# Firepower Data Path Problemen opsporen en verhelpen fase 4: Toegangsbeheerbeleid

## Inhoud

Inleiding Probleemoplossing voor de fase van het toegangscontrolebeleid (ACS) Op aansluitingen controleren Snelle beperking Ontduiking van de ACS-landen Voorbeeld 1: Verkeer komt overeen met een vertrouwensregel Voorbeeld 2: Verkeersovereenstemming met een vertrouwensregel is geblokkeerd Scenario 3: Verkeer geblokkeerd door toepassingslabel Gegevens om te leveren aan TAC Volgende stap: Probleemoplossing voor de SSL-beleidslaag

## Inleiding

Dit artikel maakt deel uit van een reeks artikelen waarin wordt uitgelegd hoe u het gegevenspad op FirePOWER-systemen systematisch moet oplossen om te bepalen of onderdelen van Firepower invloed kunnen hebben op het verkeer. Raadpleeg het <u>gedeelte Overzicht</u> voor informatie over de architectuur van FirePOWER-platforms en de koppelingen naar de andere artikelen voor probleemoplossing in datacenters.

Dit artikel heeft betrekking op de vierde fase van de oplossing voor het FirePOWER-gegevenspad, het Access Control Policy (ACS). Deze informatie is van toepassing op alle momenteel ondersteunde FirePOWER-platforms en -versies.



## Probleemoplossing voor de fase van het toegangscontrolebeleid (ACS)

In het algemeen moet het vaststellen van welke ACS-regel een stroming op elkaar afgestemd wordt, vrij rechtuit zijn. De verbindingsgebeurtenissen kunnen worden herzien om te zien welke regel/actie wordt afgedwongen. Als dat niet duidelijk aantoont wat de ACS met het verkeer doet, kan het debuggen worden uitgevoerd op de Firepower Opdracht Line Interface (CLI).

## Op aansluitingen controleren

Na het krijgen van een idee van de ingang en de spanning interface zou het verkeer zowel als de stroominformatie bij elkaar moeten passen, zou de eerste stap om te identificeren of Firepower de stroom blokkeert zijn om de verbindingsgebeurtenissen voor het betrokken verkeer te controleren.

## U kunt deze informatie in het FireSIGHT Management Center bekijken onder **Analyse > Connecties > Evenementen.**

Opmerking: Voordat u de verbindingsgebeurtenissen controleert, moet u ervoor zorgen dat houtkap is ingeschakeld in uw ACS-regels. Vastlegging is ingesteld in het tabblad "Vastlegging" binnen elke regel van het toegangsbeleid en in het tabblad Security Intelligence. Zorg ervoor dat de verdachte regels zijn ingesteld om de logbestanden naar het "Event Viewer" te sturen. Dit is ook van toepassing op de standaardinstelling.

