

Informazioni sulle azioni delle regole delle policy di controllo degli accessi di Firepower Threat Defense

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Modalità di implementazione della policy ACP](#)

[Configurazione](#)

[Azioni disponibili della policy ACP](#)

[Interazione tra la policy ACP e la policy di prefiltro](#)

[Azione di blocco della policy ACP](#)

[Scenario 1. Eliminazione anticipata da parte del motore LINA](#)

[Scenario 2. Eliminazione dei pacchetti in seguito al verdetto Snort](#)

[Azione di blocco con reset della policy ACP](#)

[Azione di autorizzazione della policy ACP](#)

[Scenario 1. Azione di autorizzazione della policy ACP \(condizioni L3/L4\)](#)

[Scenario 2. Azione di autorizzazione della policy ACP \(condizioni L3-7\)](#)

[Scenario 3. Verdetto di inoltro rapido di Snort con autorizzazione](#)

[Azione considera attendibile della policy ACP](#)

[Scenario 1. Azione considera attendibile della policy ACP](#)

[Scenario 2. Azione trust ACP \(senza SI, QoS e criteri di identità\)](#)

[Azione di blocco della policy di prefiltro](#)

[Azione Fastpath della policy di prefiltro](#)

[Azione Fastpath della policy di prefiltro \(inline-set\)](#)

[Azione Fastpath della policy di prefiltro \(inline-set con tap\)](#)

[Azione di analisi della policy di prefiltro](#)

[Scenario 1. Analisi di prefiltro con regola di blocco ACP](#)

[Scenario 2. Analisi di prefiltro con regola di autorizzazione ACP](#)

[Scenario 3. Analisi di prefiltro con regola di attendibilità ACP](#)

[Scenario 4. Analisi di prefiltro con regola di attendibilità ACP](#)

[Azione di monitoraggio della policy ACP](#)

[Azione di blocco interattivo della policy ACP](#)

[Azione di blocco interattivo con reset della policy ACP](#)

[Connessioni secondarie dell'FTD e pinhole](#)

[Linee guida della regola FTD](#)

[Riepilogo](#)

[Informazioni correlate](#)

Introduzione

In questo documento vengono descritte le diverse operazioni disponibili su Firepower Threat Defense (FTD) per le opzioni Access Control Policy (ACP) e Prefilter Policy.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Funzionalità Flow Offload
- Acquisizione di pacchetti su appliance Firepower Threat Defense
- Traccia e acquisizione dei pacchetti con l'opzione trace sulle appliance FTD

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Firepower 4110 Threat Defense versioni 6.4.0 (Build 113) e 6.6.0 (Build 90)
- Firepower Management Center (FMC) versioni 6.4.0 (Build 113) e 6.6.0 (Build 90)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Le informazioni in questo documento sono applicabili anche ai seguenti hardware e versioni software:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR1000, FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), Kernel-based Virtual Machine (KVM)
- Modulo Integrated Service Router (ISR)
- Software FTD versione 6.1.x e successive

Nota: Flow Offload è supportato solo sulle istanze native delle applicazioni ASA e FTD e sulle piattaforme FPR4100 e FPR9300. Le istanze del contenitore FTD non supportano l'offload del flusso.

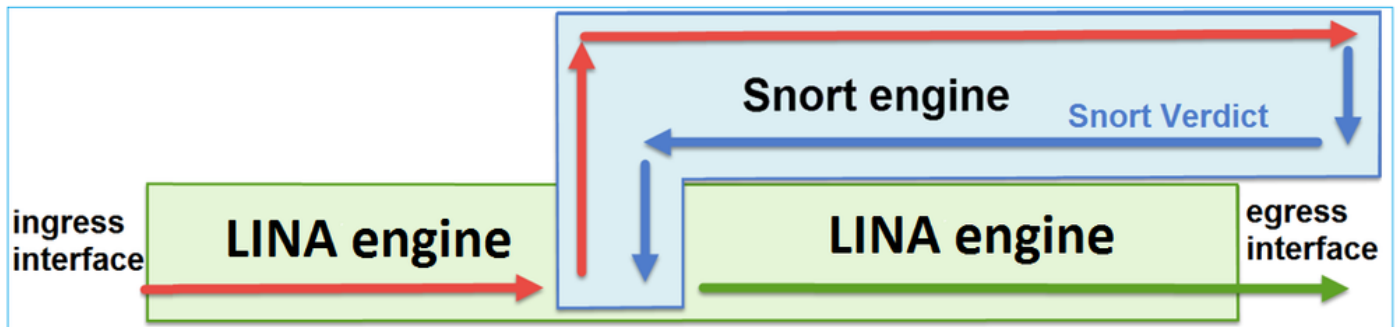
Premesse

Viene esaminata l'operazione in background di ogni azione e la relativa interazione con altre funzionalità, quali Flow Offload e protocolli che aprono connessioni secondarie.

FTD è un'immagine software unificata costituita da 2 motori principali:

- Motore LINA
- Motore Snort

Questa figura mostra il rapporto tra i 2 motori:



- Il pacchetto entra dall'interfaccia di ingresso e viene gestito dal motore LINA
- Se richiesto dalla policy FTD, il pacchetto viene ispezionato dal motore Snort
- Il motore Snort restituisce un verdetto (elenco dei permessi o elenco dei blocchi) per il pacchetto
- In base a questo verdetto, il motore LINA elimina il pacchetto o lo inoltra

Modalità di implementazione della policy ACP

La policy FTD è configurata su FMC se si adotta la gestione remota o su Firepower Device Manager (FDM) se si adotta la gestione locale. In entrambi gli scenari, la policy ACP viene applicata come segue:

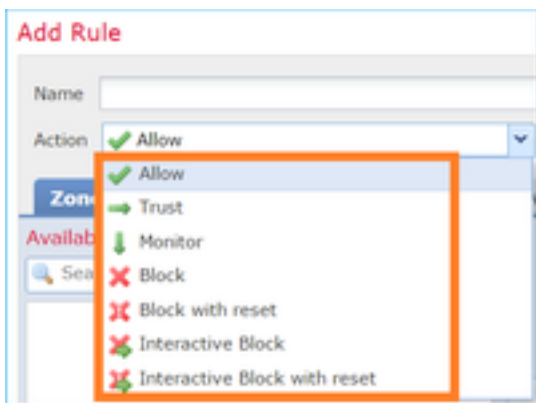
- Una lista di controllo degli accessi globale (ACL) denominata CSM_FW_ACL_ al motore LINA FTD
- Regole di controllo degli accessi nel file /ngfw/var/sf/detection_engines/<UUID>/ngfw.rules sul motore Snort dell'FTD

Configurazione

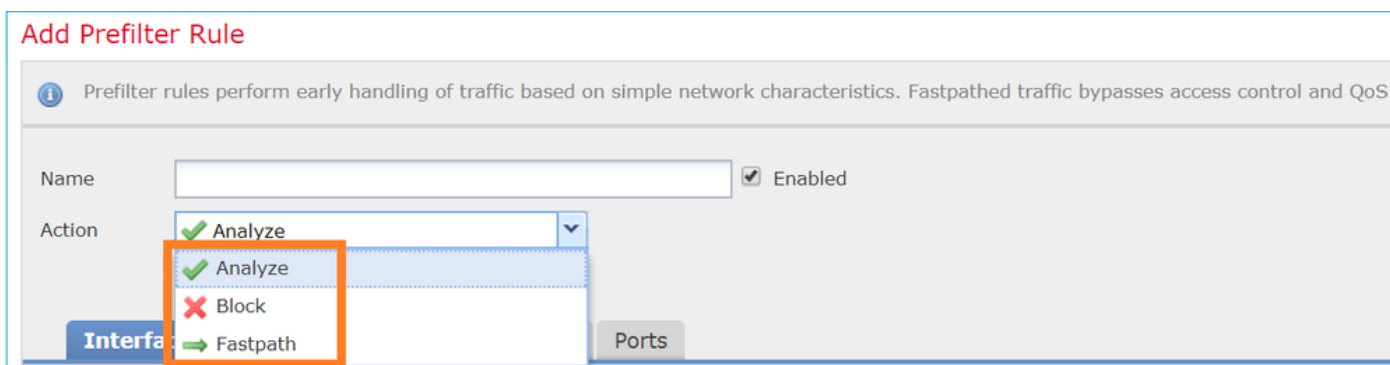
Azioni disponibili della policy ACP

La policy ACP dell'FTD contiene una o più regole e ogni regola può prevedere una di queste azioni, come mostrato nell'immagine:

- Allow
- Trust
- Monitor
- Block
- Block with reset
- Interactive Block
- Interactive Block with reset



Analogamente, la policy di prefiltro può contenere una o più regole e le azioni mostrate nell'immagine:



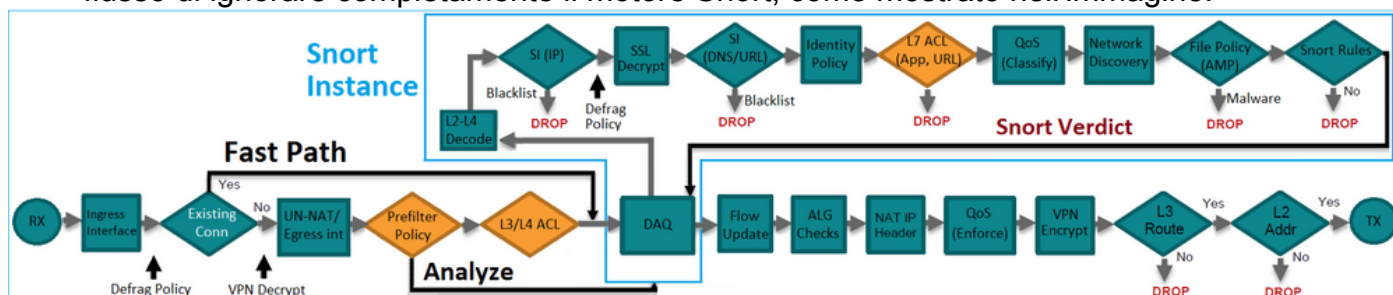
Interazione tra la policy ACP e la policy di prefiltro

Il criterio di prefiltrazione è stato introdotto nella versione 6.1 e ha due finalità principali:

1. Consentire l'ispezione del traffico con tunneling quando il motore LINA dell'FTD controlla l'intestazione IP esterna e il motore Snort controlla l'intestazione IP interna. In particolare, nel caso del traffico di tunneling (ad esempio il GRE), le regole dei criteri di prefiltro agiscono sempre sul **outer headers**, mentre le regole nei paesi ACP sono sempre applicabili alle sessioni interne (**inner headers**). Il traffico con tunneling fa riferimento a questi protocolli:

- GRE
- IP-in-IP
- IPv6-in-IP
- Teredo Port 3544

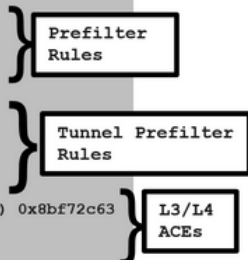
2. Fornisce il controllo dell'accesso anticipato (EAC, Early Access Control) che consente al flusso di ignorare completamente il motore Snort, come mostrato nell'immagine.



