Fase 3 da solução de problemas de caminho de dados do Firepower: Inteligência de segurança

Contents

[Introduction](#)
[Prerequisites](#)
[Solução de problemas da fase de inteligência de segurança do Firepower](#)
[Determine se o registro está ativado para eventos de inteligência de segurança](#)
[Revisar os eventos de inteligência de segurança](#)
[Como remover as configurações de inteligência de segurança](#)
[Verifique a configuração no back-end](#)
[Dados a fornecer ao TAC](#)
[Próxima etapa](#)

Introduction

Este artigo faz parte de uma série de artigos que explicam como solucionar problemas sistematicamente no caminho de dados em sistemas Firepower para determinar se os componentes do Firepower podem estar afetando o tráfego. Consulte o artigo Visão geral para obter informações sobre a arquitetura das plataformas Firepower e links para outros artigos de solução de problemas de caminho de dados.

Este artigo abrange o terceiro estágio da solução de problemas de caminho de dados do Firepower, o recurso de inteligência de segurança.

Prerequisites

- Este artigo se refere a todas as plataformas Firepower suportadas atualmente
- A inteligência de segurança para URLs e DNS foi apresentada na versão 6.0.0

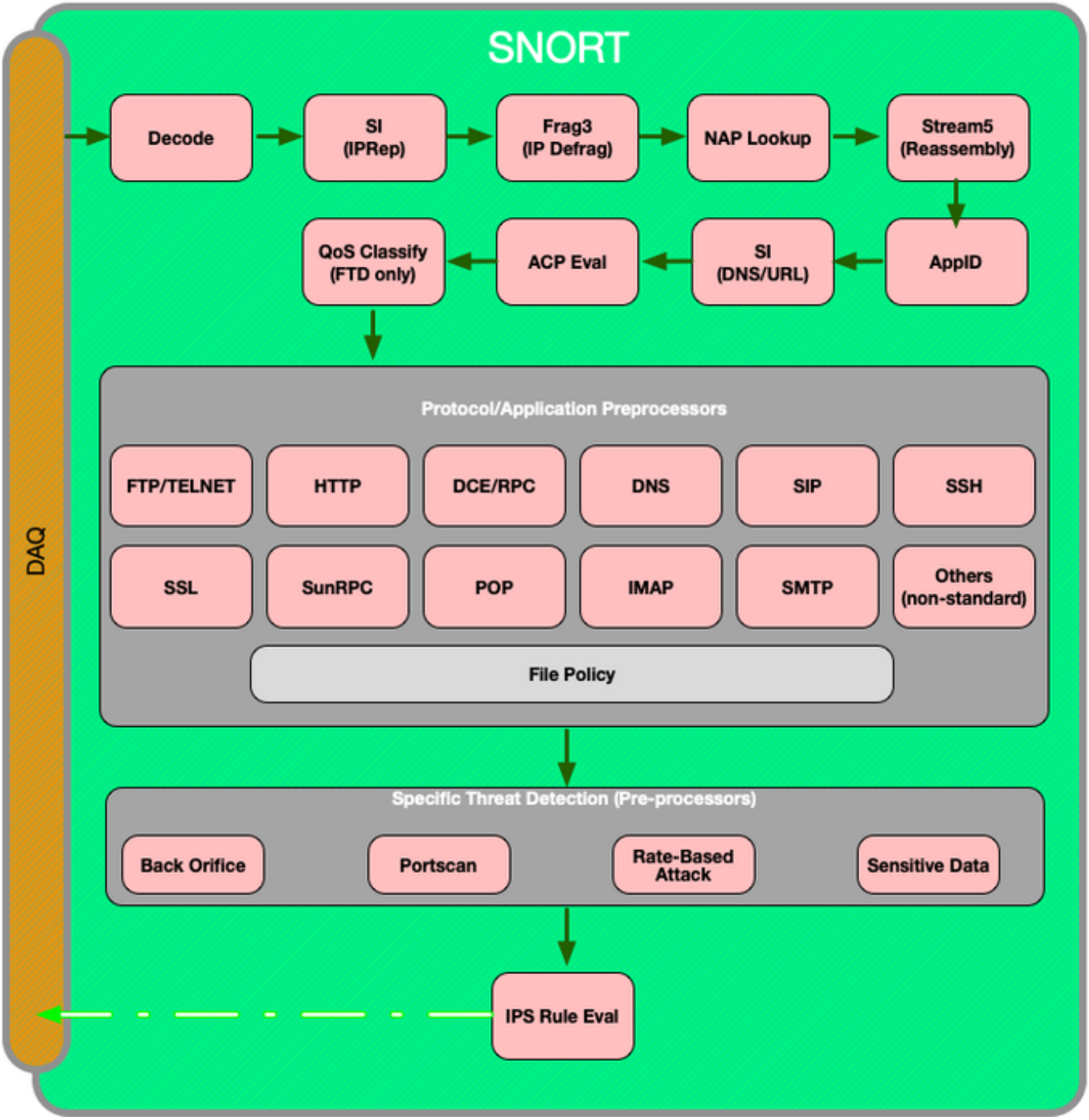
Solução de problemas da fase de inteligência de segurança do Firepower

