Como bloquear aplicativos desconhecidos em um aplicativo da Web seguro

Contents

Introduction

Este documento descreve vários métodos para bloquear aplicativos desconhecidos no Cisco Secure Web Appliance.

Métodos para bloquear aplicativos desconhecidos

Você pode usar qualquer um desses métodos sozinho ou em combinação.

> **Note**: Este artigo da base de conhecimento faz referência ao software para o qual a Cisco não oferece manutenção ou compatibilidade. As informações foram disponibilizadas como cortesia para sua conveniência. Para obter mais assistência, entre em contato com o fornecedor do software.

Bloquear aplicativos com base em strings de agentes de usuário

A primeira defesa é usar as strings de Agente de Usuário para bloquear aplicativos desconhecidos.

- Adicione o Agente de usuário em **Web Security Manager** > **Access Policies** > **Protocols and User Agents** column <para a política de acesso necessária>.
- Adicione a cadeia de caracteres do Agente de Usuário em **Block Custom User Agents** (um por linha).

> **Note**: Você pode usar os links fornecidos em Referência para pesquisar Agentes de usuário.

Bloquear aplicativos com base nos controles de visibilidade de aplicativos

Se o Application Visibility Controls (AVC) estiver habilitado (em **GUI > Security Services > Web Reputation and Anti-Malware**), você pode bloquear o acesso com base em tipos de aplicativos como Proxies, Compartilhamento de Arquivos, Utilitários da Internet e assim por diante. Você pode fazer isso sob **Web Security Manager > Access Policies > Applications** column <para a política de acesso necessária>.

Bloquear aplicativos com base no tipo MIME

Se o Agente de usuário não existir, você pode tentar adicionar o tipo MIME (Multipurpose Internet Mail Extensions):

- Adicionar tipos MIME em **Web Security Manager** > **Web Access Policies** > **Objects** column <para a política de acesso necessária>.
- Adicionar o tipo de objeto/MIME no **Block Custom MIME Types** (uma por linha). Por exemplo, para bloquear aplicativos BitTorrent, digite application/x-bittorrent.

Note: Você pode usar os links fornecidos em Referência para pesquisar tipos MIME.

Bloquear categorias de URL em políticas de acesso

Certifique-se de que categorias como Prevenção de filtros, Atividades ilegais, Downloads ilegais e assim por diante estejam bloqueadas nas políticas de acesso. Se alguns aplicativos usarem URLs ou endereços IP conhecidos para suas conexões, você poderá bloquear suas categorias de URL predefinidas associadas ou configurá-las em uma categoria de URL personalizada bloqueada usando seu endereço IP, FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) ou um regex que corresponda aos domínios. Você pode fazer isso sob **Web Security Manager > Access Policies > URL Categories** coluna.

Restringir a configuração de portas de CONEXÃO HTTP na política de acesso

Alguns aplicativos podem usar o método HTTP CONNECT para se conectarem a portas diferentes. Permitir apenas portas conhecidas ou as portas específicas necessárias em seu ambiente nos domínios de configuração de portas HTTP CONNECT:

- O HTTP CONNECT pode ser configurado em **Web Security Manager** > **Access Policies** > **Protocols and User Agents** column <para a política de acesso necessária>.
- Adicionar portas permitidas em **HTTP CONNECT Ports**.

Bloquear acesso para endereços IP específicos

Para aplicativos nos quais você só sabe sobre endereços IP de destino que estão sendo acessados, é possível usar o recurso L4 Traffic Monitor para bloquear o acesso para esses endereços IP específicos. Você pode adicionar os IPs de destino em **Web Security Manager > L4 Traffic Monitor > Additional Suspected Malware Addresses**.

Como localizar o agente de usuário ou o tipo MIME que um aplicativo usa

Se você não souber qual tipo de agente de usuário ou MIME está sendo usado por determinados aplicativos, poderá executar qualquer uma destas etapas para encontrar essas informações:

- Execute uma captura de pacote com o WireShark (Ethereal) na máquina do cliente e filtre para o protocolo 'http'.
- Execute a captura no Secure Web Appliance (em **Support and Help** > **Packet Capture**), filtrado no endereço IP do cliente.

Referência

> **Note**: Os sites externos listados aqui são fornecidos apenas para referência. Os links e o conteúdo não são controlados pela Cisco e estão sujeitos a alterações.

Lista de agentes de usuário

User Agent String.Com (em useragentstring.com)

Lista de tipos MIME

- Tipos MIME comuns (em mozilla.org)
- Tipos de MIME: Lista completa de tipos MIME (em w3cub.com)
- A lista completa de tipos MIME (em site.point.com)