Fase 4 de solução de problemas de caminho de dados do Firepower: Política de controle de acesso

Contents

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 quarto estágio da solução de problemas de caminho de dados do Firepower, a Política de Controle de Acesso (ACP - Access Control Policy). Essas informações se aplicam a todas as plataformas e versões do Firepower suportadas atualmente.

Troubleshooting da Fase de Política de Controle de Acesso (ACP)

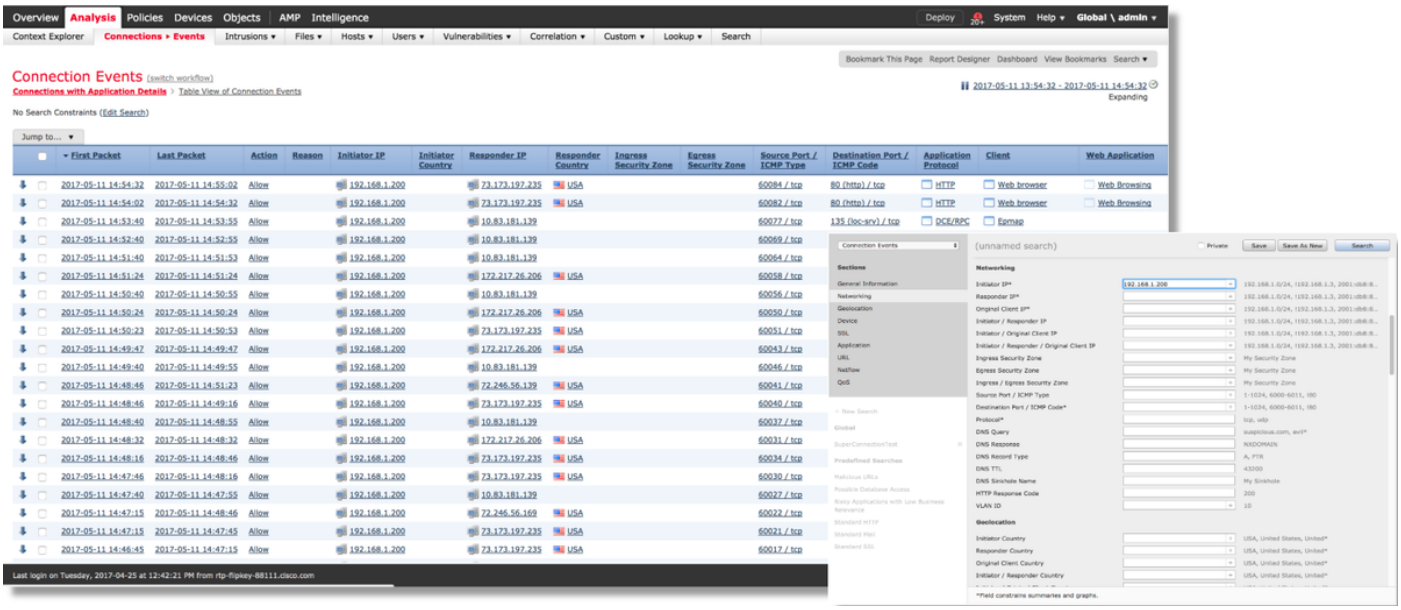
Em termos gerais, determinar qual regra ACP um fluxo corresponde deve ser bastante direta. Os eventos de conexão podem ser revisados para ver qual regra/ação está sendo aplicada. Se isso não mostrar claramente o que o ACP está fazendo com o tráfego, a depuração pode ser executada na CLI (Command Line Interface, interface de linha de comando) do Firepower.