A inteligência de segurança é um recurso que realiza a inspeção contra listas negras e listas brancas para:

- Endereços IP (também conhecidos como "Redes" em certas partes da IU)
- URLs (Uniform Resource Locators, localizadores de recursos uniformes)
- Consultas do Domain Name System (DNS)

As listas na Inteligência de segurança podem ser preenchidas por feeds fornecidos pela Cisco e/ou listas e feeds configurados pelo usuário.

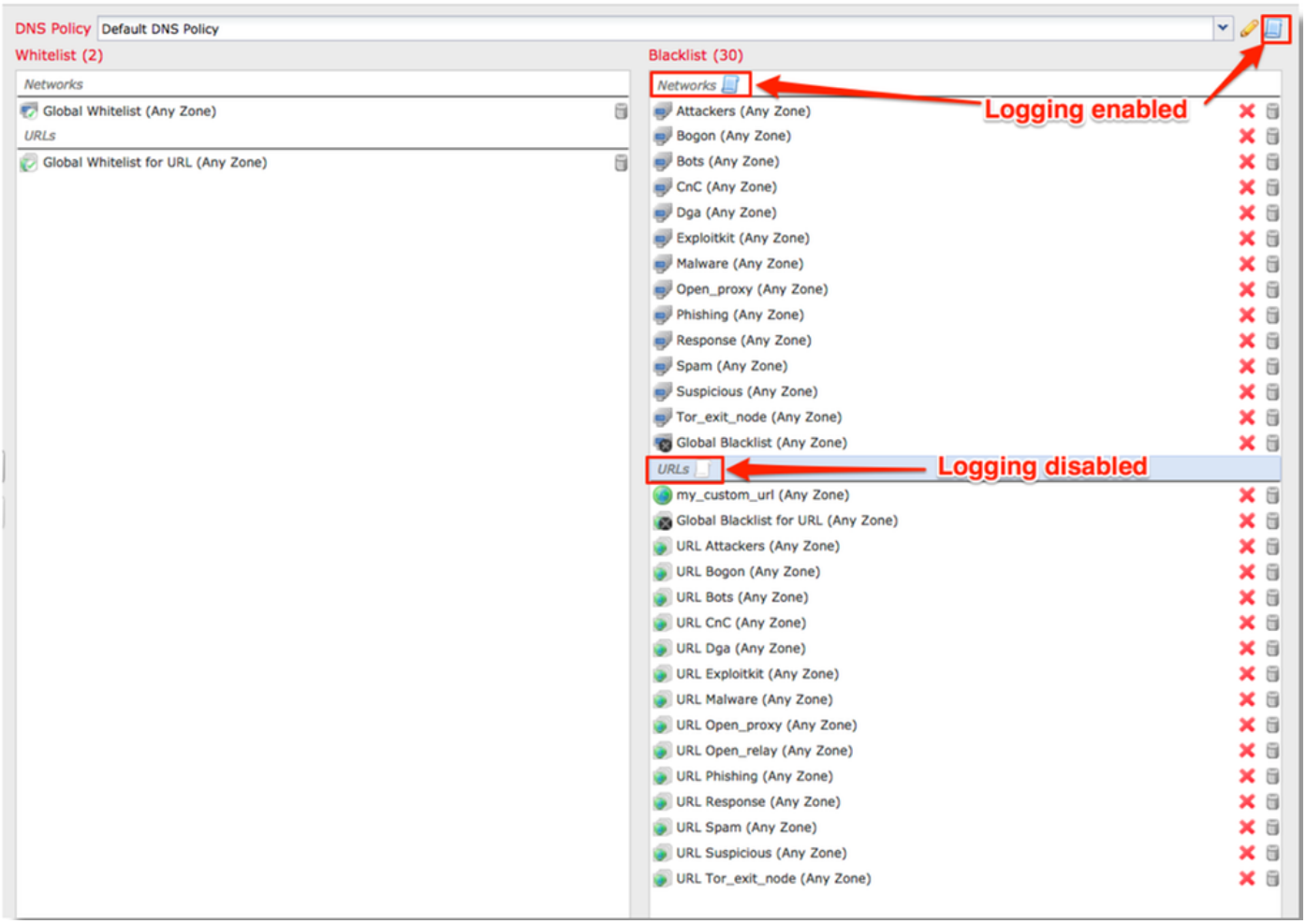
A reputação da Security Intelligence baseada em endereços IP é o primeiro componente do Firepower a inspecionar o tráfego. A inteligência de segurança de URL e DNS é executada assim que o protocolo de aplicação relevante é descoberto. Abaixo está um diagrama que descreve o fluxo de trabalho de inspeção do software Firepower.



