisa de atividade de acesso seguro exibem o Nome da regra como DESCONHECIDO em vez de mostrar as regras de política nomeadas. Esse comportamento foi observado para vários tipos de tráfego, incluindo tráfego permitido, como solicitações para chatgpt.com. A preocupação era se essas entradas de nome de regra DESCONHECIDO indicavam um problema de configuração de política ou problema de migração que exigia correção.

Ambiente

- Cisco Secure Access (SSE)
- Organização que está passando pela migração do Umbrella para SSE
- Relatório de pesquisa de atividade de acesso seguro
- Tráfego categorizado como Domínios Vistos Recentemente

Resolução

O comportamento Nome da regra DESCONHECIDO é esperado e normal para eventos tratados pela lógica do sistema Secure Access em vez de regras nomeadas/criadas pelo cliente. Isso geralmente ocorre para o tráfego categorizado como Domínios vistos recentemente, onde o domínio foi visto recentemente no momento da consulta e é relatado como tal nos relatórios de Atividade de pesquisa ou Atividade de segurança.

Interpretando Eventos de Pesquisa de Atividade com Nomes de Regra DESCONHECIDOS

Ao encontrar eventos com Nome da regra DESCONHECIDO, revise estes campos de evento para determinar o motivo da aplicação e confirme a aplicação correta da política:

- Ação - Mostra se o tráfego foi permitido ou bloqueado
- Motivo do bloqueio do evento/Motivo do bloqueio - Fornece detalhes específicos de aplicação
- Categorias - Mostra a categorização de conteúdo (como Domínios Vistos Recentemente)
- Domínio/IP de destino - Destino da solicitação
- Identidade do usuário/origem - Origem do tráfego
- Timestamp - Quando o evento ocorreu

Se o campo Categories mostrar Newly Seen Domains, então UNKNOWN no campo do nome da regra é o comportamento esperado e não indica uma falha na migração ou corrupção da política.

Etapas de validação para comportamento inesperado

Se era esperado que o tráfego correspondesse a uma regra nomeada específica, mas mostra UNKNOWN, colete essas informações para validação de caminho de política:

- 2-3 exemplos de carimbos de data/hora de eventos
- Domínio/IP de destino para cada evento
- Identidade de usuário/origem para cada evento

Essas informações podem ser usadas para comparar o caminho de política esperado com o comportamento real do evento e determinar se é necessária uma investigação mais detalhada.

Causa

O nome da regra UNKNOWN é exibido quando a lógica do sistema Secure Access processa o tráfego em vez de aplicar uma regra de política nomeada/criada pelo cliente. Esse é o comportamento documentado para determinadas categorias de tráfego, particularmente Domínios recentemente vistos, em que os mecanismos de classificação e tratamento internos têm precedência sobre as regras nomeadas durante a avaliação inicial do domínio.

Conteúdo relacionado

- Habilitar Segurança de Domínios Recentemente Vistos
- 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.