Verificar eventos de conexão

Depois de obter uma ideia da interface de entrada e saída, o tráfego deve corresponder, bem

como as informações de fluxo, o primeiro passo para identificar se o Firepower está bloqueando o fluxo seria verificar os Eventos de Conexão para o tráfego em questão. Eles podem ser vistos no Firepower Management Center em **Analysis > Connections > Events.**

> **Note**: Antes de verificar Eventos de conexão, verifique se o registro está habilitado em suas regras ACP. O registro é configurado na guia "Registro" em cada regra da política de controle de acesso, bem como na guia Inteligência de segurança. Verifique se as regras suspeitas estão configuradas para enviar os registros para o "Visualizador de Eventos". Isso também se aplica à ação padrão.



Ao clicar em "Editar pesquisa" e filtrado por um IP de origem (iniciador) exclusivo, você pode ver os fluxos que estavam sendo detectados pelo Firepower. A coluna Ação mostra "Permitir" para o tráfego deste host.

Se o Firepower estiver bloqueando intencionalmente o tráfego, a Ação conterá a palavra "Bloquear". Clicar em "Table View of Connection Events" fornece mais dados. Os seguintes campos nos Eventos de Conexão podem ser revisados se a ação for "Bloquear":

-Razão

- Regra de controle de acesso

Etapas de mitigação rápida

A fim de atenuar rapidamente um problema que se acredita ser causado pelas regras ACP, pode-se realizar o seguinte:

- Crie uma regra com a ação de "Confiar" ou "Permitir" para o tráfego em questão e coloque-a no topo do ACP ou, acima de tudo, regras de bloqueio.
- Desative temporariamente quaisquer regras com uma ação que contenha a palavra "Bloquear"
- Se a ação padrão estiver definida como "Bloquear todo o tráfego", mude temporariamente para "Somente descoberta de rede"

Note: Essas atenuações rápidas exigem alterações de política que podem não ser possíveis em todos os ambientes. Recomenda-se primeiro tentar usar o rastreamento de suporte do sistema para determinar qual regra o tráfego corresponde antes de fazer alterações de política.

Depurando o ACP

Mais solução de problemas pode ser executada em relação às operações ACP através do **> utilitário CLI de suporte de firewall-engine-debug**.

Note: Nas plataformas Firepower 9300 e 4100, o shell em questão pode ser acessado por meio dos seguintes comandos:

 # conectar o módulo 1
Firepower-module1**> connect ftd**
>

Para várias instâncias, a CLI do dispositivo lógico pode ser acessada com os seguintes comandos.
 # connect module 1 telnet
Firepower-module1**> conectar ftd ftd1**
Conectando ao console do contêiner ftd(ftd1)... digite "exit" para voltar à CLI de inicialização
>

O utilitário **firewall-engine-debug do sistema** tem uma entrada para cada pacote que está sendo avaliado pelo ACP. Mostra o processo de avaliação de regra que está ocorrendo, juntamente com o motivo pelo qual uma regra é correspondida ou não.

Note: Na versão 6.2 e superior, a ferramenta **de rastreamento de suporte do sistema** pode ser executada. Ele usa os mesmos parâmetros, mas inclui mais detalhes. Certifique-se de inserir 'y' quando solicitado com "**Enable firewall-engine-debug too?"**.

Exemplo 1: O tráfego corresponde a uma regra de confiança

No exemplo abaixo, o estabelecimento de uma sessão SSH é avaliado usando o **suporte do sistema firewall-engine-debug**.

Este é o ACP que está sendo executado no dispositivo Firepower.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Acti...
Mandatory - JG AC (all) (1-6)													
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	SSH	Any	Any	Trust
2	inspect	Any	Any	10.0.0.0/8	Any	Any	Any	Any	Any	Any	Any	Any	Allow
3	trust server backup	Any	Any	192.168.62.3	10.123.175.22	Any	Any	Any	Any	Any	Any	Any	Trust

O ACP tem três regras.

1. A primeira regra é confiar em qualquer tráfego de 192.168.0.7 com portas de destino usadas

pelo SSH.