Ov Cor	erview itext E	Analysis Polic	cles Devices Objectes Devices Intro	ects   # usions •	AMP Inte Files ▼	Hosts V User	s • Vuin	erabilities • Corr	elation •	Custom • Loo	kup • Search			Deploy	👷 System Help 🕶 G	ilobal \	admin +			
Bookmark This Page. Report Designer: Dashboard View Bookmarks. Search •																				
Connection Events (wetch workdow)																				
Connections with Application Details > Table View of Connection Events Expansion																				
No Search Constraints (( <u>dd Search</u> )																				
3	Jump to •																			
		+ First Packet	Last Packet	Action	Reason	Initiator IP	Initiator	Responder IP	Responder	Ingress	Egress	Source Port /	Destination Port /	Application	Client	Web A	plication			
	<u> </u>			000000			Country		Country	Security Zone	Security Zone	ICMP Type	ICMP Code	Protocol						
- 4		2017-05-11 14:54:32	2017-05-11 14:55:02	Allow		192.168.1.200		73.173.197.235	JUSA			60084 / tcp	80 (http) / tcp	HTTP HTTP	Web browser	Web	Browsing			
-8		2017-05-11 14:54:02	2017-05-11 14:54:32	Allow		192.168.1.200		<b>173.173.197.235</b>	SA USA			60082 / tcp	80 (http) / tcp	HTTP :	Web browser	Web	Browsing			
- 4		2017-05-11 14:53:40	2017-05-11 14:53:55	Allow		192.168.1.200		10.83.181.139				60077 / tcp	135 (loc-srv) / tcp	DCE/RPC	Epmap					
-8		2017-05-11 14:52:40	2017-05-11 14:52:55	Allow		192.168.1.200		10.83.181.139				60069 / tcp	Connection Events		(unnamed search)			Private	Save Save As	New Search
4		2017-05-11 14:51:40	2017-05-11 14:51:53	Allow		192.168.1.200		10.83.181.139				60064 / tcp								
4		2017-05-11 14:51:24	2017-05-11 14:51:24	Allow		192.168.1.200		172.217.26.206	USA			60058 / tcp	Sections		Networking					
4		2017-05-11 14:50:40	2017-05-11 14:50:55	Allow		192.168.1.200		10.83.181.139				60056 / tcp	Networking		Initiator IP* Responder IP*		192.168.1.200	-	192.168.1.0/24, 1192	.168.1.3, 2001:db8:8
		2017-05-11 14:50:24	2017-05-11 14:50:24	Allow		192,168,1,200		172.217.26.206	III USA			60050 / tro	Geolocation		Original Client 3P*				192.168.1.0/24, 1192	1168.1.3, 2001:db8:8
		2012 05 11 14 50-22	2012 05 11 14-50-52	Allens		102 168 1 200						60051 / http	Device		Initiator / Responder IP				192.168.1.0/24, 1192	.168.1.3, 2001:088.8
		2017-05-11 14:50:23	2017-05-11 14:50:53	Allow		192.168.1.200		13.173.197.235	<u> </u>			600517 tcp	SSL.		Initiator / Original Client IP				192.168.1.0/24, 1192	168.1.3, 2001:058:8
-		2017-05-11 14:49:47	2017-05-11 14:49:47	Allow		······································		H 172.217.26.206	SA USA			60043 / tcp	URL		Increas Security Zone				My Security Zone	108.1.3, 2001.008.8.
- 4		2017-05-11 14:49:40	2017-05-11 14:49:55	Allow		192.168.1.200		10.83.181.139				60046 / tcp	Netflow		Egress Security Zone				My Security Zone	
4		2017-05-11 14:48:46	2017-05-11 14:51:23	Allow		192.168.1.200		72.246.56.139	USA USA			60041 / tcp	QoS		Ingress / Egress Security Zone				My Security Zone	
4		2017-05-11 14:48:46	2017-05-11 14:49:16	Allow		192.168.1.200		73.173.197.235	USA USA			60040 / tcp		_	Source Port / ICMP Type				1-1024, 6000-6011, 1	60
4		2017-05-11 14:48:40	2017-05-11 14:48:55	Allow		192,168,1,200		10.83.181.139				60037 / tcp			Protocol*				tcp, udp	
		2012.05.11.14.49.22	2012 05 11 14 49 22	Aller								60031 ( here	Global		DNS Query				suspicious.com, evil*	
		2017-05-11 14:48:32	2017-05-11 14:48:32	ALIOW		192.168.1.200		172.217.26.206	<u> </u>			600317 tcp	SuperConnectionTest		DNS Response				INKDOMAIN	
		2017-05-11 14:48:16	2017-05-11 14:48:46	Allow		192.168.1.200		B 73.173.197.235	USA USA			600.34 / tcp	Predefined Searches		DNS Record Type				A, PTR 43200	
- 4		2017-05-11 14:47:46	2017-05-11 14:48:16	Allow		192.168.1.200		73.173.197.235	SA USA			60030 / tcp	Malicious URLs		DNS Sinkhole Name				My Sinkhole	
4		2017-05-11 14:47:40	2017-05-11 14:47:55	Allow		192.168.1.200		10.83.181.139				60027 / tcp			HTTP Response Code				200	
4		2017-05-11 14:47:15	2017-05-11 14:48:46	Allow		192.168.1.200		# 72.246.56.169	usa			60022 / tcp	Relevance		VLAN ID				10	
4		2017-05-11 14:47:15	2017-05-11 14:47:45	Allow		192.168.1.200		73.173.197.235	USA			60021 / tcp	Standard HTTP		Geolocation					
		2012-05-11 14:45:45	2012-05-11 14-42-15	Allow		102 168 1 200		73 173 197 334				60017 / http			Initiator Country				USA, United States, U	nited*
	0	2017-02-11 14:46:45	2017-03-11 14:47:15	CONTR.		m 124.168.1.200			<u>2028</u>			SPACE A SED			Responder Country Orioinal Client Country				USA, United States, U USA, United States, U	inted*
Last	login or	Tuesday, 2017-04-25 at	12:42:21 PM from rtp-flipi	ey-88111.c	isco.com										Initiator / Responder Country				USA, United States, U	inted*
100							_													