Determine se o registro está ativado para eventos de inteligência

de segurança

Blocos no nível Security Intelligence são muito fáceis de determinar, desde que o registro esteja ativado. Isso pode ser determinado na Interface de Usuário (IU) do Firepower Management Center (FMC) navegando até **Políticas > Controle de Acesso > Política de Controle de Acesso**. Depois de clicar no ícone de edição ao lado da política em questão, navegue até a guia **Security Intelligence**.



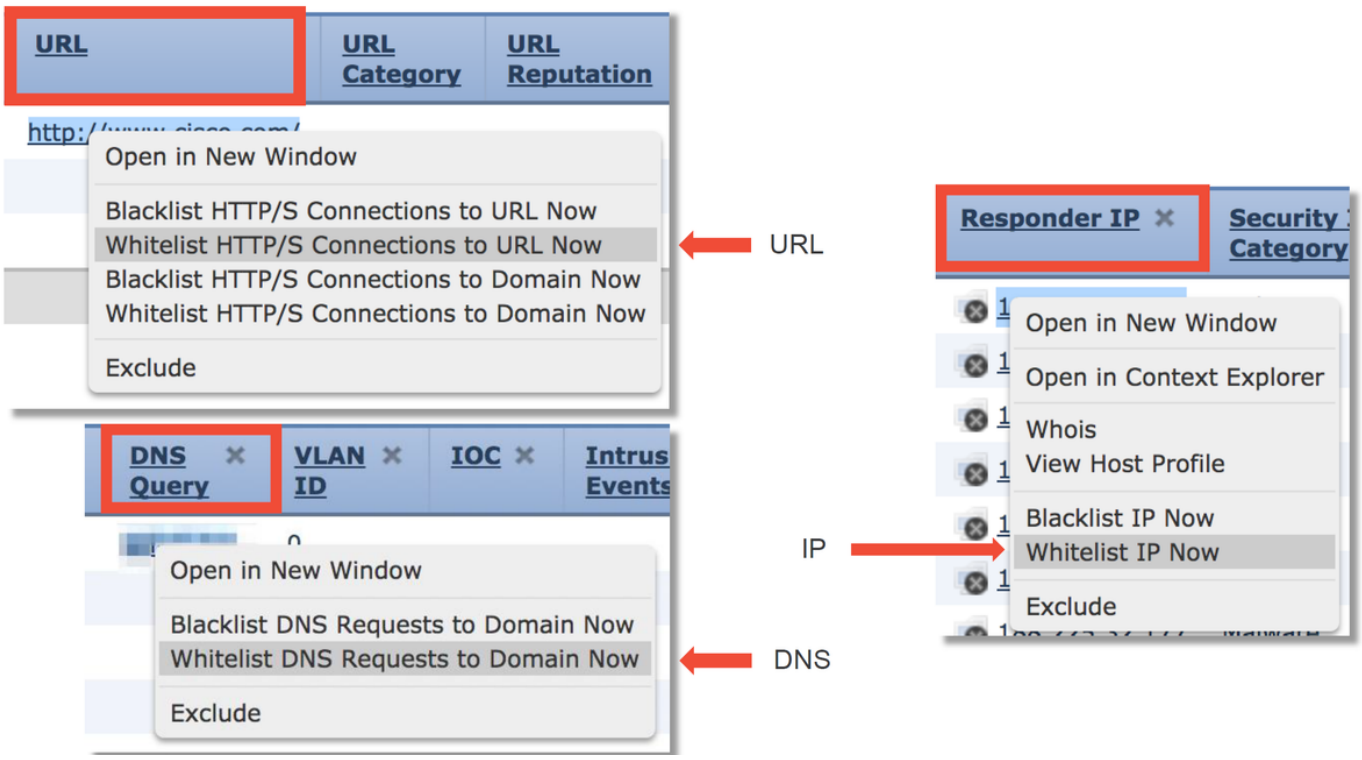
Revisar os eventos de inteligência de segurança