2. A segunda regra inspeciona todo o tráfego originado de 10.0.0.0/8 no qual os critérios de rede correspondem com base nos dados do cabeçalho XFF (conforme indicado pelo ícone ao lado do objeto de rede)
3. A terceira regra confia em todo o tráfego de 192.168.62.3 a 10.123.175.22

No cenário de solução de problemas, uma conexão SSH de 192.168.62.3 a 10.123.175.22 está sendo analisada.

A expectativa é que a sessão corresponda à regra 3 de AC "backup de servidor confiável". A questão é, quantos pacotes deve ser necessário para que esta sessão corresponda a esta regra. Todas as informações necessárias no primeiro pacote para determinar a regra CA ou vários pacotes são necessários e, se for esse o caso, quantas?

Na CLI do Firepower, é inserido o seguinte para ver qual processo de avaliação de regras ACP.

```
>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages
```

> **Tip**: É melhor preencher o máximo possível de parâmetros ao executar o **firewall-engine-debug**, para que somente as mensagens de depuração interessantes sejam impressas na tela.

Na saída de depuração abaixo, você vê os quatro primeiros pacotes da sessão sendo avaliados.

SYN

SYN,ACK

ACK

Primeiro pacote SSH (cliente para servidor)

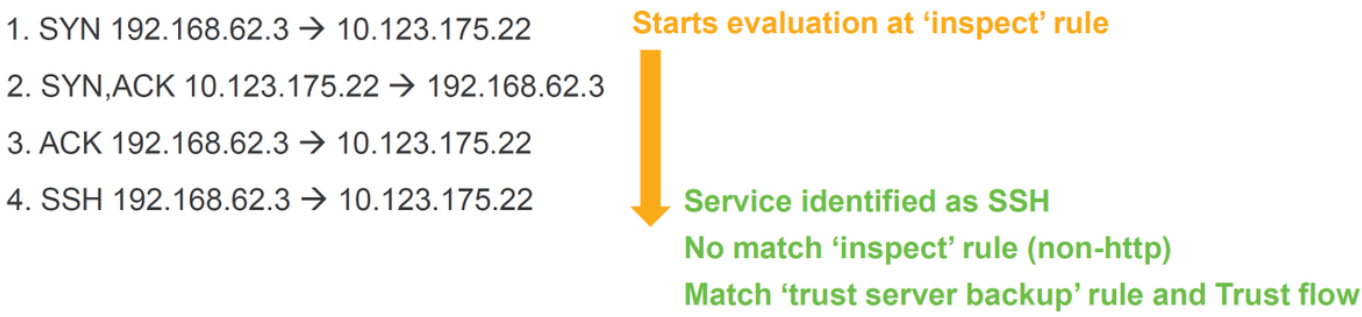
```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

Este é um gráfico que ilustra a lógica de depuração.



Para esse fluxo, são necessários 4 pacotes para que o dispositivo corresponda à regra.

Esta é uma explicação detalhada da saída de depuração.

- O processo de avaliação ACP inicia na regra "inspecionar" porque a regra "confiar no host" não foi correspondida, pois o endereço IP não correspondia ao requisito. Essa é uma correspondência rápida devido a todas as informações necessárias para determinar se essa regra deve corresponder está presente no primeiro pacote (IPs e portas)
- Não é possível determinar se o tráfego corresponde à regra "inspecionar" até que o aplicativo seja identificado, uma vez que as informações X-Forwarded-For (XFF) são encontradas no tráfego do aplicativo HTTP, o aplicativo ainda não é conhecido, portanto isso coloca a sessão em um estado pendente para a regra 2, dados pendentes do aplicativo.
- Quando o aplicativo é identificado no quarto pacote, a regra "inspecionar" resulta em uma não correspondência, já que o aplicativo é SSH, em vez de HTTP
- A regra de "backup de servidor confiável" é então combinada, com base nos endereços IP.

Em resumo, a conexão leva 4 pacotes para corresponder à sessão, pois precisa esperar que o firewall identifique o aplicativo, já que a regra 2 tem uma restrição de aplicativo nele.

Se a regra 2 tivesse apenas redes de origem e não fosse XFF, então teria levado 1 pacote para corresponder à sessão.

Você deve sempre colocar as regras das camadas 1 a 4 acima de todas as outras regras na política quando possível, pois essas regras normalmente exigem um pacote para tomar uma decisão. No entanto, você também pode observar que mesmo com regras das camadas 1 a 4, pode haver mais de um pacote para corresponder a uma regra de CA, e o motivo para isso é a inteligência de segurança de URL/DNS. Se você tiver uma dessas ativações, o firewall precisará determinar o aplicativo para todas as sessões que estão sendo avaliadas pela política AC, pois ele precisa determinar se são HTTP ou DNS. Em seguida, ele deve determinar se deve permitir a sessão com base nas listas negras.

Abaixo está uma saída truncada do comando **firewall-engine-debug**, que tem os campos relevantes destacados em vermelho. Observe o comando usado para obter o nome do aplicativo identificado.

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

[…omitted for brevity]

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust


[! How to map service/application ID to name]
> expert
$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh
```