Door op "Zoeken bewerken" te klikken en door een unieke bron (Initiator) IP te filteren, ziet u de stromen die door Firepower werden gedetecteerd. De kolom Actie toont "toestaan" voor het verkeer van deze gastheer.

Als Firepower bedoeld verkeer blokkeert, zal de Action het woord "Block" bevatten. Wanneer u op "Tabelweergave van verbindingsgebeurtenissen" klikt, worden er meer gegevens gegenereerd. De volgende velden in de verbindingsgebeurtenissen kunnen worden bekeken als de actie "Blok" is:

- Reden
- Toegangscontroleregels

## Snelle beperking

Om snel een probleem op te lossen dat vermoedelijk het gevolg is van de ACS-regels, kunnen de volgende maatregelen worden genomen:

- Schep een regel met "vertrouwen" of "toestaan" voor het betreffende verkeer en plaats deze bovenaan de ACS-regels, of bovenal de algemene regels.
- schakelt tijdelijk alle regels uit met een actie die het woord "Blok" bevat
- Als de standaardoptie is ingesteld op "Alle verkeer blokkeren", moet u deze tijdelijk overzetten op "Alleen netwerkontdekking"

Opmerking: Deze snelle verzachting vereist beleidswijzigingen die mogelijk niet in alle

omgevingen mogelijk zijn. Aanbevolen wordt om eerst te proberen om sporen van systeemondersteuning te gebruiken om te bepalen welke regel het verkeer bij elkaar past voordat u het beleid wijzigt.

### Ontduiking van de ACS-landen

Verdere problemen oplossen bij de ACS-operaties kan worden uitgevoerd via het CLIhulpprogramma **voor systeemondersteuning**.

Opmerking: Op de platforms Firepower 9300 en 4100 kan de shell in kwestie worden benaderd via de volgende opdrachten:

# sluit module 1 console aan
Firepower-module1> verbinding-ftd
>

Voor meerdere instellingen kan het logische apparaat CLI worden benaderd met de volgende opdrachten. # connect module 1 telnet Firepower-module1> verbinding ftd1 Vet "exit" in om terug te keren naar CLI voor Opstarten

>

Het **systeem-ondersteuning** van **firewalls-machine-debug**-gebruik heeft een ingang voor elk pakket dat door de ACS-landen wordt geëvalueerd. Het laat zien dat het proces van evaluatie van de regels plaatsvindt, en waarom een regel wordt gematcht of niet wordt gematcht.

Opmerking: In versie 6.2 en hoger kan het **systeemondersteunende** traceringstool worden uitgevoerd. Het gebruikt dezelfde parameters maar bevat meer details. Vergeet niet 'y' in te voeren als dit wordt gevraagd met **ook** "**Schakel** de **firewall-motor uit?**".

#### Voorbeeld 1: Verkeer komt overeen met een vertrouwensregel

In het onderstaande voorbeeld wordt het opzetten van een SSH-sessie geëvalueerd met behulp van systeemondersteuning firewall-engine-debug.