Quando o registro estiver ativado, você poderá visualizar os Eventos de Inteligência de Segurança em **Analysis > Connections > Security Intelligence Events**. Deve ficar claro por que o tráfego está sendo bloqueado.

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

Como uma rápida etapa de mitigação, você pode clicar com o botão direito do mouse na Consulta

IP, URL ou DNS sendo bloqueada pelo recurso Security Intelligence e escolher uma opção de lista branca.



Se você suspeitar que algo foi colocado incorretamente na lista negra, ou se quiser solicitar que você altere a reputação, poderá abrir um tíquete diretamente com o Cisco Talos no link a seguir:

https://www.talosintelligence.com/reputation_center/support

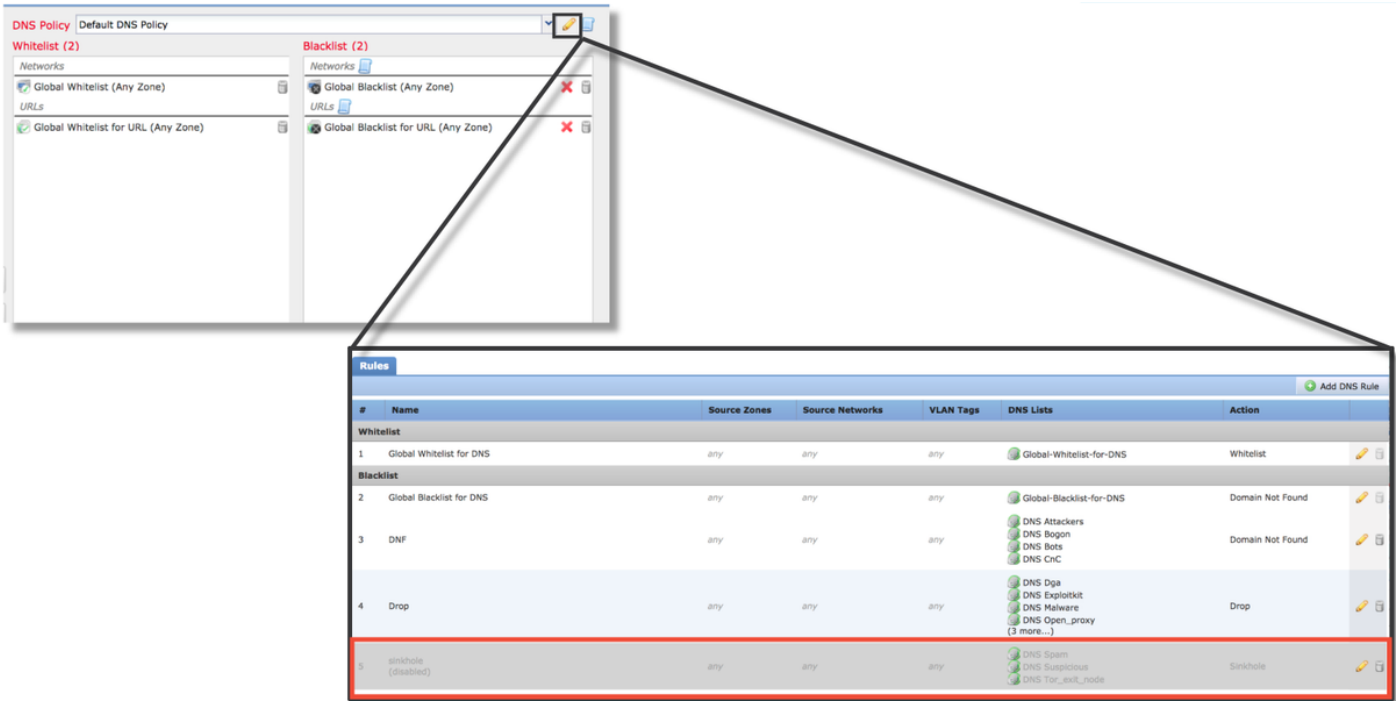
Você também pode fornecer os dados ao Cisco Technical Assistance Center (TAC) para investigar se um item deve ser removido da lista negra.