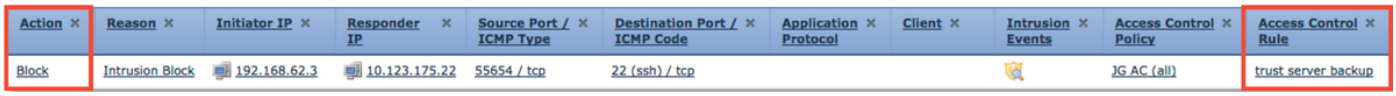
Exemplo 2: O tráfego correspondente a uma regra de confiança está bloqueado

Em alguns cenários, o tráfego pode ser bloqueado apesar de corresponder a uma regra de Confiança no ACP. O exemplo abaixo avalia o tráfego com a mesma política de controle de acesso e hosts.

```
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blacklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline
sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user 9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```



Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Intrusion Events	Access Control Policy	Access Control Rule
Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp				JG AC (all)	trust server backup

Como visto acima, a saída **firewall-engine-debug** mostra que o tráfego corresponde a uma "Confiança", enquanto os Eventos de Conexão mostram a ação de **Bloquear** devido a uma regra de Política de Intrusão (determinada porque a coluna Razão mostra **Bloco de Intrusão**).

A razão pela qual isso pode ocorrer é devido à **Política de intrusão usada antes que a regra de controle de acesso seja determinada** Configuração na guia **Avançado** no ACP. Antes que o tráfego possa ser confiável de acordo com a ação da regra, a Política de intrusão em questão identifica uma correspondência de padrão e descarta o tráfego. No entanto, a avaliação de regra ACP resulta em uma correspondência da regra de Confiança, já que os endereços IP correspondem aos critérios da regra de "backup do servidor de confiança".