Dit is de ACS die op het FirePOWER-apparaat draait.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applic	Sourc	Dest P	URLs	ISE/S Attrib	Acti	V h
•	▼ 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	⇒ Tru	ist 🛈 🗋
2	inspect	Any	Any	👳 10.0.0/8 🗜	Any	Any	Any	Any	Any	Any	Any	Any	🛹 Allo	ow🤍 🐚
3	trust server backup	Any	Any	👳 192.168.62.3	2 10.123.175.22	Any	Any	Any	Any	Any	Any	Any	⇒ Tru	ist 🗍 🖺

De ACS-landen hebben drie regels.

1. De eerste regel is het vertrouwen van elk verkeer vanaf 192.168.0.7 met de bestemmingspoorten die door SSH worden gebruikt.

- De tweede regel inspecteert al verkeer dat afkomstig is van 10.0.0.0/8 waarin de netwerkcriteria overeenkomen op basis van de XFF header gegevens (zoals aangegeven door het pictogram naast het netwerkobject)
- 3. De derde regel vertrouwt al het verkeer van 192.168.62.3 tot 10.123.175.22

In het scenario voor het oplossen van problemen wordt een SSH-verbinding van 192.168.62.3 tot 10.123.175.22 geanalyseerd.

De verwachting is dat de sessie overeenkomt met AC regel 3 "back-up van vertrouwensserver". De vraag is hoeveel pakketten het voor deze sessie zou moeten nemen om deze regel aan te passen. Is alle informatie nodig in het eerste pakket om de AC-regel te bepalen of zijn er meerdere pakketten nodig, en als dat zo is, hoeveel?

Op de FirePOWER CLI wordt het volgende ingevoerd om te zien hoe de ACS-regel wordt geëvalueerd.

#### >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**: Het is best om zoveel mogelijk parameters in te vullen wanneer **firewall-engine-debug wordt** uitgevoerd, zodat alleen de interessante debug-berichten naar het scherm worden afgedrukt.

In de debug uitvoer hieronder ziet u de eerste vier pakketten van de sessie die worden geëvalueerd.