Le regole di prefiltro vengono distribuite su FTD come ACE (Access Control Element) L3/L4 e

precedono le ACE L3/L4 configurate, come mostrato nell'immagine:

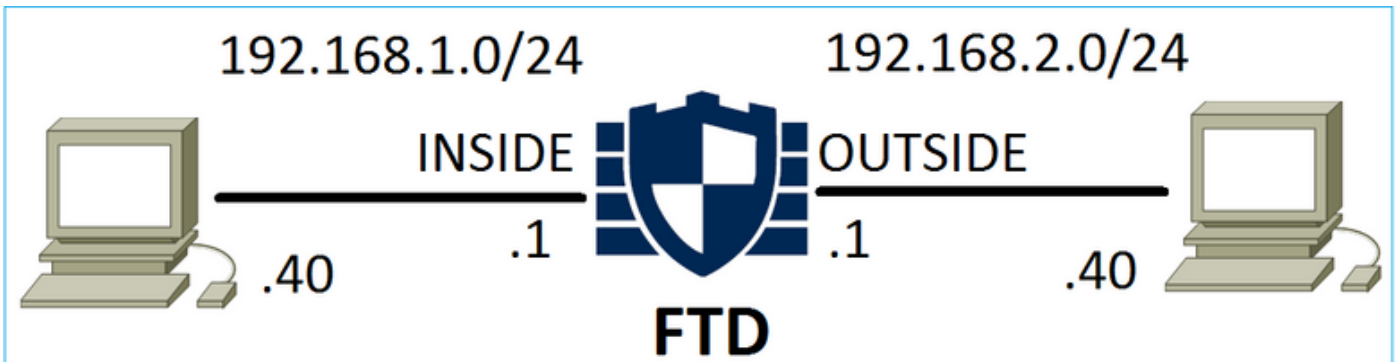
```
firepower# show access-list
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log both (hitcnt=0)
access-list CSM_FW_ACL_ line 4 remark rule-id 268434456: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268434456: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id 268434456 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268434456 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268434456 (hitcnt=2) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any any eq 3544 rule-id 268434456 (hitcnt=0) 0xcf6309bc
access-list CSM_FW_ACL_ line 10 remark rule-id 268434445: ACCESS POLICY: FTD5506-1 - Mandatory/1
access-list CSM_FW_ACL_ line 12 advanced deny ip host 10.1.1.1 any rule-id 268434445 event-log flow-start (hitcnt=0) 0x8bf72c63
access-list CSM_FW_ACL_ line 14 remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 15 advanced permit ip any any rule-id 268434434 (hitcnt=410) 0xald3780e
```



Nota: regole di prefiltro e regole ACP: viene applicata la regola soddisfatta per prima.

Azione di blocco della policy ACP

Prendere in considerazione la topologia mostrata in questa immagine:



Scenario 1. Eliminazione anticipata da parte del motore LINA

La policy ACP contiene una regola Block (Blocca) che usa una condizione L4 (porta TCP di destinazione 80) come mostrato in questa immagine:

Access Control													
ACP1													
Enter Description													
Prefilter Policy: Default Prefilter Policy													
SSL Policy: None													
Identity Policy: None													
Inheritance Set													
Rules													
Security Intelligence													
HTTP Responses													
Advanced													
Filter by Device													
Show Rule Conflicts													
Add Category													
Add Rule													
Search Rule													
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Any	Block

La policy applicata in Snort:

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

La policy applicata in LINA. Si noti che la regola viene sottoposta a push come deny azione:

```
firepower# show access-list
```

...

```
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 event-log flow-start (hitcnt=0) 0x6149c43c
```

Verificare gli effetti di questa azione.

Quando l'host A (192.168.1.40) tenta di aprire una sessione HTTP sull'host B (192.168.2.40), i pacchetti di sincronizzazione TCP (SYN) vengono scartati dal motore LINA FTD e non raggiungono lo Snort Engine o la destinazione:

```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
430 bytes]
  match ip host 192.168.1.40 any
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
0 bytes]
  match ip host 192.168.1.40 any
```

```
firepower# show capture CAPI
1: 11:08:09.672801 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4060517 0>
2: 11:08:12.672435 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4063517 0>
3: 11:08:18.672847 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4069517 0>
4: 11:08:30.673610 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4081517 0>
```

```
firepower# show capture CAPI packet-number 1 trace
1: 11:08:09.672801 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4060517 0>
...
```

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id
268435461 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268435461: L4 RULE: Rule1
Additional Information:
```

<- No Additional Information = No Snort Inspection

```
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Scenario 2. Eliminazione dei pacchetti in seguito al verdetto Snort

La policy ACP contiene una regola Block (Blocca) che usa una condizione L7 (HTTP dell'applicazione) come mostrato in questa immagine:

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	HTTP	Any	Any	Any	Any	Block

La policy applicata in Snort:

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any (appid 676:1)
```

Appid 676:1 = HTTP

La policy applicata in LINA.

Nota: Viene eseguito il push della regola come **permit** perché LINA non è in grado di determinare che la sessione utilizza HTTP. Su FTD il meccanismo di rilevamento delle applicazioni è nel motore Snort.

```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 (hitcnt=0) 0xb788b786
```

Per una regola di blocco che utilizza **Application** come condizione, la traccia di un vero pacchetto mostra che la sessione viene scartata dalla LINA a causa del verdetto del motore Snort.

Nota: affinché il motore Snort possa individuare l'applicazione, deve ispezionare alcuni pacchetti (in genere 3-10 a seconda del decodificatore delle applicazioni). Pertanto, alcuni pacchetti vengono fatti passare tramite l'FTD e raggiungono la destinazione. I pacchetti consentiti sono ancora soggetti al controllo dei criteri per le intrusioni in base ai **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** opzione.

Verificare gli effetti di questa azione.

Quando l'host A (192.168.1.40) cerca di stabilire una connessione HTTP con l'host B (192.168.2.40), il motore LINA acquisisce in ingresso quanto segue:

```
firepower# show capture CAPI
8 packets captured
```

```
1: 11:31:19.825564 192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
2: 11:31:19.826403 192.168.2.40.80 > 192.168.1.40.32790: S 1283931030:1283931030(0) ack
357753152 win 2896 <mss 1380,sackOK,timestamp 5449236 5450579>
3: 11:31:19.826556 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>
4: 11:31:20.026899 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450781 5449236>
5: 11:31:20.428887 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5451183 5449236>
...
```

Acquisizione in uscita:

```
firepower# show capture CAPO
```

5 packets captured

```
1: 11:31:19.825869 192.168.1.40.32790 > 192.168.2.40.80: S 1163713179:1163713179(0) win 2920
<mss 1380,sackOK,timestamp 5450579 0>
2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
3: 11:31:23.426049 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5452836 5450579>
4: 11:31:29.426430 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5458836 5450579>
5: 11:31:41.427208 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5470836 5450579>
```

La traccia mostra che il primo pacchetto (TCP SYN) è consentito dallo Snort poiché il verdetto di rilevamento applicazione non è stato ancora raggiunto:

```
firepower# show capture CAPI packet-number 1 trace
```

```
1: 11:31:19.825564 192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
...
```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435461

access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory

access-list CSM_FW_ACL_ remark rule-id 268435461: L7 RULE: Rule1

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

...

Phase: 10

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 23194, packet dispatched to next module

...

Phase: 12

Type: SNORT

Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 357753151
AppID: service unknown (0), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
Firewall: **pending rule-matching, id 268435461, pending AppID**
NAP id 1, IPS id 0, **Verdict PASS**
Snort Verdict: (pass-packet) allow this packet

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow

Lo stesso accade per il pacchetto TCP SYN/ACK:

```
firepower# show capture CAPO packet-number 2 trace
  2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
```

...

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 23194, using existing flow

...

Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, ACK, seq 1283931030, ack 357753152
AppID: service unknown (0), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
Firewall: **pending rule-matching, id 268435461, pending AppID**
NAP id 1, IPS id 0, **Verdict PASS**
Snort Verdict: (pass-packet) allow this packet

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: INSIDE
output-status: up
output-line-status: up
Action: allow

Snort restituisce un verdetto DROP una volta completata l'ispezione del terzo pacchetto:

```
firepower# show capture CAPI packet-number 3 trace
  3: 11:31:19.826556 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 23194, using existing flow

Phase: 5
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 357753152, ack 1283931031
AppID: service HTTP (676), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0(0) -> 0, vlan 0, sgt 65535, user 9999997,
url http://192.168.2.40/128k.html
Firewall: block rule, id 268435461, drop
Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0, Verdict BLOCKLIST, Blocked by Firewall
Snort Verdict: (block-list) block list this flow

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor
```

È inoltre possibile eseguire il comando `system support trace` dalla modalità FTD CLISH. Lo strumento offre 2 funzioni:

- Mostra il verdetto Snort per ogni pacchetto inviato alla libreria di acquisizione dei dati (DAQ) e visualizzato in LINA. DAQ è un componente situato tra il motore LINA dell'FTD e il motore Snort.
- Consente l'esecuzione `system support firewall-engine-debug` allo stesso tempo per vedere cosa succede all'interno del motore Snort stesso

Questo è l'output:

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages
```

Tracing enabled by Lina

```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, seq 2620409313
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 New session
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, 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
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS
```

Tracing enabled by Lina

```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, ACK, seq 3700371680, ack 2620409314
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, 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
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS
```

Tracing enabled by Lina

```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, ACK, seq 2620409314, ack 3700371681
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service HTTP (676), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc
676, payload 0, client 686, misc 0, user 9999997, url http://192.168.2.40/128k.html, xff
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0(0)
-> 0, vlan 0, sgt 65535, user 9999997, url http://192.168.2.40/128k.html
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 match rule order 2, 'Rule1', action Block
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 deny action
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: block rule, 'Rule1', drop
192.168.1.40-32791 > 192.168.2.40-80 6 Snort: processed decoder alerts or actions queue, drop
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Deleting session
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict BLOCKLIST
192.168.1.40-32791 > 192.168.2.40-80 6 ==> Blocked by Firewall
```

Riepilogo

- L'azione di blocco della policy ACP viene applicata come regola permit o deny nel motore LINA a seconda delle condizioni impostate per la regola.
- Se le condizioni sono L3/L4, LINA blocca il pacchetto. Nel caso del TCP, il primo pacchetto (TCP SYN) è bloccato
- Se le condizioni sono L7, il pacchetto viene inoltrato al motore Snort per un'ulteriore ispezione. Se viene usato il protocollo TCP, alcuni pacchetti vengono comunque inoltrati tramite l'FTD finché Snort non formula un verdetto. I pacchetti consentiti sono ancora soggetti al controllo dei criteri per le intrusioni in base ai **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** opzione.

Azione di blocco con reset della policy ACP

Una regola Block with reset (Blocca con reset) configurata nell'interfaccia utente FMC:

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
▼ Mandatory - ACP1 (1-4)													
1 Block-RST-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Block with reset
2 Block-RST_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Block with reset

La regola di blocco con reimpostazione viene distribuita nel motore LINA FTD come **permit** e snort engine come **reset** regola:

```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=0) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Block-RST_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Motore Snort:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
...
# Start of AC rule.
268438864 reset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 reset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

Quando un pacchetto corrisponde a Blocco con regola di reimpostazione FTD invia **TCP Reset** pacchetto o **ICMP Type 3 Code 13** Messaggio Destination Unreachable (filtrato in modo amministrativo):

```
root@kali:~/tests# wget 192.168.11.50/file1.zip
--2020-06-20 22:48:10-- http://192.168.11.50/file1.zip
Connecting to 192.168.11.50:80... failed: Connection refused.
```

Ecco l'acquisizione eseguita sull'interfaccia di ingresso dell'FTD:

```
firepower# show capture CAPI
2 packets captured
1: 21:01:00.977259 802.1Q vlan#202 P0 192.168.10.50.41986 > 192.168.11.50.80: S
3120295488:3120295488(0) win 29200 <mss 1460,sackOK,timestamp 3740873275 0,nop,wscale 7>
2: 21:01:00.978114 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.41986: R 0:0(0) ack
3120295489 win 0 2 packets shown
```

System support trace Questo output, in questo caso, mostra che il pacchetto è stato scartato a causa del verdetto Snort:

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.50
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages
```

```
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3387496622
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 new firewall session
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 using HW or preset rule order 2, 'Block-RST-
Rule1', action Reset and prefilter rule 0
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 HitCount data sent for rule id: 268438864,
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 reset action
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 deleting firewall session flags = 0x0,
fwFlags = 0x0
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: block w/ reset rule, 'Block-RST-
Rule1', drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 9, NAP id 1, IPS id 0, Verdict
BLOCKLIST
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ
```

Scenari d'uso

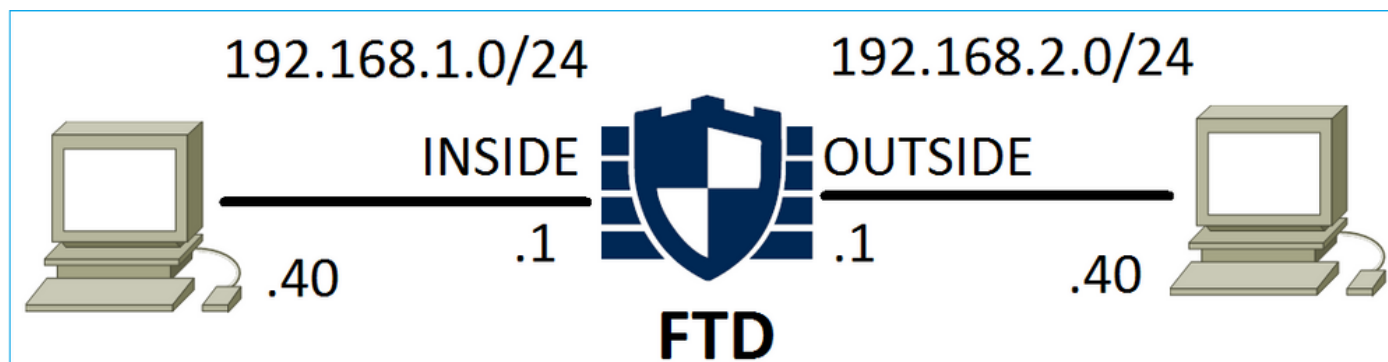
Uguale a **Block** , ma interrompe immediatamente la connessione.

