Bloquear carregamento de TXT via DLP no acesso seguro

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Antes de Começar

- Configuration Steps
- Etapa 1. Criar Classificação de Dados
- Etapa 2. Configurar a Política DLP

Monitoramento

- Expressões regulares de exemplo

Informações Relacionadas

Introdução

Este documento descreve as etapas para bloquear o upload de arquivo .TXT no Cisco Secure Access com DLP.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração do Cisco Secure Access.
- Prevenção contra perda de dados (DLP).

A Cisco recomenda que você:

- Acesso administrativo ao Cisco Secure Access.

Componentes Utilizados

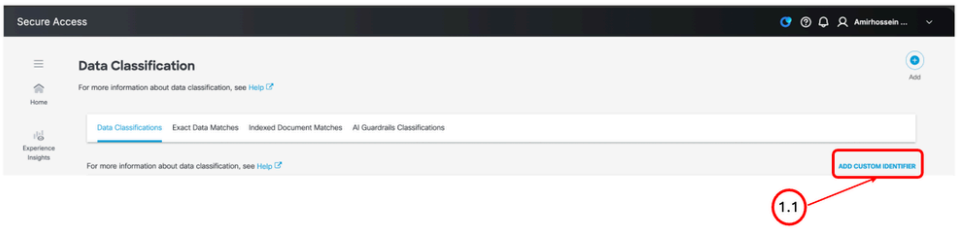
Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Antes de Começar

1. Use essas etapas com cuidado, pois elas adicionam carga extra ao processo PPD e podem causar degradação do desempenho. Até que o bloqueio de arquivos TXT esteja disponível, você pode consultar este link para obter informações sobre os tipos de arquivos atualmente suportados: Cisco Secure Access - Tipos de arquivos suportados
2. Este artigo inclui exemplos de expressões regulares que podem ser usados como referência. Antes de usar qualquer um dos exemplos, certifique-se de que você compreende totalmente as condições de correspondência e os padrões que eles são projetados para identificar. Você também pode criar suas próprias expressões regulares quando necessário. Em todos os casos, valide cuidadosamente a expressão para garantir que ela cobre corretamente todas as condições de correspondência desejadas e possíveis variações.
3. Certifique-se de que o tráfego seja descriptografado antes de aplicar políticas DLP. A inspeção DLP exige acesso ao conteúdo descriptografado; o tráfego criptografado não pode ser verificado para correspondências DLP.

Configuration Steps

Categoria	Etapas
Etapa 1. Criar Classificação de Dados	Etapa 1.1. No portal de gerenciamento do Cisco Secure Access, navegue para Secure > Data Classification e clique em Add Custom Identifier.  Imagem - Criar um novo identificador personalizado Etapa 1.2. Definir um nome para o novo Identificador

Etapa 1.3. Na seção Limite, configure os Critérios de Severidade e clique em Adicionar.

Etapa 1.4. Defina cada expressão regular separadamente e clique em Adicionar.

Dica: as expressões regulares fornecidas neste artigo são apenas exemplos. Antes de usá-los, verifique se a expressão cobre corretamente todas as condições de correspondência necessárias e possíveis variações.