SYN

SYN,ACK

**KRIJGEN** 

#### Eerste SSH-pakket (client naar server)

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 110 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 110 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 110 pending rule order 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 110 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 110 pending rule order 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 110 pending rule order 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 110 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-46594 > 10.123.175.22-22 6 AS 110 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-46594 > 10.123.175.22-22 6 AS 110 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-46594 > 10.123.175.22-22 6 AS 110 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-46594 > 10.123.175.22-22 6 AS 110 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-46594 > 10.123.175.22-22 6 AS 110 pending rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 >
```

Dit is een grafiek die verder de Debug-logica illustreert.

- 1. SYN 192.168.62.3 → 10.123.175.22
- 2. SYN,ACK 10.123.175.22 → 192.168.62.3
- 3. ACK 192.168.62.3 → 10.123.175.22
- 4. SSH 192.168.62.3 → 10.123.175.22

Starts evaluation at 'inspect' rule

Service identified as SSH No match 'inspect' rule (non-http) Match 'trust server backup' rule and Trust flow

Voor deze stroom duurt het 4 pakketten zodat het apparaat aan de regel voldoet.

Dit is een gedetailleerde verklaring van de debug uitvoer.

- Het ACS-evaluatieproces begint met de "inspect"-regel, omdat de "trust ssh for host"-regel niet werd afgestemd, aangezien het IP-adres niet aan de eis voldeed. Dit is een snelle overeenkomst vanwege alle informatie die nodig is om te bepalen of deze regel moet worden aangepast is aanwezig in het eerste pakket (IP's en poorten)
- Het kan niet worden bepaald of het verkeer overeenkomt met de "inspectie"-regel totdat de toepassing is geïdentificeerd, aangezien de X-Forwarded-For (XFF) informatie wordt gevonden in het HTTP-toepassingsverkeer, is de toepassing nog niet bekend, dus dit zet de sessie in een hangende status voor regel 2, in afwachting van toepassingsgegevens.
- Zodra de toepassing in het vierde pakket is geïdentificeerd, resulteert de "inspect"-regel in een niet-overeenkomend product, omdat de toepassing SSH in plaats van HTTP is
- De regel "backup server-back-up" van de trust is dan aangepast, op basis van de IPadressen.

Samengevat duurt de verbinding 4 pakketten om de sessie aan te passen omdat het op de firewall moet wachten om de toepassing te identificeren aangezien regel 2 een toepassingsbeperking heeft.

Als regel 2 alleen bronnetwerken had en het geen XFF was, dan had dit 1 pakje nodig om de sessie aan te passen.

U dient altijd de regels van lagen 1-4 boven alle andere regels in het beleid te plaatsen wanneer mogelijk, aangezien deze regels doorgaans 1 pakje vereisen om een beslissing te nemen. U kunt echter ook opmerken dat zelfs met slechts lagen 1-4 regels het meer dan slechts 1 pakket kan zijn om een AC-regel aan te passen en dat de reden hiervoor URL/DNS-security intelligentie is. Als u één van deze machtigt, moet de firewall de toepassing voor alle sessies bepalen die door het AC beleid worden geëvalueerd omdat het moet bepalen of zij HTTP of DNS zijn. Dan moet zij bepalen of zij de sessie op basis van de zwarte lijsten moet toestaan.

Hieronder staat een ingekapselde uitvoer van de opdracht **firewall-motor-debug**, die de relevante velden in rood heeft gemarkeerd. Let op de opdracht die wordt gebruikt om de naam van de applicatie te verkrijgen die geïdentificeerd is.



#### Voorbeeld 2: Verkeersovereenstemming met een vertrouwensregel is geblokkeerd

In sommige scenario's kan het verkeer worden geblokkeerd, ondanks de overeenstemming van een vertrouwensregel in de ACS-landen. Het onderstaande voorbeeld evalueert verkeer met het zelfde toegangscontrolebeleid en hosts.

Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp			<b>S</b>	JG AC (all)	trust server backup
Action ×	<u>Reason</u> ×	Initiator IP ×	Responder X IP	Source Port / × ICMP Type	Destination Port / × ICMP Code	Application × Protocol	<u>Client</u> ×	Intrusion × Events	Access Control × Policy	Access Control × Rule
1 5 1 1	92.168.62.3-5 gt tag: 0, ISE s 92.168.62.3-5 92.168.62.3-5 92.168.62.3-5 92.168.62.3-5	4650 > 10.123.1 gt id: 0, svc -1, 4650 > 10.123.1 4650 > 10.123.1 4650 > 10.123.1	175.22-22 6 AS 1 payload -1, clien 175.22-22 6 AS 1 175.22-22 6 AS 1 175.22-22 6 AS 1	I 0 Starting with t -1, misc -1, use I 0 no match ru I 0 no match ru I 0 match rule	n minimum 0, id 0 and er 9999997, icmpTyp ale order 3, 'Trust s ale order 4, 'inspect order 5, 'trust serve	d IPProto first v e 102, icmpCo sh for host', s ', XFF non-htt r backup', act	vith zones 1 · de 22 rc network a p tion Trust	-> 2, geo 0 -> and GEO	0, vlan 0, inline	
E F	Session was This happened Firewall engine	deleted becaus before AC rule will re-evalua	se we hit a drop e was matched te from top of A	IPS rule and bl (Intrusion polic C policy to find	lacklisted the flow. y before AC rule ma l a rule for logging o	atch dropped) decision]				
1 1 1 1	92.168.62.3-54 92.168.62.3-54 nline sgt tag: ui 92.168.62.3-54 92.168.62.3-54	4650 > 10.123.1 4650 > 10.123.1 ntagged, ISE sg 4650 > 10.123.1 4650 > 10.123.1	175.22-22 6 AS 1 175.22-22 6 AS 1 1t id: 0, svc 0, pa 175.22-22 6 AS 1 175.22-22 6 AS 1	I 0 New sessio I 0 Starting wit yload 0, client 0, I 0 pending rul I 0 Deleting se	n h minimum 4, 'insp misc 0, user 999999 e order 4, 'inspect', ssion	ect', and IPPro 7, icmpType 0 XFF wait for ,	oto first with z , icmpCode 0 <b>AppId</b>	cones 1 -> 2,	geo 0 -> 0, vlan (	),