> **Note:** Adicionar à lista branca apenas adiciona uma entrada à lista branca de inteligência de segurança em questão, o que significa que o objeto tem permissão para passar a verificação de inteligência de segurança. No entanto, todos os outros componentes do Firepower ainda podem inspecionar o tráfego.

Como remover as configurações de inteligência de segurança

Para remover as configurações de inteligência de segurança, navegue até a guia **Inteligência de segurança**, conforme mencionado acima. Há três seções: um para redes, URL e uma política para DNS.

A partir daí, as listas e os feeds podem ser removidos clicando no símbolo da lixeira.



Observe na captura de tela acima que todas as listas de inteligência de segurança de IP e URL foram removidas, exceto a lista negra global e a lista branca.

Na Política DNS, que é onde a configuração de inteligência de segurança DNS é armazenada, uma das regras é desabilitada.

> **Note**: Para visualizar o conteúdo das listas negras globais e das listas brancas, navegue para **Objetos > Gerenciamento de objetos > Inteligência de segurança**. Em seguida, clique na seção de interesse (Rede, URL, DNS). A edição de uma lista exibirá o conteúdo, embora a configuração deva ser executada na Política de controle de acesso.

Verifique a configuração no back-end

A configuração do Security Intelligence pode ser verificada na CLI por meio do comando **> show access-control-config**, que mostra o conteúdo da política de controle de acesso ativa em execução no dispositivo Firepower.

```
> show access-control-config

==================[ My AC Policy ]==================
Description              :
Default Action            : Allow
Default Policy            : SOC
Logging Configuration
   DC                   : Enabled
   Beginning             : Disabled
   End                  : Enabled
Rule Hits                 : 0
Variable Set              : Default-Set

===[ Security Intelligence - Network Whitelist ]====
   Name                 : Global-Whitelist (List)
   IP Count             : 0
   Zone                 : any

===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Enabled
   DC                   : Enabled


--------------------[ Block ]---------------------
   Name                 : Attackers (Feed)
   Zone                 : any

   Name                 : Bogon (Feed)
   Zone                 : any
…[omitted for brevity]
```

Observe no exemplo acima que o registro está configurado para a lista negra da rede e pelo menos dois feeds foram incluídos na lista negra (Invasores e Bogon).

Se um item individual está em uma lista de inteligência de segurança pode ser determinado no modo de especialista. Veja as etapas abaixo:

```
> expert
$ grep <ip.addr> /var/sf/iprep_download/*
/var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf:<ip.addr>

$ head -1 /var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf
#Cisco intelligence feed: Malware



$ grep <url> /var/sf/siurl_download/*
/var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf:<url>

$ head -1 /var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf
#URL object: my_custom_url



$ grep <dns.hostname> /var/sf/sidns_download/*
/var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf: <dns.hostname>

$ head -1 /var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf
#Cisco DNS and URL intelligence feed: DNS Response
```

IP SI lists are in /var/sf/iprep_download/

URL SI lists are in /var/sf/siurl_download/

DNS SI lists are in /var/sf/sidns_download/

Há um arquivo para cada lista de inteligência de segurança com um UUID exclusivo. O exemplo

acima mostra como identificar o nome da lista, usando o comando **head -n1**.

Dados a fornecer ao TAC

Dados	Instruções
Solucionar problemas de arquivos do FMC e do dispositivo Firepower inspecionando o tráfego	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-tecl
Capturas de tela de eventos (com marcadores de data e hora incluídos)	Consulte este artigo para obter instruções
Saída de texto de sessões CLI	Consulte este artigo para obter instruções
Se estiver enviando um caso falso positivo, forneça o item (IP, URL, domínio) a ser contestado.	Indicar as razões e os elementos que justificam a realização do litígio.

Próxima etapa

Se for determinado que o componente Security Intelligence não é a causa do problema, a próxima etapa será solucionar os problemas das regras da política de controle de acesso.

Clique aqui para continuar com o próximo artigo.