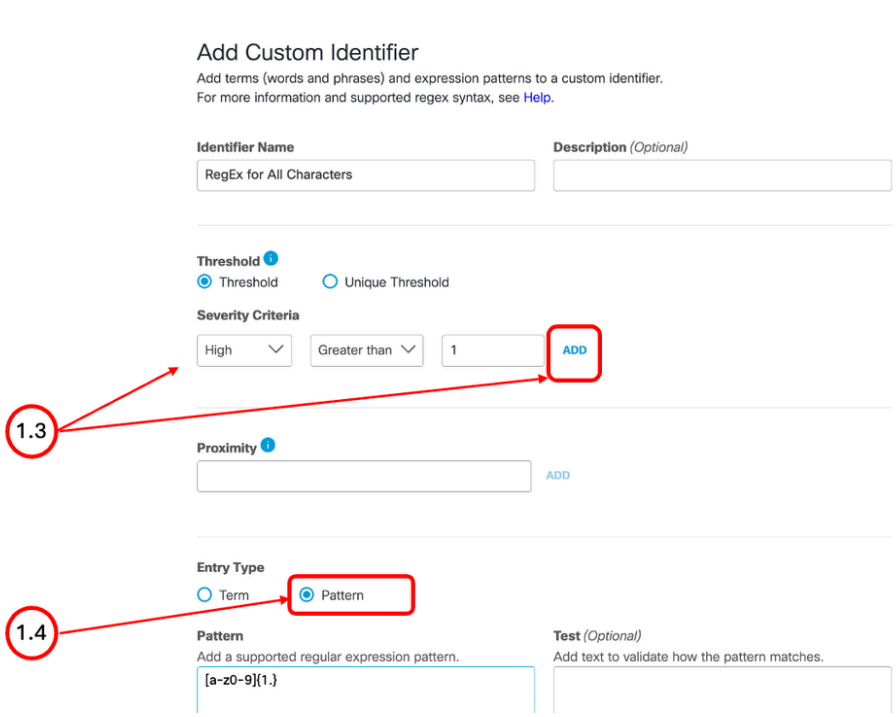


Imagem - Adicionar identificador personalizado

Note: Se houver mais de 10 expressões regulares, você precisará usar as mesmas etapas para criar outro identificador personalizado.

Etapa 1.5. Clique em Salvar.

Etapa 1.6. Clique no ícone Adicionar para criar uma nova Classificação de Dados

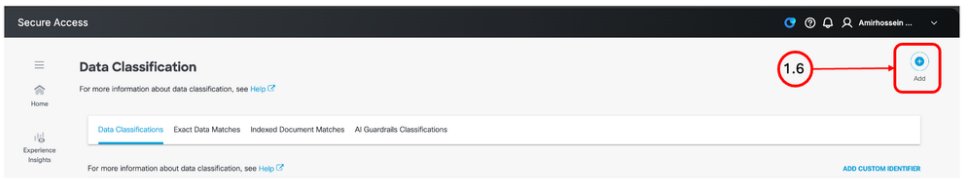
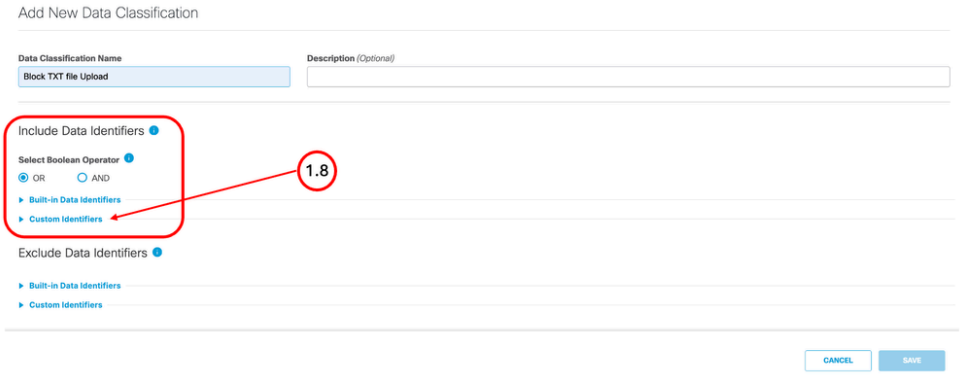
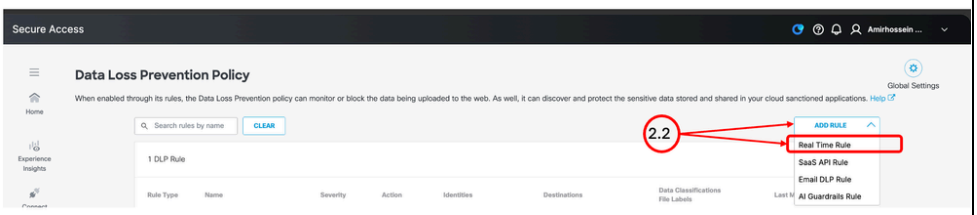


Imagem - Criar uma nova classificação de dados

	Etapa 1.7. Defina um Nome. Etapa 1.8. Na seção Incluir Identificadores de Dados, clique em Identificador Personalizado e escolha o(s) Identificador(es) que você criou nas etapas anteriores.  Imagem - Configurar a classificação de dados Etapa 1.9. Clique em Salvar.
Etapa 2. Configurar a Política DLP	Etapa 2.1. No portal de gerenciamento do Cisco Secure Access, navegue até Secure > Data Loss Prevention Policy Etapa 2.2. Clique em Add Rule e selecione Real Time Rule.  Imagem - Criar uma nova política DLP em tempo real Etapa 2.3. Defina o nome da política. Etapa 2.4. Na seção Classificações de Dados, selecione a Classificação de Dados que você criou na Etapa 1. Note: Aguarde até 5 minutos para que as classificações de dados recém-criadas apareçam na lista de políticas PPD. Etapa 2.5. Na seção Controle de arquivos, ative o Tipo de arquivo e selecione TXT.