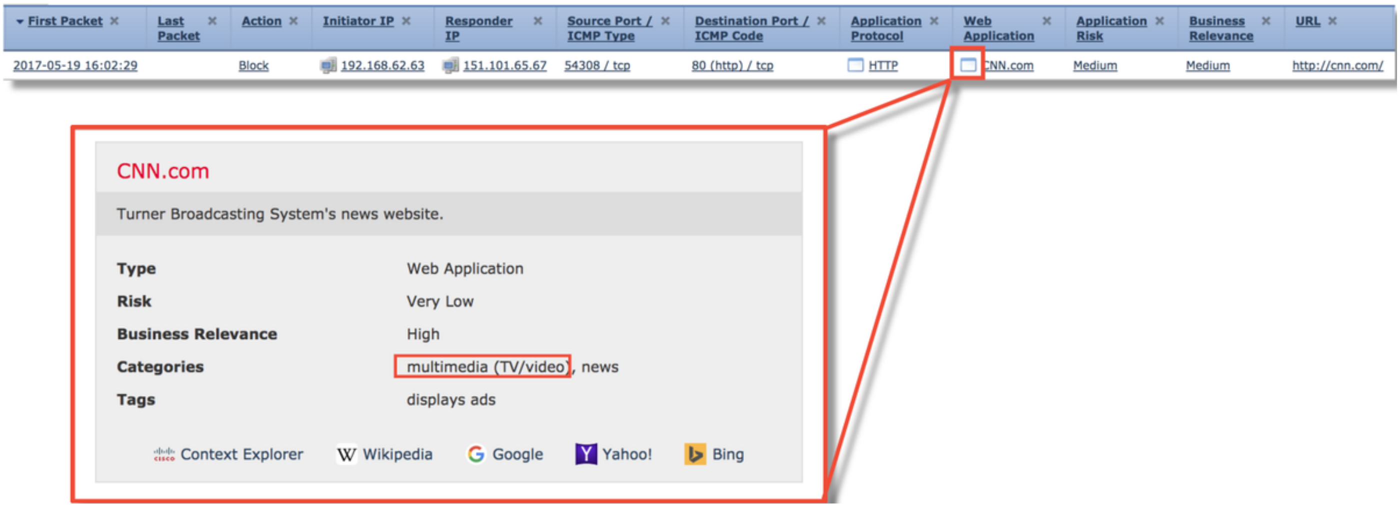
Para que o tráfego não seja submetido à inspeção da política de intrusão, a regra Trust pode ser colocada acima da regra "inspect" (inspecionar), o que seria uma prática recomendada em ambos os casos. Como a identificação do aplicativo é necessária para uma correspondência e não correspondência da regra de "inspeção", a **Política de intrusão usada antes que a regra de controle de acesso seja determinada** é usada para o tráfego que é avaliado pelo mesmo. Colocar a regra de "backup do servidor de confiança" acima da regra de "inspeção" faz com que o tráfego corresponda à regra quando o primeiro pacote é visto, pois a regra é baseada no endereço IP, que pode ser determinado no primeiro pacote. Portanto, a **Política de intrusão usada antes que a**

regra de Controle de Acesso seja determinada não precisa ser usada.

Cenário 3: Tráfego bloqueado pela etiqueta do aplicativo

Neste cenário, os usuários relatam que cnn.com está sendo bloqueado. No entanto, não há uma regra específica que bloqueie a CNN. Os Eventos de Conexão, juntamente com a saída **firewall-engine-debug**, mostram o motivo do bloqueio.

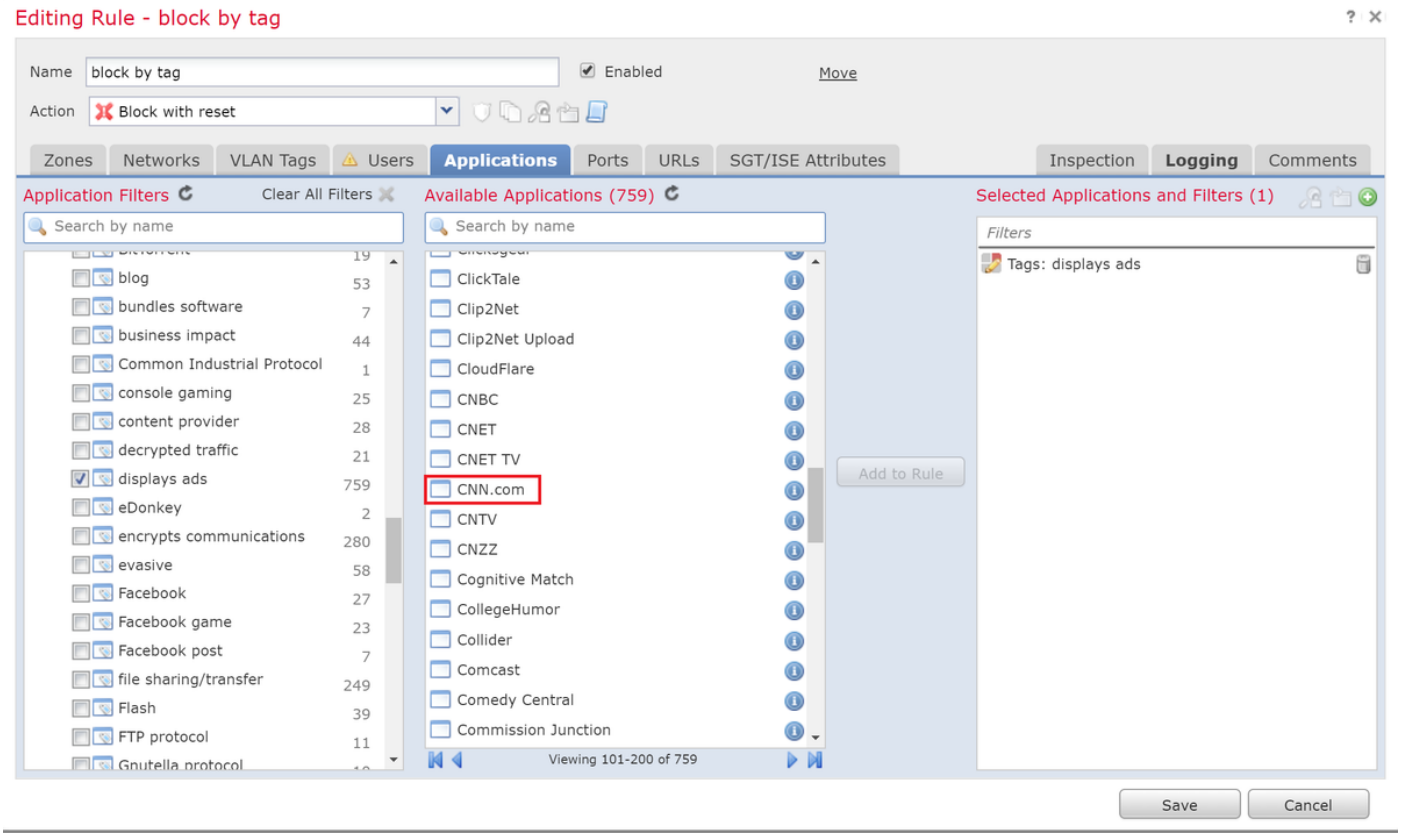