Azione di autorizzazione della policy ACP

Scenario 1. Azione di autorizzazione della policy ACP (condizioni L3/L4)

In genere, si configura una regola Allow (Autorizza) per condurre ulteriori ispezioni, come accade con una policy anti-intrusione e/o una policy di controllo file. In questo primo scenario viene illustrato il funzionamento di una regola Allow quando viene applicata una condizione L3/L4.

Supponiamo di avere questa topologia:



La policy viene applicata come mostrato nell'immagine:

Access Control > Access Control													
Network Discovery			Application Detectors			Correlation			Actions				
ACP1													
Enter Description													
Prefilter Policy: Default Prefilter Policy				SSL Policy: None				Identity Policy: None					
Inheritance Settings													
Rules Security Intelligence HTTP Responses Advanced													
Filter by Device <input type="checkbox"/> Show Rule Conflicts <input type="checkbox"/> Add Category <input type="button" value="+"/> Add Rule <input type="button" value="Search Rules"/>													
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Any	Allow

La policy applicata in Snort. Si noti che la regola viene distribuita come **allow** azione:

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

La policy in LINA.

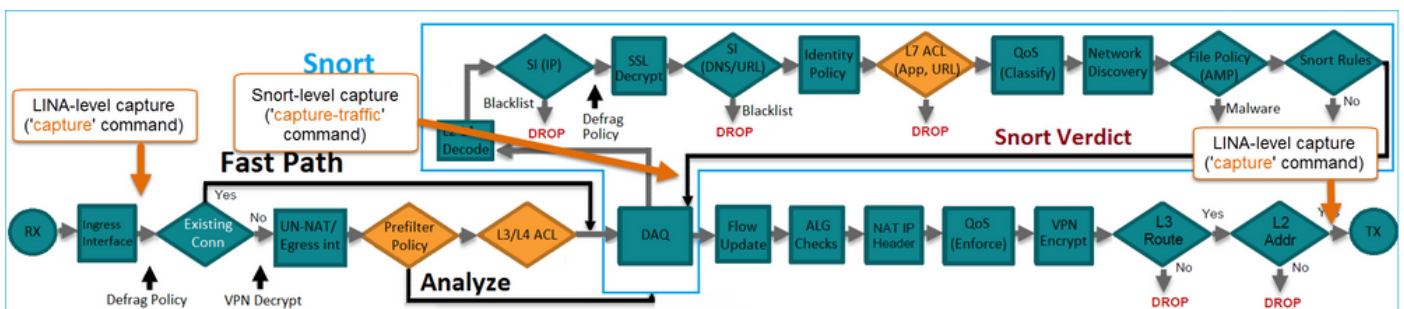
Nota: La regola viene distribuita come **permit** un'azione che essenzialmente comporta il reindirizzamento verso Snort per un'ulteriore ispezione.

```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 (hitcnt=1) 0x641a20c3
```

Per verificare come FTD gestisce un flusso che corrisponde a una regola Allow, sono disponibili alcuni modi:

- Verificare le statistiche di Snort
- Usare il comando `system support trace` dallo strumento CLISH
- Usare il comando `capture` con l'opzione `trace` in LINA ed eventualmente usare il comando `capture-traffic` nel motore Snort

Differenze tra comando `capture` in LINA e il comando `capture-traffic` in Snort:



Verificare gli effetti di questa azione.

Cancellare le statistiche Snort, abilitare `system support trace` from CLISH, and initiate an HTTP flow from host-A (192.168.1.40) to host-B (192.168.2.40). All the packets are forwarded to the Snort engine and get the PASS verdict by the Snort:

```
firepower# clear snort statistics
```

```
> system support trace
```

```
Please specify an IP protocol:  
Please specify a client IP address: 192.168.1.40  
Please specify a client port:  
Please specify a server IP address: 192.168.2.40  
Please specify a server port:  
Enable firewall-engine-debug too? [n]:  
Monitoring packet tracer debug messages
```

```
Tracing enabled by Lina  
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, seq 361134402  
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)  
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow  
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS  
Trace buffer and verdict reason are sent to DAQ's PDTS
```

```
Tracing enabled by Lina  
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, ACK, seq 1591434735, ack 361134403  
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)  
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow  
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS  
Trace buffer and verdict reason are sent to DAQ's PDTS
```

```
Tracing enabled by Lina  
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, ACK, seq 361134403, ack 1591434736  
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service HTTP (676), application unknown (0)  
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow  
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
```

Aumento contatori Pacchetti passati:

```
> show snort statistics
```

```
Packet Counters:  
  Passed Packets                    54  
  Blocked Packets                    0  
  Injected Packets                    0  
  Packets bypassed (Snort Down)      0  
  Packets bypassed (Snort Busy)      0  
  
Flow Counters:  
  Fast-Forwarded Flows                0  
  Blocklisted Flows                    0  
...
```

Pacchetti autorizzati = Ispezionati dal motore Snort

Scenario 2. Azione di autorizzazione della policy ACP (condizioni L3-7)

Un comportamento simile si verifica quando la regola Allow (Autorizza) viene applicata nel modo seguente.

Solo una condizione L3/L4 come mostrato nell'immagine:

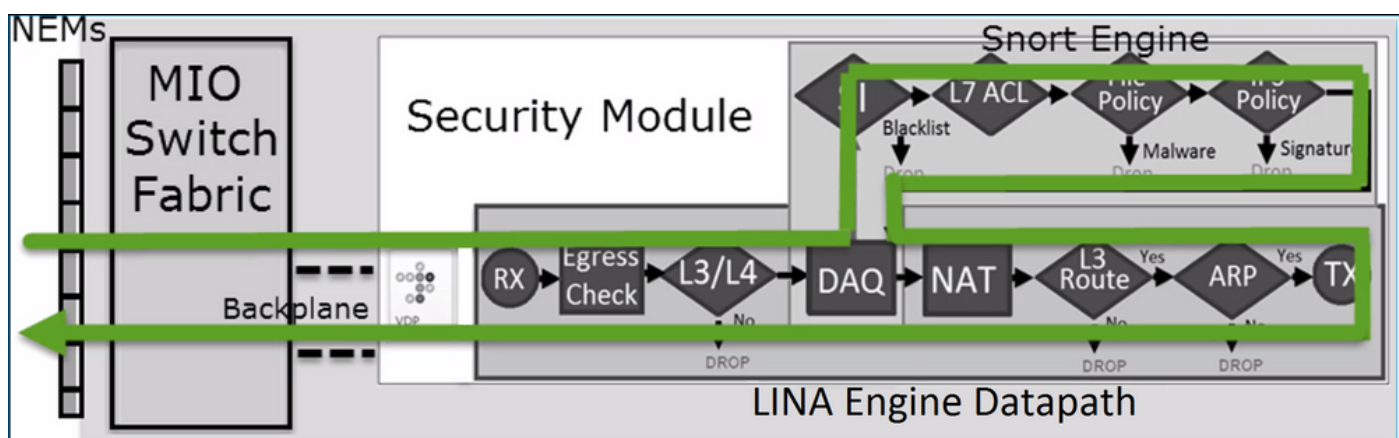
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

Nell'immagine è illustrata una condizione L7 (ad esempio criteri intrusione, criteri file, applicazioni e così via):

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

Riepilogo

L'immagine mostra come un flusso, che soddisfa la regola di autorizzazione, viene gestito dall'FTD implementato su un FP4100/9300:



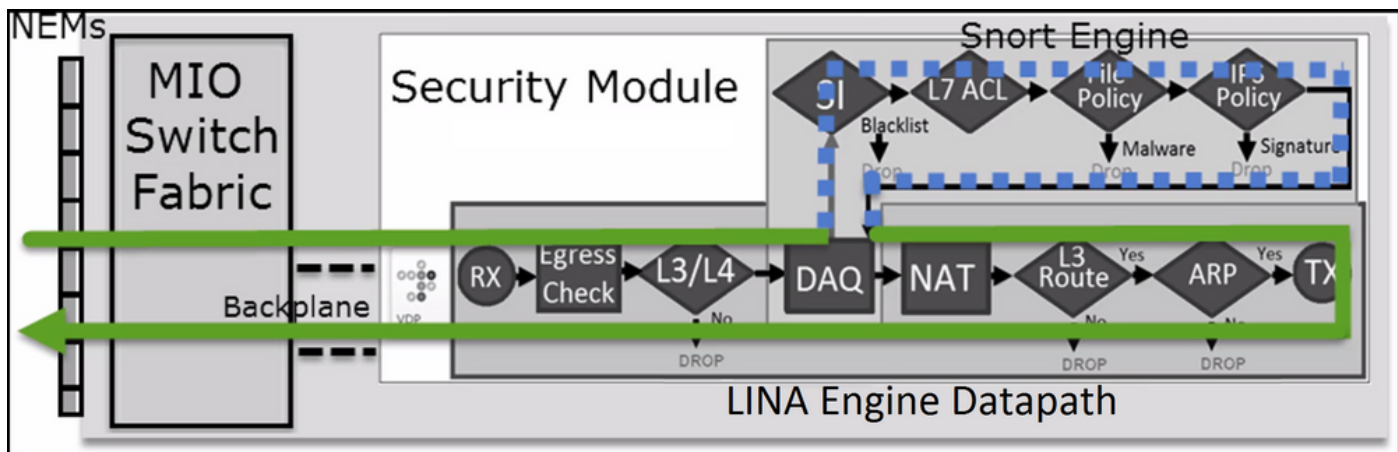
Nota: Management Input Output (MIO) è il Supervisor Engine dello chassis di Firepower.