Zoals hierboven te zien is, toont de **firewall-motor-debug** uitvoer aan dat het verkeer overeenkomt met een "vertrouwen", terwijl de verbindingsgebeurtenissen actie van **Blok** laten zien door een regel van het inbraakbeleid (bepaald omdat de kolom van de Reason **Inbraakblok** toont).

Dit kan gebeuren omdat het **inbraakbeleid** is **gebruikt voordat de toegangscontroleregel wordt bepaald** Instellen in het **tabblad Geavanceerd** op de ACS-landen. Voordat het verkeer op basis van de regel kan worden aangestuurd, identificeert het betrokken Inbraakbeleid een patroonmatch en laat het verkeer vallen. De evaluatie van de ACS-regel resulteert echter in een overeenstemming met de vertrouwensregel, aangezien de IP-adressen voldeden aan de criteria van de "trust server back-up"-regel.

Om ervoor te zorgen dat het verkeer geen inbraakbeleid ondergaat, kan de vertrouwensregel boven de "inspectie"-regel worden geplaatst, wat in beide gevallen een goede praktijk zou zijn. Aangezien de identificatie van de toepassing noodzakelijk is voor een match of non-match van de "inspectie"-regel, **wordt** het **inbraakbeleid dat vóór de toegangscontroleregel wordt gebruikt** gebruikt voor verkeer dat door hetzelfde wordt beoordeeld. Het plaatsen van de "steun van de server van het vertrouwen" regel boven de "inspect" regel veroorzaakt het verkeer om de regel aan te passen wanneer het eerste pakket wordt gezien aangezien de regel op IP adres gebaseerd is, dat in het eerste pakket kan worden bepaald. Daarom **is** het **inbraakbeleid dat wordt gebruikt**  voor de toegangscontrole niet nodig.

#### Scenario 3: Verkeer geblokkeerd door toepassingslabel

In dit scenario melden gebruikers dat CNN.com wordt geblokkeerd. Er is echter geen specifieke regel die CNN blokkeert. De gebeurtenissen van de verbinding, in combinatie met **firewall-motor-debug** uitvoer, tonen de reden voor het blok.

Eerst heeft de verbinding gebeurtenissen een informatievak naast de toepassingsvelden die informatie over de toepassing en hoe Firepower de genoemde toepassing categoriseert, bevat.

▼ First Packet ×	¢	<u>Last</u> × Packet	Action ×	Initiator IP ×	Responder ×	Source Port / × ICMP Type	Destination Port / × ICMP Code	Application × Protocol	Web × Application	Application × Risk	Business X Relevance	<u>URL</u> ×
2017-05-19 16:02	2:29		Block	192.168.62.63	151.101.65.67	<u>54308 / tcp</u>	80 (http) / tcp	HTTP HTTP	CNN.com	Medium	Medium	http://cnn.com/
	CNN Turne	I.com	sting Syste	m's news website	2.			1				
	Type Risk Busir Categ Tags	ness Rele gories	vance	Wet Ven Higt mut disp	o Application y Low h timedia (TV/vide plays ads	o), news						
	¢	Contex	t Explorer	W Wikipedia	G Google	Yahoo!	b Bing					

Met deze informatie in gedachten wordt **firewall-engine-debug** uitgevoerd. In de debug-uitvoer wordt het verkeer geblokkeerd op basis van de toepassingstag.

<ul> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 110 New session</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 110 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0 -&gt; 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</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 110 pending rule order 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0 -&gt; 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</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 110 pending rule order 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0 -&gt; 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</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 110 pending rule order 4, 'block by tag', AppID</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 110 pending rule order 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0 -&gt; 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</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 110 pending rule order 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0 -&gt; 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</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 110 pending rule order 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0(0) -&gt; 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1100, client 638, misc 0, user 9999997, urthtp://cnn.com/") returned 0</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 11 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0(0) -&gt; 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, ur</li></ul>	
<ul> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 1 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0 -&gt; 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</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 1 0 pending rule order 4, 'block by tag', AppID</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 1 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0 -&gt; 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</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 1 0 pending rule order 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0 -&gt; 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</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 1 0 pending rule order 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0 -&gt; 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</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 1 0 pending rule order 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0 -&gt; 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</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 1 0 pending rule order 4, 'block by tag', AppID</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 1 0 pending rule order 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0(0) -&gt; 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// sqt</li> <li>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 1 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -&gt; 2, geo 0(0) -&gt; 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payl</li></ul>	192.168.62.63-54308 > 151.101.65.67-80 6 AS 110 New session