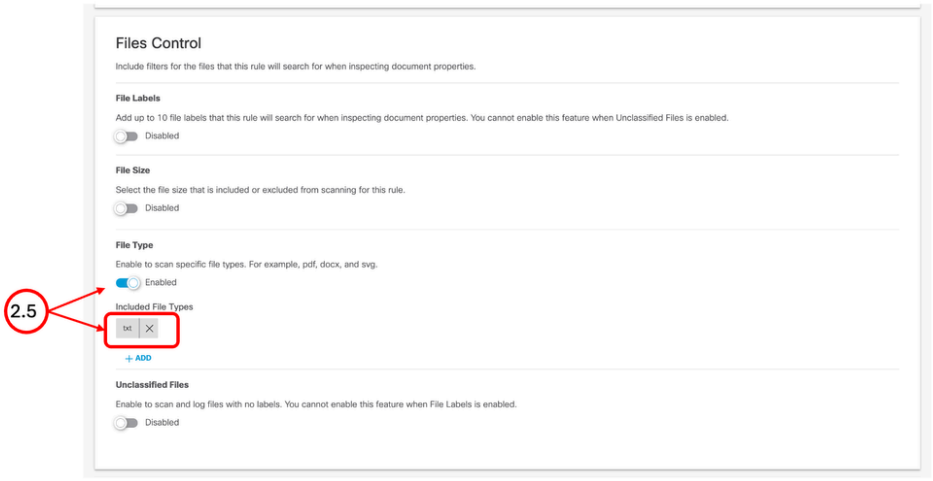


Imagem - Configurar tipo de arquivo

Etapa 2.6. Na seção Action, escolha Block.

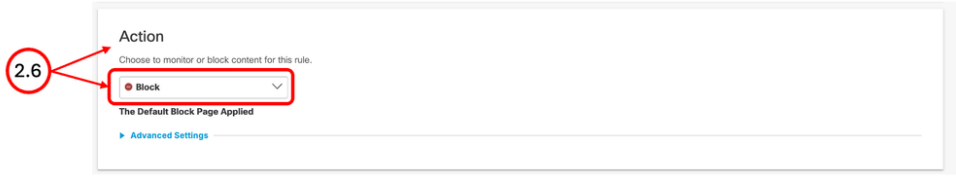


Imagem - Definir a ação como Bloquear

Etapa 2.7. Salve as alterações.

Monitoramento

Para verificar a atividade DLP e os logs relacionados, vá para Monitor > Data Loss Prevention. Use os filtros disponíveis para restringir os resultados e identificar os eventos DLP relevantes.

Expressões regulares de exemplo

Corresponde aos caracteres japoneses Hiragana, Katakana e Kanji:

```
[ぁ-けァ-ヲー-□]{1,}
```

Corresponde às letras maiúsculas do alfabeto latino:

```
[A-Z]{1,}
```

Corresponde a letras minúsculas e dígitos:

```
[a-z0-9]{1,}
```

Corresponde a caracteres de pontuação comuns:

```
[.,;:!?]
```

Corresponde a aspas simples, aspas duplas e backticks:

```
['"`]
```

Corresponde parênteses, colchetes e chaves:

```
[()\[\]{}]
```

Corresponde a símbolos comuns e caracteres especiais:

```
[@#$%^&*+=|\\/_~-]
```

Corresponde a caracteres latinos no intervalo Unicode À-ÿ:

```
[À-ÿ]
```

Corresponde a caracteres cirílicos:

```
[È-ж]
```

Corresponde a caracteres gregos e coptas:

```
[ㅏ-ㅢ]
```

Corresponde a caracteres de script árabe:

```
[-ۿ]
```

Corresponde a Ideogramas Unificados CJK:

```
[丄-□]
```

Corresponde os caracteres poloneses selecionados aos sinais diacríticos:

```
[ĄąĆćĘęŁłŃńÓóŚśŹźŻż]
```

Combina com as sílabas Hangul coreanas:

```
[가-힣]
```

Informações Relacionadas

Lista completa do Cisco Secure Access dos tipos de arquivos suportados pelo DLP: https://securitydocs.cisco.com/docs/csa/olh/120218.dita

Tipos de arquivos suportados pelo Cisco Secure Access DLP — Comunidade Cisco: https://community.cisco.com/t5/security-knowledge-base/cisco-secure-access-complete-list-of-dlp-supported-file-types/ta-p/5274268

Configuração e referência de política do Cisco Secure Access DLP: https://securitydocs.cisco.com/docs/csa/olh/161419.dita

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.