Scenario 3. Verdetto di inoltro rapido di Snort con autorizzazione

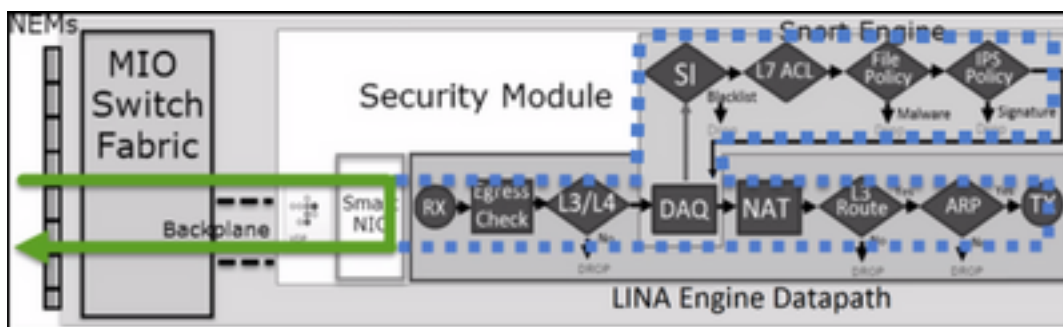
Esistono scenari specifici in cui il motore FTD Snort emette un verdetto PERMITLIST (avanzamento rapido) e il resto del flusso viene scaricato sul motore LINA (in alcuni casi viene scaricato sull'acceleratore HW - SmartNIC). ossia SmartNIC):

1. Traffico SSL senza una policy SSL configurata
2. Intelligent Application Bypass (IAB)

Questa è la rappresentazione visiva del percorso del pacchetto:



O in alcuni casi:



Considerazioni principali

- La regola Consenti viene distribuita come **allow** Snort e **permit** In LINA
- Nella maggior parte dei casi, tutti i pacchetti di una sessione vengono inoltrati al motore Snort per un'ulteriore ispezione

Scenari d'uso

Si desidera configurare una regola di autorizzazione per i casi in cui è necessario effettuare un controllo L7 sul motore Snort, ad esempio:

- Policy anti-intrusione
- Policy di controllo file

Azione considerata attendibile della policy ACP

Scenario 1. Azione considerata attendibile della policy ACP

Se non si desidera applicare l'ispezione L7 avanzata a livello di snort (ad esempio, Criteri intrusione, Criteri file, Individuazione rete), ma si desidera comunque utilizzare funzionalità quali Security Intelligence (SI), Identity Policy, QoS e così via, è consigliabile utilizzare l'azione Trust nella regola.

Topologia:



La policy configurata:

ACP1															Analyze Hit Counts	Save	Cancel					
Enter Description															Inheritance Settings Policy Assignments (1)							
Rules	Security Intelligence	HTTP Responses	Logging	Advanced	Prefilter Policy: Prefilter1					SSL Policy: None		Identity Policy: None										
Filter by Device															Search Rules	Show Rule Conflicts	Add Category	Add Rule				
Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action									
Mandatory - ACP1 (1-4)																						
1	trust_L3-L4	Any	Any	192.168.10.50 192.168.10.51	192.168.11.50 192.168.11.51	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Trust								

La regola di attendibilità viene applicata nel motore Snort dell'FTD:

```
# Start of AC rule.
268438858 fastpath any 192.168.10.50 31 any any 192.168.11.50 31 80 any 6 (log dcforward
flowend)
```

Nota: Il numero 6 è il protocollo (TCP).

La regola nel motore LINA dell'FTD:

```
firepower# show access-list | i 268438858
access-list CSM_FW_ACL_ line 17 remark rule-id 268438858: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 18 remark rule-id 268438858: L7 RULE: trust_L3-L4
access-list CSM_FW_ACL_ line 19 advanced permit tcp object-group FMC_INLINE_src_rule_268438858
object-group FMC_INLINE_dst_rule_268438858 eq www rule-id 268438858 (hitcnt=19) 0x29588b4f
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=19) 0x9d442895
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0xd026252b
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=0) 0x0d785cc4
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0x3b3234f1
```

Verifica:

Attiva **system support trace** e avviare una sessione HTTP dall'host A (192.168.10.50) all'host B (192.168.11.50). I pacchetti inoltrati al motore Snort sono 3. Snort Engine invia a LINA il verdetto PERMITLIST che essenzialmente scarica il resto del flusso sul motore LINA:

> **system support trace**

Enable firewall-engine-debug too? [n]: **y**

Please specify an IP protocol: **tcp**

Please specify a client IP address: **192.168.10.50**

Please specify a client port:

Please specify a server IP address: **192.168.11.50**

Please specify a server port: **80**

Monitoring packet tracer and firewall debug messages

```
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 453426648
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 new firewall session
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 using HW or preset rule order 5, 'trust_L3-
L4', action Trust and prefilter rule 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 HitCount data sent for rule id: 268438858,
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2820426532, ack
453426649
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 453426649, ack
2820426533
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PERMITLIST
```

Una volta terminata la connessione, il motore Snort ottiene le informazioni sui metadati dal motore LINA ed elimina la sessione:

```
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Got end of flow event from hardware with
flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 3
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Logging EOF for event from hardware with
rule_id = 268438858 ruleAction = 3 ruleReason = 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 : Received EOF, deleting the snort session.

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleting snort session, reason:
timeout
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 deleting firewall session flags = 0x10003,
fwFlags = 0x1115
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleted snort session using 0
bytes; protocol id:(-1) : LWstate 0xf LWFlags 0x6007
```

Snort Capture mostra i 3 pacchetti che vanno al motore Snort:

> **capture-traffic**

Please choose domain to capture traffic from:

- 0 - management0
- 1 - management1
- 2 - Global

Selection? **2**

Please specify tcpdump options desired.

(or enter '?' for a list of supported options)

Options: **-n vlan and (host 192.168.10.50 and host 192.168.11.50)**

10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [S], seq 3065553465, win 29200, options [mss 1380,sackOK,TS val 3789188468 ecr 0,nop,wscale 7], length 0

10:26:16.525928 IP 192.168.11.50.80 > 192.168.10.50.42144: Flags [S.], seq 3581351172, ack 3065553466, win 8192, options [mss 1380,nop,wscale 8,sackOK,TS val 57650410 ecr 3789188468], length 0

10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [.], ack 1, win 229, options [nop,nop,TS val 3789188470 ecr 57650410], length 0

Il comando capture di LINA mostra il flusso che lo sta attraversando:

```
firepower# show capture CAPI
```

437 packets captured

1: 09:51:19.431007 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: S 2459891187:2459891187(0) win 29200 <mss 1460,sackOK,timestamp 3787091387 0,nop,wscale 7>

2: 09:51:19.431648 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: S 2860907367:2860907367(0) ack 2459891188 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp 57440579 3787091387>

3: 09:51:19.431847 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: . ack 2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>

4: 09:51:19.431953 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: P 2459891188:2459891337(149) ack 2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>

5: 09:51:19.444816 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: . 2860907368:2860908736(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>

6: 09:51:19.444831 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: . 2860908736:2860910104(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>

...

La traccia dei pacchetti provenienti da LINA è un altro modo per visualizzare i verdetti Snort. Il primo pacchetto ha ottenuto il verdetto PASS:

```
firepower# show capture CAPI packet-number 1 trace | i Type|Verdict
```

Type: CAPTURE

Type: ACCESS-LIST

Type: ROUTE-LOOKUP

Type: ACCESS-LIST

Type: CONN-SETTINGS

Type: NAT

Type: NAT

Type: IP-OPTIONS

Type: CAPTURE

Type: CAPTURE

Type: NAT

Type: CAPTURE

Type: NAT

```
Type: IP-OPTIONS
Type: CAPTURE
Type: FLOW-CREATION
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

Traccia del pacchetto TCP SYN/ACK sull'interfaccia esterna:

```
firepower# show capture CAPO packet-number 2 trace | i Type|Verdict
Type: CAPTURE
Type: ACCESS-LIST
Type: FLOW-LOOKUP
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

L'ACK TCP ottiene il verdetto PERMITLIST:

```
firepower# show capture CAPI packet-number 3 trace | i Type|Verdict
Type: CAPTURE
Type: ACCESS-LIST
Type: FLOW-LOOKUP
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
Type: CAPTURE
```

Questo è l'output completo del verdetto Snort (pacchetto 3):

```
firepower# show capture CAPI packet-number 3 trace | b Type: SNORT
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 687485179, ack 1029625865
AppID: service unknown (0), application unknown (0)
Firewall: trust/fastpath rule, id 268438858, allow
Snort id 31, NAP id 2, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
```

Il quarto pacchetto non viene inoltrato al motore Snort poiché il verdetto è memorizzato nella cache dal motore LINA:

firepower# show capture CAPI packet-number 4 trace

441 packets captured

4: 10:34:02.741523 802.1Q vlan#202 P0 192.168.10.50.42158 > 192.168.11.50.80: P
164375589:164375738(149) ack 3008397532 win 229 <nop,nop,timestamp 3789654678 57697031>

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: FLOW-LOOKUP

Subtype:

Result: ALLOW

Config:

Additional Information:

Found flow with id 1254, using existing flow

Phase: 4

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Verdict: (fast-forward) fast forward this flow

Result:

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

Action: allow

1 packet shown

Le statistiche di Snort lo confermano:

firepower# show snort statistics

Packet Counters:

Passed Packets	2
Blocked Packets	0
Injected Packets	0
Packets bypassed (Snort Down)	0
Packets bypassed (Snort Busy)	0

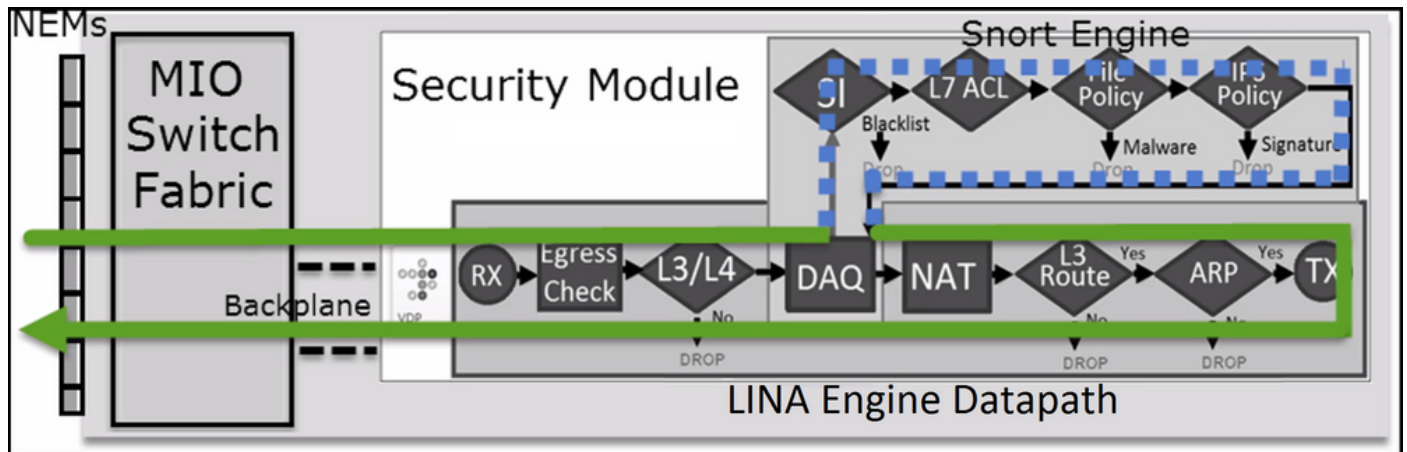
Flow Counters:

Fast-Forwarded Flows	1
Blacklisted Flows	0

Miscellaneous Counters:

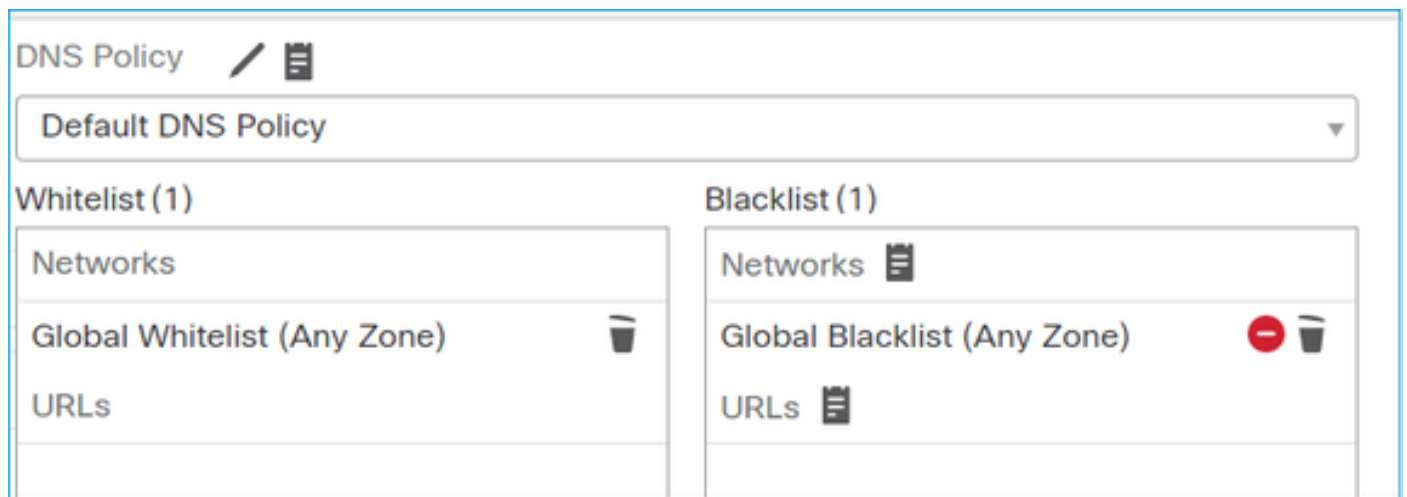
Start-of-Flow events	0
End-of-Flow events	1
Denied flow events	0
Frames forwarded to Snort before drop	0
Inject packets dropped	0

Flusso del pacchetto con la regola di attendibilità. Alcuni pacchetti sono ispezionati dal motore Snort mentre gli altri vengono elaborati dal motore LINA:



Scenario 2. Azione trust ACP (senza SI, QoS e criteri di identità)

Se si desidera che l'FTD applichi i controlli di intelligence di sicurezza (SI) a tutti i flussi, si è già abilitato a livello di ACP ed è possibile specificare le origini SI (talos, feed, elenchi e così via). Al contrario, se si desidera disabilitare questi controlli, disattivare SI per le reti a livello globale per ACP, per URL e per DNS. La funzionalità SI per reti e URL è disabilitata come mostrato nell'immagine:



In questo caso, la regola di attendibilità viene applicata al motore LINA come trust:

```
> show access-list
```

```
...  
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1  
access-list CSM_FW_ACL_ line 10 advanced-trust ip host 192.168.1.40 host 192.168.2.40 rule-id  
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
```

Nota: A partire dalla versione 6.2.2 FTD supporta TID. TID funziona in modo simile a SI, ma se la funzionalità SI è disabilitata, non "forza" il reindirizzamento del pacchetto al motore Snort per ispezionarlo.

Verificare gli effetti di questa azione.

Stabilire una connessione HTTP tra l'host A (192.168.1.40) e l'host B (192.168.2.40). Poiché si tratta di un FP4100 e supporta Flow Offload nell'hardware, si verificano le seguenti situazioni:

- Alcuni pacchetti vengono inoltrati tramite il motore LINA dell'FTD, gli altri pacchetti del flusso vengono trasferiti alla SmartNIC (acceleratore hardware).
- Nessun pacchetto viene inoltrato al motore Snort

Nella tabella delle connessioni LINA FTD viene visualizzato il contrassegno 'o', che indica che il flusso è stato scaricato su hardware. Si noti inoltre l'assenza delnflag, che sta per "no Snort redirection" (nessun reindirizzamento a Snort):

```
firepower# show conn
1 in use, 15 most used
```

```
TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:32809, idle 0:00:00, bytes 949584, flags UIOo
```

Le statistiche di Snort mostrano solo gli eventi all'inizio e alla fine della sessione:

```
firepower# show snort statistics
```

Packet Counters:

Passed Packets	0
Blocked Packets	0
Injected Packets	0
Packets bypassed (Snort Down)	0
Packets bypassed (Snort Busy)	0

Flow Counters:

Fast-Forwarded Flows	0
Blacklisted Flows	0

Miscellaneous Counters:

Start-of-Flow events	1
End-of-Flow events	1

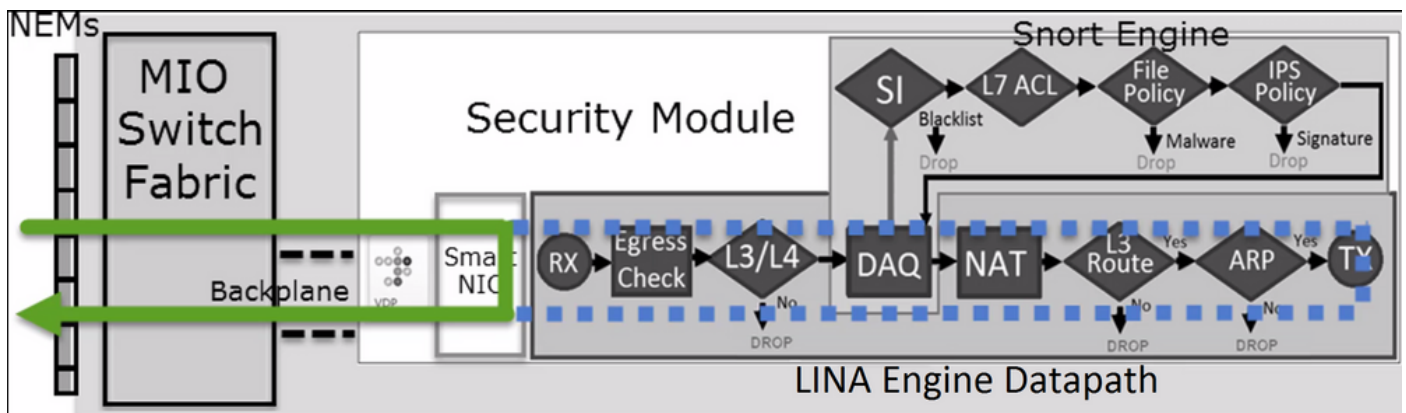
I log di LINA dell'FTD mostrano che per ciascuna sessione sono stati trasferiti nell'hardware 2 flussi (uno per ogni direzione):

```
Sep 27 2017 20:16:05: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Sep 27 2017 20:16:05: %ASA-6-302013: Built inbound TCP connection 25384 for
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
```


Sep 27 2017 20:16:05: %ASA-6-302014: Teardown TCP connection 25384 for INSIDE:192.168.1.40/32809 to OUTSIDE:192.168.2.40/80 duration 0:00:00 bytes 1055048 TCP FINs

Sep 27 2017 20:16:05: %ASA-7-609002: Teardown local-host INSIDE:192.168.1.40 duration 0:00:00

Flusso pacchetto con regola di trust distribuita come **trust** in LINA. Alcuni pacchetti vengono ispezionati da LINA, gli altri pacchetti vengono trasferiti alla SmartNIC (FP4100/FP9300):

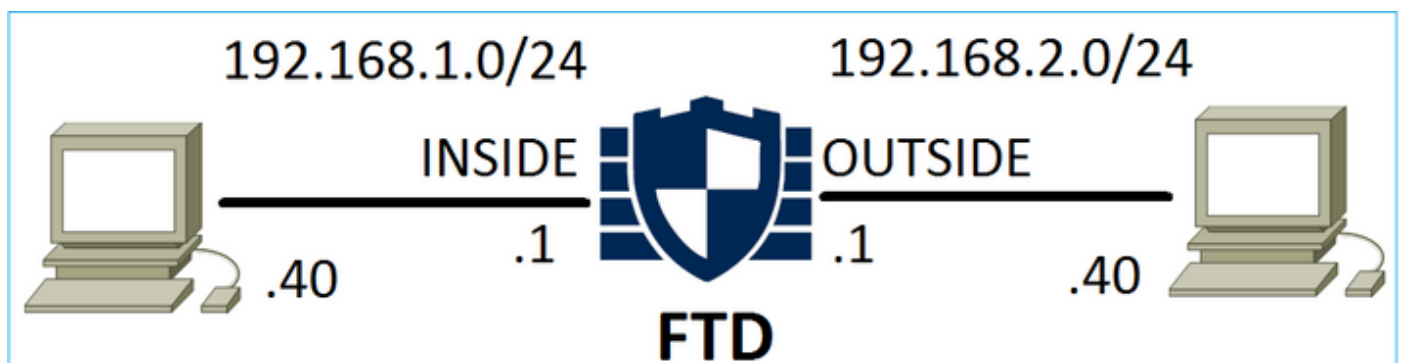


Scenari d'uso

- È necessario utilizzare **Trust** azione quando si desidera che il motore Snort controlli solo pochi pacchetti (ad esempio rilevamento applicazioni, controllo SI) e il resto del flusso venga scaricato sul motore LINA
- Se si utilizza FTD su FP4100/9300 e si desidera che il flusso ignori completamente l'ispezione Snort, prendere in considerazione la regola Prefiltro con **Fastpath** (vedere la sezione correlata in questo documento)

Azione di blocco della policy di prefiltro

Supponiamo di avere questa topologia:



Supponiamo anche di avere la seguente policy:

Access Control ▶ Prefilter										
Network Discovery			Application Detectors			Correlation		Actions ▼		
FTD_Prefilter										
Enter Description										
Rules										
					Add Tunnel Rule		Add Prefilter Rule		Search Rules	
#	Name	Rule T...	...	De	Source	Destination	Source	Destinat...	VLAN Tag	Action
			...	Ini	Networks	Networks	Port	Port		
1	Prefilter1	Prefilter	any any		192.168.1.40	192.168.2.40	any	any	any	Block

Questo è il criterio distribuito nel motore Snort FTD (file ngfw.rules):

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268437506 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any (tunnel -1
```

In LINA:

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id
268437506 event-log flow-start (hitcnt=0) 0x76476240
```

sui pacchetti virtuali, la traccia mostra come il pacchetto sia stato eliminato da LINA e non sia mai stato inoltrato a Snort:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id 268437506
event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ remark rule-id 268437506: RULE: Prefilter1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Le statistiche di Snort mostrano:

```
firepower# show snort statistics
```

```

Packet Counters:
  Passed Packets                0
  Blocked Packets              0
  Injected Packets             0
  Packets bypassed (Snort Down) 0
  Packets bypassed (Snort Busy) 0

Flow Counters:
  Fast-Forwarded Flows        0
  Blacklisted Flows          0

Miscellaneous Counters:
  Start-of-Flow events        0
  End-of-Flow events          0
  Denied flow events        1

```

Il comando show ASP drop di LINA mostra:

```

firepower# show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)          1

```

Scenari d'uso

È possibile utilizzare una regola di blocco del prefiltro quando si desidera bloccare il traffico in base alle condizioni L3/L4 e senza eseguire un'ispezione diretta del traffico.

Azione Fastpath della policy di prefiltro

Supponiamo di avere questa regola della policy di prefiltro:

#	Name	Rule T...	Sot Int	De Int	Source Networks	Destination Networks	Source Port	Destinati...	VLAN Tag	Action
1	Prefilter1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	TCP (6):80	any	→ Fastpath

Questo è il criterio distribuito nel motore Snort FTD:

```
268437506 fastpath any any any any any any any (log dcfoward flowend) (tunnel -1)
```

Nel motore LINA dell'FTD:

```

access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced trust tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268437506 event-log flow-end (hitcnt=0) 0xf3410b6f

```

Verificare gli effetti di questa azione.