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 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 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 sending block response of 605 bytes 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 peleting 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,
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 pending rule order 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', 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 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 pending session	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 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', 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 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 pending block response of 605 bytes 192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending block response of 605 bytes	192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
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 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 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 sending block response of 605 bytes 192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 bendering 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,
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 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 <b>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block</b> 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 pending session	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 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 sending block response of 605 bytes	192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
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 sending block response of 605 bytes	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,
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 sending block response of 605 bytes 192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 beleting session	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 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	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) -> 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 <b>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block</b> 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	192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 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 <b>192.168.62.63-54308 &gt; 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block</b> 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	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,
<b>192.168.62.63-54308</b> > <b>151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block</b> 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	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 sending block response of 605 bytes 192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session	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 Deleting session	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

Ook al is er geen regel die expliciet <u>http://cnn.com</u> blokkeert, wordt de **gelabelde** advertenties geblokkeerd in het **tabblad Toepassingen** van een ACS-regel.

Editing	Rule	- bl	ock	by	tag	
---------	------	------	-----	----	-----	--

Name	block by tag			🕑 Enabled	1	Move				
Action	💢 Block with reset		• • • • 2 *	1 🔎						
Zone	Networks VLAN	Tags 🛆 Users	Applications	Ports UF	RLs SGT/ISE At	tributes		Inspection	Logging	Comments
Applicat	ion Filters 🖒 Cle	ear All Filters 💢	Available Applicati	ons (759) ⊄	;		Selecte	d Applications	s and Filters (	1) 🔏 📩 🕑
🔍 Sear	ch by name		🔍 Search by name				Filters			
	Defortene	19	eneroyeen		۷.		Jag	: displays ads		8
	💿 blog	53	ClickTale				M rug.	. aispiajo ado		9
	💿 bundles software	7	Clip2Net		0					
	💿 business impact	44	Clip2Net Upload							
	💿 Common Industrial Pro	otocol 1	CloudFlare		0					
	💿 console gaming	25	CNBC							
	💿 content provider	28	CNET		0					
	lecrypted traffic	21	CNET TV		<u> </u>					
1	💿 displays ads	759	CNN.com		<u> </u>	Add to Rule				
	💿 eDonkey	2								
	💿 encrypts communicatio	ons 280								
	💿 evasive	58	Cognitive Match							
	💿 Facebook	27								
	🔝 Facebook game	23	Collegenumor		0					
	💽 Facebook post	7	Collider		0					
	🔝 file sharing/transfer	249	Comcast							
	💿 Flash	39	Comedy Central							
	FTP protocol	11	Commission Jun	ction	0.					
	Gnutella protocol	•	Viev Viev	ving 101-200 of	759 🕨 🕅					
									Save	Cancel

#### Gegevens om te leveren aan TAC

<b>Gegevens</b> Probleemoplossing bestand via het	Instructies
FirePOWER-apparaat dat het verkeer controleert systeemondersteuning	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/1
voor firewall-motor- debug en	Zie dit artikel voor instructies
systeemondersteunende uitvoer	
Uitvoer van toegangsbeheerbeleid	Navigeren in op Systeem > Gereedschappen > Importeren / Exporteren, selecte de knop Exporteren

**Voorzichtig:** Indien de ACS een SSL-beleid bevat, verwijdert u het SSL-beleid van de ACSlanden alvorens te exporteren om gevoelige PKI-informatie te vermijden

#### Volgende stap: Probleemoplossing voor de SSL-beleidslaag

Als een SSL Policy in gebruik is en de probleemoplossing bij toegangsbeheer het probleem niet heeft blootgelegd, is de volgende stap de probleemoplossing in het SSL-beleid.

Klik hier om verder te gaan met het volgende artikel.