Primeiro, os Eventos de Conexão têm uma caixa de informações ao lado dos campos do aplicativo que mostra informações sobre o aplicativo, bem como como o Firepower categoriza esse aplicativo.



Com essas informações em mente, **firewall-engine-debug** é executado. Na saída de depuração, o tráfego é bloqueado com base na etiqueta de aplicativo.

```
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session
```

Embora não haja uma regra que bloqueasse explicitamente http://cnn.com, os **anúncios exibidos** marcados estão sendo bloqueados na guia **Aplicativos** de uma regra ACP.



Dados a fornecer ao TAC

Dados	Instruções
Solucionar problemas do dispositivo Firepower que inspeciona o tráfego	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/1176
sistema suporta firewall-engine-debug e **system-support-trace** output	Consulte este artigo para obter instruções
Exportação da política de controle de acesso	Navegue até **Sistema > Ferramentas > Importar/Exportar**, selecione a Política de C botão **Exportar**

> **Caution**: Se o ACP contiver uma política SSL, remova a política SSL do ACP antes de exportar para evitar a divulgação de informações confidenciais de PKI

Próxima etapa: Solucionar problemas da camada de política SSL

Se uma política SSL estiver em uso e a solução de problemas da política de controle de acesso não revelar o problema, a próxima etapa será solucionar o problema da política SSL.