Quando l'host A (192.168.1.40) cerca di stabilire una connessione HTTP con l'host B (192.168.2.40), alcuni pacchetti passano attraverso LINA mentre il resto del traffico viene trasferito alla SmartNIC. In questo caso `system support trace` con `firewall-engine-debug` enabled visualizza:

```
> system support trace
```

```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages
```

```
192.168.1.40-32840 > 192.168.2.40-80 6 AS 1 I 8 Got end of flow event from hardware with flags
04000000
```

I log LINA mostrano il flusso trasferito:

```
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host OUTSIDE:192.168.2.40
Oct 01 2017 14:36:51: %ASA-6-302013: Built inbound TCP connection 966 for
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32840 (192.168.1.40/32840)
```

LINA acquisisce show 8 pacchetti attraverso:

```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40
```

```
firepower# show capture CAPI
```

8 packets captured

```
1: 14:45:32.700021 192.168.1.40.32842 > 192.168.2.40.80: S 3195173118:3195173118(0) win 2920
<mss 1460,sackOK,timestamp 332569060 0>
2: 14:45:32.700372 192.168.2.40.80 > 192.168.1.40.32842: S 184794124:184794124(0) ack
3195173119 win 2896 <mss 1380,sackOK,timestamp 332567732 332569060>
3: 14:45:32.700540 192.168.1.40.32842 > 192.168.2.40.80: P 3195173119:3195173317(198) ack
184794125 win 2920 <nop,nop,timestamp 332569060 332567732>
4: 14:45:32.700876 192.168.2.40.80 > 192.168.1.40.32842: . 184794125:184795493(1368) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
5: 14:45:32.700922 192.168.2.40.80 > 192.168.1.40.32842: P 184795493:184796861(1368) ack
```

```

3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
 6: 14:45:32.701425 192.168.2.40.80 > 192.168.1.40.32842: FP 184810541:184810851(310) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569061>
 7: 14:45:32.701532 192.168.1.40.32842 > 192.168.2.40.80: F 3195173317:3195173317(0) ack
184810852 win 2736 <nop,nop,timestamp 332569061 332567733>
 8: 14:45:32.701639 192.168.2.40.80 > 192.168.1.40.32842: . ack 3195173318 win 2697
<nop,nop,timestamp 332567734 332569061>

```

Le statistiche di flow-offload nell'FTD mostrano 22 pacchetti trasferiti all'hardware:

```

firepower# show flow-offload statistics
Packet stats of port : 0
Tx Packet count      :                22
Rx Packet count      :                22
Dropped Packet count :                0
VNIC transmitted packet :                22
VNIC transmitted bytes :              15308
VNIC Dropped packets  :                0
VNIC erroneous received :                0
VNIC CRC errors       :                0
VNIC transmit failed  :                0
VNIC multicast received :                0

```

È inoltre possibile utilizzare il `show flow-offload flow` per visualizzare informazioni aggiuntive correlate ai flussi scaricati. Di seguito è riportato un esempio:

```

firepower# show flow-offload flow
Total offloaded flow stats: 2 in use, 4 most used, 20% offloaded, 0 collisions
TCP intf 103 src 192.168.1.40:39301 dest 192.168.2.40:20, static, timestamp 616063741, packets
33240, bytes 2326800
TCP intf 104 src 192.168.2.40:20 dest 192.168.1.40:39301, static, timestamp 616063760, packets
249140, bytes 358263320
firepower# show conn
5 in use, 5 most used
Inspect Snort:
  preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 0 most in effect

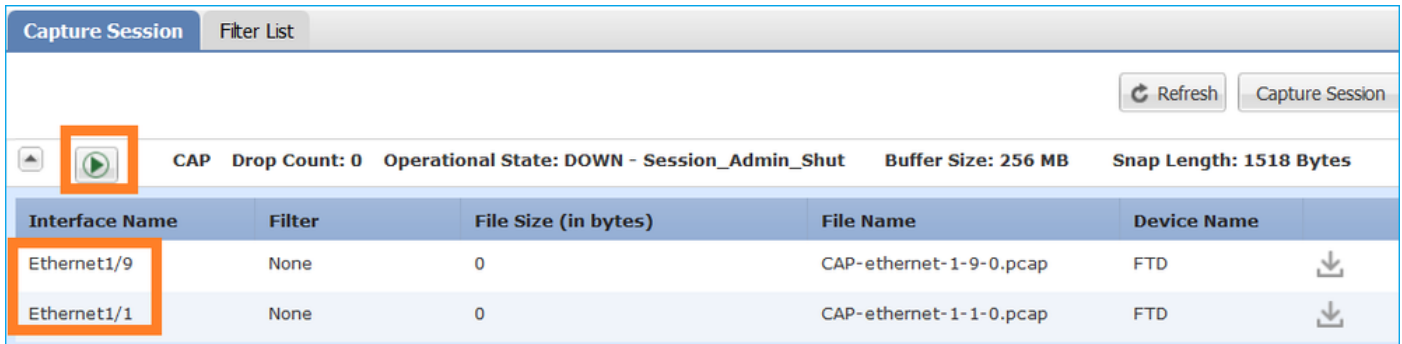
TCP OUTSIDE 192.168.2.40:21 INSIDE 192.168.1.40:40988, idle 0:00:00, bytes 723, flags UIO
TCP OUTSIDE 192.168.2.40:21 INSIDE 192.168.1.40:40980, idle 0:02:40, bytes 1086, flags UIO
TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:49442, idle 0:00:00, bytes 86348310, flags UIO
N1
TCP OUTSIDE 192.168.2.40:20 INSIDE 192.168.1.40:39301, idle 0:00:00, bytes 485268628, flags Uo
<- offloaded flow
TCP OUTSIDE 192.168.2.40:20 INSIDE 192.168.1.40:34713, idle 0:02:40, bytes 821799360, flags
UFRIO

```

- La percentuale è basata sul 'show conn' uscita. Ad esempio, se 5 conns in totale passano attraverso il motore LINA FTD e 1 di essi viene scaricato, il 20% viene indicato come scaricato
- Il limite massimo di sessioni scaricate dipende dalla versione del software (ad esempio, ASA 9.8.3 e FTD 6.2.3 supportano 4 milioni di flussi di offload bidirezionali (o 8 milioni unidirezionali)
- Se il numero di flussi scaricati raggiunge il limite (ad esempio, 4 milioni di flussi bidirezionali), non viene eseguito lo scaricamento delle nuove connessioni finché le connessioni correnti non vengono rimosse dalla tabella scaricata

Per visualizzare tutti i pacchetti sull'FP4100/9300 che passano attraverso l'FTD (trasferiti + LINA),

è necessario avviare una sessione di acquisizione al livello dello chassis, come mostrato nell'immagine:



Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/9	None	0	CAP-ethernet-1-9-0.pcap	FTD
Ethernet1/1	None	0	CAP-ethernet-1-1-0.pcap	FTD

L'acquisizione del backplane dello chassis mostra entrambe le direzioni. A causa dell'architettura di acquisizione FXOS (2 punti di acquisizione per direzione), ogni pacchetto viene mostrato **due volte** come mostrato nell'immagine:

Statistiche pacchetti:

- Il totale dei pacchetti che passa tramite l'FTD è 30
- I pacchetti che passano attraverso il motore LINA dell'FTD sono 8
- I pacchetti trasferiti all'acceleratore hardware SmartNIC sono 22

Nel caso di una piattaforma diversa da FP4100/FP9300, tutti i pacchetti vengono gestiti dal motore LINA poiché il flow-offload non è supportato (notare l'assenza del flag **o**):

```
FP2100-6# show conn addr 192.168.1.40
```

```
33 in use, 123 most used
```

```
Inspect Snort:
```

```
preserve-connection: 0 enabled, 0 in effect, 2 most enabled, 0 most in effect
```

```
TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:50890, idle 0:00:09, bytes 175, flags UxIO
```

I syslog di LINA mostrano solo gli eventi iniziali e finali della connessione:

```
FP2100-6# show log | i 192.168.2.40
```

```
Jun 21 2020 14:29:44: %FTD-6-302013: Built inbound TCP connection 6914 for
```

```
INSIDE:192.168.1.40/50900 (192.168.11.101/50900) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
```

```
Jun 21 2020 14:30:30: %FTD-6-302014: Teardown TCP connection 6914 for INSIDE:192.168.1.40/50900
```

```
to OUTSIDE:192.168.2.40/80 duration 0:00:46 bytes 565 TCP FINs from OUTSIDE
```

Scenari d'uso

- Utilizzo **Prefilter Fastpath** quando si desidera ignorare completamente l'ispezione Snort. In genere, questa azione è utile quando i flussi contengono volumi elevati di dati che si riconoscono come attendibili, ad esempio backup, trasferimenti di database, ecc.
- Sugli accessori FP4100/9300, **Fastpath** L'azione attiva il flow-offload e solo pochi pacchetti passano attraverso il motore LINA FTD. Il resto del traffico viene gestito dalla SmartNIC che riduce la latenza.

Azione Fastpath della policy di prefiltro (inline-set)

Se viene applicata un'azione Fastpath del criterio Prefiltro al traffico che attraversa un inline-set (interfacce NGIPS), è necessario tenere in considerazione i seguenti punti:

- La regola viene applicata al motore LINA come `trust` azione
- Il flusso non viene ispezionato dal motore Snort.
- La funzionalità Flow Offload non è supportata dalle interfacce NGIPS, quindi non si verificherà alcun trasferimento del flusso (acceleratore hardware).

Di seguito è riportato un esempio di traccia di un pacchetto nel caso dell'azione Prefilter Fastpath applicata a un set in linea:

```
firepower# packet-tracer input inside tcp 192.168.1.40 12345 192.168.1.50 80 detailed
```

```
Phase: 1
```

```
Type: NGIPS-MODE
```

```
Subtype: ngips-mode
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied
```

```
Forward Flow based lookup yields rule:
```

```
in id=0x2ad7ac48b330, priority=501, domain=ips-mode, deny=false
```

```
hits=2, user_data=0x2ad80d54abd0, cs_id=0x0, flags=0x0, protocol=0
```

```
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
```

```
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
```

```
input_ifc=inside, output_ifc=any
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype: log
```

```
Result: ALLOW
```

```
Config:
```

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced trust ip object 192.168.1.0 object 192.168.1.0 rule-id
```

```
268438531 event-log flow-end
```

```
access-list CSM_FW_ACL_ remark rule-id 268438531: PREFILTER POLICY: PF1
```

```
access-list CSM_FW_ACL_ remark rule-id 268438531: RULE: 1
```

```
Additional Information:
```

```
Forward Flow based lookup yields rule:
```

```
in id=0x2ad9f9f8a7f0, priority=12, domain=permit, trust
```

```
hits=1, user_data=0x2ad9b23c5d40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
```

```
src ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any
```

```
dst ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
```

```
input_ifc=any, output_ifc=any
```

```
Phase: 3
```

```
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Ingress interface inside is in NGIPS inline mode.
```

```
Egress interface outside is determined by inline-set configuration
```

```
Phase: 4
```

```
Type: FLOW-CREATION
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
New flow created with id 7, packet dispatched to next module
```

```

Module information for forward flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

```

```

Module information for reverse flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

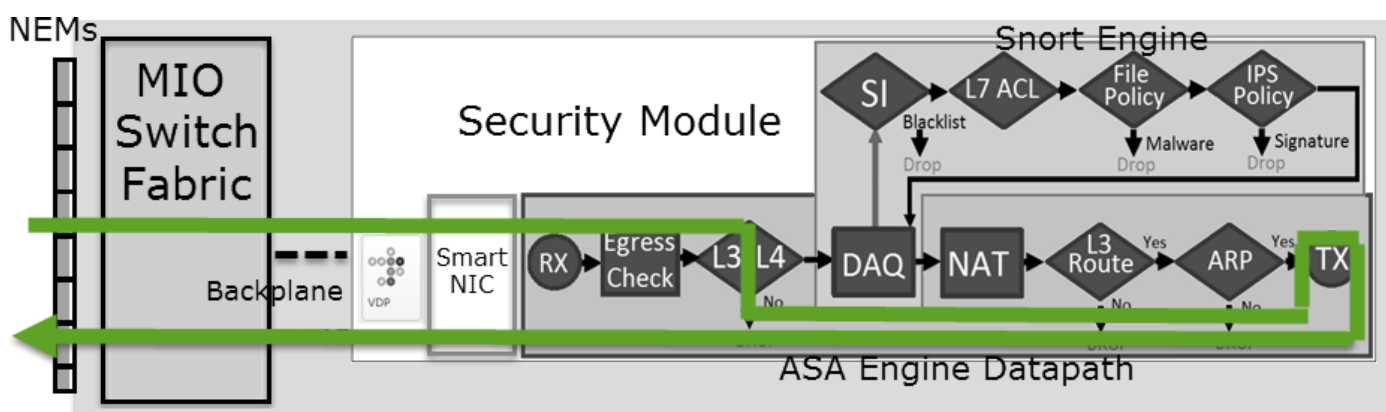
```

```

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow

```

Questa è la rappresentazione visiva del percorso del pacchetto:



Azione Fastpath della policy di prefiltro (inline-set con tap)

Uguale allo scenario inline-set.

Azione di analisi della policy di prefiltro

Scenario 1. Analisi di prefiltro con regola di blocco ACP

Supponiamo di avere una policy di prefiltro con la regola Analyze (Analisi) come mostrato nell'immagine:

Access Control > Prefilter										
Network Discovery										
Application Detectors										
Correlation										
Actions										
Prefilter_Policy1										
Enter Description										
Rules										
+ Add Tunnel Rule + Add Prefilter Rule Search R										
#	Name	Rule T...	Source Interfac...	Destinat...	Source Networks	Destination Networks	Source Port	Destinat...	VLAN Tag	Action
1	Prefilter_Rule1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	any	any	Analyze

Il punto ACP contiene solo la regola predefinita impostata su Block All Traffic come mostrato nell'immagine:

Access Control ▶ Access Control Network Discovery Application Detectors Correlation Actions ▼

ACP1
Enter Description

Prefilter Policy: **Prefilter_Policy1** SSL Policy: None

Rules Security Intelligence HTTP Responses Advanced

Show Rule Conflicts

#	Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Action
▼ Mandatory - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
▼ Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action												Access Control: Block All Traffic	

Questo è il criterio distribuito nel motore Snort FTD (file ngfw.rules):

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268435460 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any (tunnel -1)
268435459 allow any any 1025-65535 any any 3544 any 17 (tunnel -1)
268435459 allow any any 3544 any any 1025-65535 any 17 (tunnel -1)
268435459 allow any any any any any any any any 47 (tunnel -1)
268435459 allow any any any any any any any any 41 (tunnel -1)
268435459 allow any any any any any any any any 4 (tunnel -1)
# End of tunnel and priority rules.
# Start of AC rule.
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

Questa è la policy implementata nel motore LINA dell'FTD:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=0) 0xb788b786
```

Verificare gli effetti di questa azione.

Packet-tracer mostra che il pacchetto è consentito da LINA e viene inoltrato al motore Snort (a causa di permit) e Snort Engine restituisce un Block verdetto poiché l'azione predefinita di AC è corrispondente.

Nota: Snort non valuta il traffico in base alle regole del tunnel.

Quando si traccia un pacchetto, viene visualizzato quanto segue:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
```

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460

access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1

access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

...
Phase: 14

Type: SNORT

Subtype:

Result: DROP

Config:

Additional Information:

Snort Trace:

Packet: ICMP

AppID: service ICMP (3501), application unknown (0)

Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,

icmpType 8, icmpCode 0

Firewall: block rule, id 268435458, drop

Snort: processed decoder alerts or actions queue, drop

NAP id 1, IPS id 0, **Verdict BLOCKLIST, Blocked by Firewall**

Snort Verdict: **(block-list) block list this flow**

Result:

input-interface: INSIDE

input-status: up

input-line-status: up

output-interface: OUTSIDE

output-status: up

output-line-status: up

Action: drop

Drop-reason: (firewall) Blocked by the firewall preprocessor

Scenario 2. Analisi di prefiltro con regola di autorizzazione ACP

Se l'obiettivo è autorizzare il passaggio del pacchetto tramite l'FTD, è necessario aggiungere una regola nella policy ACP. L'azione può essere Consenti o Considera attendibile, a seconda dell'obiettivo. Se ad esempio si desidera applicare un'ispezione L7, è necessario utilizzare **Allow** come mostrato nell'immagine:

The screenshot shows the Cisco FTD GUI for configuring an Access Control Policy (ACP1). The 'Rules' tab is selected, showing a table of rules. Rule 1, named 'Rule1', is configured with source and destination networks 192.168.1.40 and 192.168.2.40, and an action of 'Allow'. The 'Default Action' is set to 'Access Control: Block All Traffic'.

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

La policy implementata nel motore Snort dell'FTD:

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

Nel motore LINA:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=1) 0xb788b786
```

Verificare gli effetti di questa azione.

Packet-tracer indica che il pacchetto soddisfa la regola 268435460 in LINA e 268435461 nel motore Snort:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
  This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: allow rule, id 268435461, allow
NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
...
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

Scenario 3. Analisi di prefiltro con regola di attendibilità ACP

Nel caso la policy ACP contenga la regola di attendibilità Trust (Considera attendibile), si ha la situazione descritta nell'immagine:

Access Control ▸ Access Control Network Discovery Application Detectors Correlation Actions ▾

ACP1

Enter Description

Prefilter Policy: [Prefilter_Policy1](#) SSL Policy: [None](#) Identif...

Inheritance Se...

Rules Security Intelligence HTTP Responses Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rul...

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
▼ Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	→ Trust
▼ Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action												Access Control: Block All Traffic	

Snort:

```
# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

LINA:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=2) 0xb788b786
```

Tenere presente che, poiché l'interfaccia utente è attivata per impostazione predefinita, la regola Trust viene distribuita come permit su LINA in modo che almeno alcuni pacchetti vengano reindirizzati al motore Snort per l'ispezione.

Verificare gli effetti di questa azione.

Packet-tracer mostra che il motore Snort Permitt elenca il pacchetto ed essenzialmente scarica il resto del flusso su LINA:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
  This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
```

Additional Information:

Snort Trace:

Packet: ICMP

AppID: service ICMP (3501), application unknown (0)

Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType 8, icmpCode 0

Firewall: **trust/fastpath rule, id 268435461, allow**

NAP id 1, IPS id 0, **Verdict PERMITLIST**

Snort Verdict: (fast-forward) fast forward this flow

...

Result:

input-interface: INSIDE

input-status: up

input-line-status: up

output-interface: OUTSIDE

output-status: up

output-line-status: up

Action: allow

Scenario 4. Analisi di prefiltro con regola di attendibilità ACP

In questo scenario, la funzionalità SI è stata disabilitata manualmente.

La regola viene implementata nel motore Snort come segue:

```
# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

In LINA la regola viene implementata come trust. Un pacchetto comunque corrisponde alla regola di autorizzazione (vedere il conteggio delle corrispondenze ACE) distribuita a causa della regola Analizza prefiltro e il pacchetto viene ispezionato dal motore Snort:

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=3) 0xb788b786
...
access-list CSM_FW_ACL_ line 13 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
...
access-list CSM_FW_ACL_ line 16 advanced deny ip any any rule-id 268435458 event-log flow-start
(hitcnt=0) 0x97aa021a
```

Verificare gli effetti di questa azione.

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

...

Phase: 14

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Trace:

Packet: ICMP

AppID: service ICMP (3501), application unknown (0)

Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType 8, icmpCode 0

Firewall: **trust/fastpath rule, id 268435461, allow**

NAP id 1, IPS id 0, **Verdict PERMITLIST**

Snort Verdict: (fast-forward) fast forward this flow

...

Result:

input-interface: INSIDE

input-status: up

input-line-status: up

output-interface: OUTSIDE

output-status: up

output-line-status: up

Action: allow

Considerazioni principali

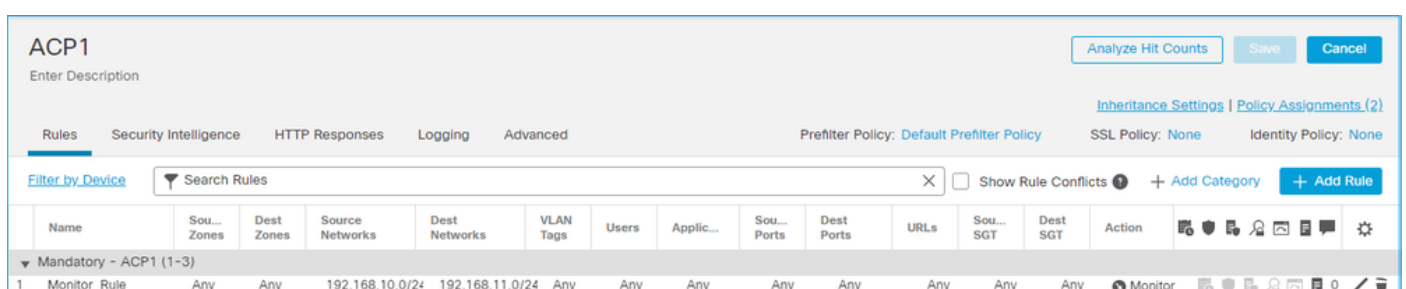
- OSPF (Open Shortest Path First) **Analyze** L'azione viene distribuita come regola di autorizzazione nel motore LINA. Questo ha un effetto sul pacchetto da inoltrare al motore Snort per l'ispezione
- OSPF (Open Shortest Path First) **Analyze** L'azione non distribuisce alcuna regola nel motore Snort, pertanto è necessario verificare di configurare una regola in ACP corrispondente in Snort
- Dipende dalla regola ACP distribuita nel motore Snort (**block** e **allow** e **fastpath**) Snort non permette di caricare tutti i pacchetti

Scenari d'uso

- Un caso di utilizzo di **Analyze** L'azione viene eseguita quando si dispone di una regola Fastpath ampia nel criterio Prefiltro e si desidera inserire alcune eccezioni per flussi specifici in modo che vengano controllati da Snort

Azione di monitoraggio della policy ACP

Una regola di monitoraggio configurata come appare sull'interfaccia utente dell'FMC:



Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Sou... Ports	Dest Ports	URLs	Sou... SGT	Dest SGT	Action	Icons
Mandatory - ACP1 (1-3)														
1 Monitor_Rule	Any	Any	192.168.10.0/24	192.168.11.0/24	Any	Any	Any	Any	Any	Any	Any	Any	Monitor	Icons

La regola di monitoraggio viene distribuita nel motore LINA FTD come **permit** e al motore Snort come **audit** azione.

```
firepower# show access-list
```

```
...  
access-list CSM_FW_ACL_ line 10 advanced permit ip 192.168.10.0 255.255.255.0 192.168.11.0  
255.255.255.0 rule-id 268438863 (hitcnt=0) 0x61bbaf0c
```

La regola Snort:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules  
...  
# Start of AC rule.  
268438863 audit any 192.168.10.0 24 any any 192.168.11.0 24 any any any (log dcfoward flowend)  
# End rule 268438863
```

Considerazioni principali

- La regola di monitoraggio non consente l'eliminazione o l'autorizzazione del traffico ma genera un evento di connessione. Il pacchetto viene verificato con le regole successive e quindi autorizzato o scartato.
- Gli eventi di connessione FMC mostrano che il pacchetto soddisfa 2 regole:

	First Packet ×	Last Packet ×	Action ×	Initiator IP ×	Responder IP ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	Access Control Policy ×	Access Control Rule ×
▼	2020-06-20 22:17:40	2020-06-20 22:17:43	Trust	192.168.10.50	192.168.11.50	41920 / tcp	80 (http) / tcp	ACP1	trust_L3-L4_Monitor_Rule

System support trace L'output mostra che i pacchetti soddisfano entrambe le regole:

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y  
Please specify an IP protocol: tcp  
Please specify a client IP address: 192.168.10.50  
Please specify a client port:  
Please specify a server IP address: 192.168.11.50  
Please specify a server port:  
Monitoring packet tracer and firewall debug messages
```

```
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 419031630  
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session  
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application  
unknown (0)  
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 new firewall session  
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 Starting AC with minimum 2, 'Monitor_Rule',  
and IPProto first with zone s -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source  
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0, svc 0, payload 0,  
client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
```

```
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 2, 'Monitor_Rule', action Audit
```

```
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 3, 'trust_L3-L4', action Trust
```

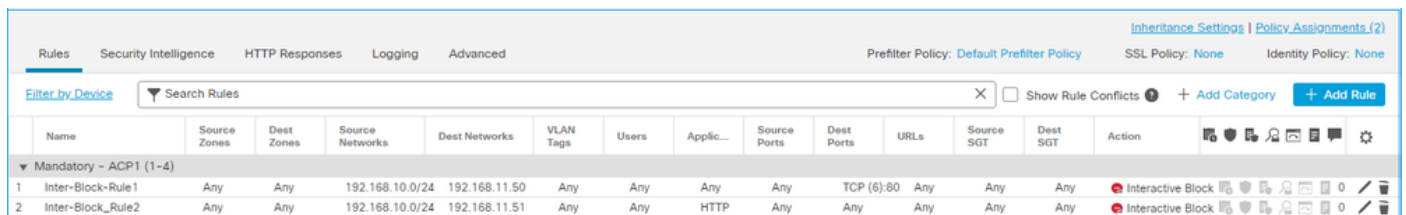
```
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 MidRecovery data sent for rule id: 268438858,rule_action:3, rev id:1078 02206, rule_match flag:0x2
```

Scenari d'uso

Utilizzato per monitorare l'attività di rete e generare un evento di connessione.

Azione di blocco interattivo della policy ACP

Una regola di blocco interattivo configurata sull'interfaccia utente dell'FMC:



Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
Mandatory - ACP1 (1-4)													
1 Inter-Block-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Interactive Block
2 Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Interactive Block

La regola di blocco interattivo viene distribuita nel motore LINA FTD come **permit** e al motore Snort come regola di bypass:

```
firepower# show access-list
```

```
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=3) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Motore Snort:

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
...
# Start of AC rule.
268438864 bypass any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 bypass any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

La regola di blocco interattivo avverte l'utente che la destinazione non può essere raggiunta.

Access Denied

You are attempting to access a forbidden site.


You may continue to the site by clicking on the button below.

Note: You must have cookies enabled in your browser to continue.

Consult your system administrator for details.

Continue

Per impostazione predefinita, il firewall consente di ignorare il blocco per 600 secondi:

Rules	Security Intelligence	HTTP Responses	Logging	Advanced
General Settings 				
Maximum URL characters to store in connection events				1024
Allow an Interactive Block to bypass blocking for (seconds)				600
Retry URL cache miss lookup				Yes
Enable Threat Intelligence Director				Yes
Inspect traffic during policy apply				Yes

Nella **system support trace** si può vedere che inizialmente il firewall blocca il traffico e mostra la pagina blocco:

```
> system support trace
```

```
...
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 983273680, ack
2014879580
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 match rule order 2, 'Inter-Block-Rule1',
action Interactive
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 bypass action sending HTTP interactive
response of 1093 bytes
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-
Block-Rule1', drop
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 22, NAP id 1, IPS id 0, Verdict
BLACKLIST
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ
```

Dopo che l'utente ha selezionato **Continue** (o aggiorna la pagina del browser) il comando debug mostra che i pacchetti sono consentiti dalla stessa regola che imita e **Allow** azione:

```
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1357413630, ack 2607625293
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application unknown (0)
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 Starting AC with minimum 2, 'Inter-Block-Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589, misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 match rule order 2, 'Inter-Block-Rule1', action Interactive
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 bypass action interactive bypass
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 allow action
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1', allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-Block-Rule1', allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 8, NAP id 1, IPS id 0, Verdict PASS
```

Scenari d'uso

Mostrare una pagina di avviso agli utenti Web dando loro la possibilità di continuare.

Azione di blocco interattivo con reset della policy ACP

La regola di blocco interattivo con reset configurata sull'interfaccia utente dell'FMC:

Name	Source Zones	Destination Zones	Source Networks	Destination Networks	VLAN Tags	Users	Applications	Source Ports	Destination Ports	URLs	Source SGT	Destination SGT	Action	Tools
1 Inter-Block-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Interactive Block with reset	[Icons]
2 Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Interactive Block with reset	[Icons]

Il blocco interattivo con regola di reimpostazione viene distribuito nel motore LINA FTD come **permit** e per ruotare il motore come regola di ripristino:

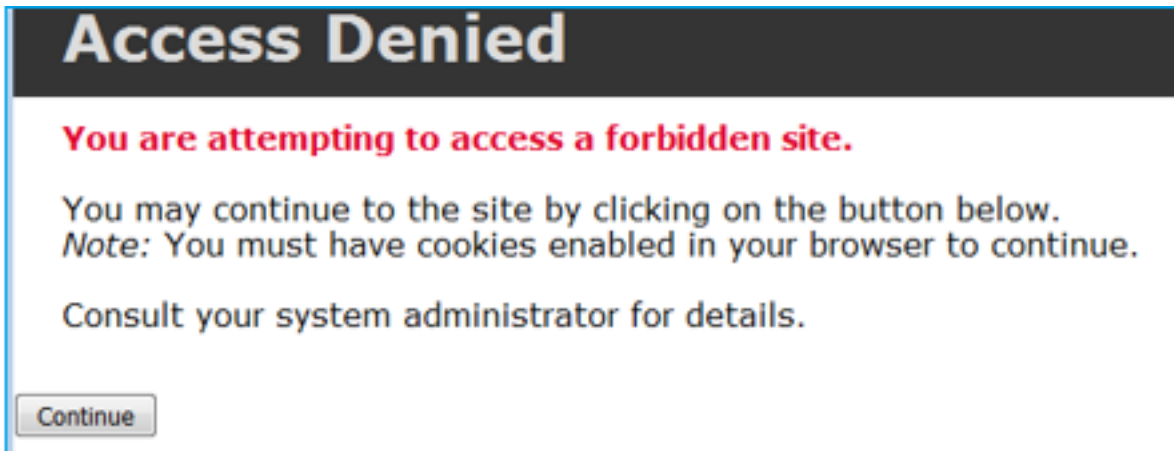
```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=13) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Motore Snort:

```
# Start of AC rule.
268438864 intreset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
```

```
# End rule 268438864
268438865 intreset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

Analogamente al Blocco con Reset, l'utente può selezionare Continue opzione:



Nel debug di Snort, l'azione mostrata nel reset interattivo:

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.52
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3232128039
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 new firewall session
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0, svc 0, payload 0, client 0,
misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 MidRecovery data sent for rule id:
268438864,rule_action:8, rev id:1099034206, rule_match flag:0x0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 HitCount data sent for rule id: 268438864,
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2228213518, ack
3232128040
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
```

```
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 bypass action sending HTTP interactive
response of 1093 bytes
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-
Block-Rule1', drop
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
BLACKLIST
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ
```

A questo punto, la pagina del blocco viene visualizzata all'utente finale. Se l'utente seleziona **Continue** (o aggiorna la pagina web) la stessa regola corrisponde che questa volta consente il traffico attraverso:

```
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1593478294, ack
3135589307
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 bypass action interactive bypass
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 allow action
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3135589307, ack
1593478786
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS
```

La regola di blocco interattivo con reset invia una richiesta TCP RST al traffico non Web:

```
firepower# show cap CAPI | i 11.50
 2: 22:13:33.112954      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: S
3109534920:3109534920(0) win 29200 <mss 1460,sackOK,timestamp 3745225378 0,nop,wscale 7>
 3: 22:13:33.113626      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: S
3422362500:3422362500(0) ack 3109534921 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
53252448 3745225378>
 4: 22:13:33.113824      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362501 win 229 <nop,nop,timestamp 3745225379 53252448>
 5: 22:13:33.114953      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362501:3422362543(42) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 6: 22:13:33.114984      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362543:3422362549(6) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 7: 22:13:33.114984      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362549:3422362570(21) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 8: 22:13:33.115182      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362543 win 229 <nop,nop,timestamp 3745225381 53252448>
 9: 22:13:33.115411      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362549 win 229 <nop,nop,timestamp 3745225381 53252448>
10: 22:13:33.115426      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362570 win 229 <nop,nop,timestamp 3745225381 53252448>
12: 22:13:34.803699      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: P
3109534921:3109534931(10) ack 3422362570 win 229 <nop,nop,timestamp 3745227069 53252448>
13: 22:13:34.804523      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: R
3422362570:3422362570(0) ack 3109534931 win 0
```

Connessioni secondarie FTD e Fori

Nelle release precedenti (ad esempio 6.2.2, 6.2.3, ecc.), il motore Snort non apre fori per le connessioni secondarie (ad esempio i dati FTD) se si utilizza il Trust azione. Nelle release più recenti, questo comportamento viene modificato e il motore Snort apre dei fori anche con Trust azione.

Linee guida della regola FTD

- Usare le regole Fastpath della policy di prefiltro per flussi con elevati volumi di dati per diminuire la latenza.
- Usare le regole Block della policy di prefiltro per il traffico che deve essere bloccato in base alle condizioni L3/L4.
- Usare le regole Trust della policy ACP se si desidera ignorare molti dei controlli Snort, ma comunque sfruttare altre funzionalità, quali policy delle identità, QoS, SI, rilevamento delle applicazioni, filtro URL.
- Inserire le regole che incidono meno sulle prestazioni del firewall all'inizio della policy ACP facendo riferimento a queste linee guida:

1. Regole Block (layer 1-4) - Policy di prefiltro
2. Regole Allow (layer 1-4) - Fastpath della policy di prefiltro
3. Regole Block della policy ACP (layer 1-4)
4. Regole Trust (layer 1-4)
5. Regole Block (layer 5-7 - rilevamento delle applicazioni, filtro URL)
6. Regole Allow (layer 1-7 - rilevamento delle applicazioni, filtro URL, policy anti-

intrusione/policy di controllo file)

7. Regola Block (regola predefinita)

- Evitare registrazioni eccessive (registrare i dati all'inizio o alla fine ed evitare di registrarli contemporaneamente)
- Tenere sotto controllo il numero di regole usate nel motore LINA.

```
firepower# show access-list | include elements  
access-list CSM_FW_ACL; 7 elements; name hash: 0x4a69e3f3
```

Riepilogo

Azioni della policy di prefiltro

Rule Action (FMC UI)	LINA Action	Snort Action	Notes
Fastpath	Trust	Fastpath	Static Flow Offload to SmartNIC (4100/9300). No packets are sent to Snort engine.
Analyze	Permit	-	The ACP rules are checked. Few or all packets are sent to Snort engine for inspection. Traffic is allowed or dropped based on Snort engine verdict
Block (Prefilter)	Deny	-	Early drop by FTD LINA No packets are sent to Snort engine

Azioni della policy ACP

Rule Action (FMC UI)	Additional Conditions	LINA Action	Snort Action	Notes
Block	The rule matches L3/L4 conditions	Deny	Deny	
Block	The rule has L7 conditions	Permit	Deny	
Allow		Permit	Allow	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, or ID) enabled	Permit	Fastpath	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, and ID) disabled	Trust	Fastpath	Static Flow Offload (4100/9300)
Monitor		Permit	Audit	Monitor Rule doesn't drop or permit traffic, but it generates a Connection Event. The packet is checked against subsequent rules and it is either allowed or dropped
Block with reset		Permit	Reset	When a packet matches Block with reset rule FTD sends a TCP Reset packet or an ICMP Type 3 Code 13 Destination Unreachable (Administratively filtered) message
Interactive Block		Permit	Bypass	Interactive Block Rule prompts the user that the destination is forbidden If bypassed, by default, the firewall allows to bypass the block for 600 seconds
Interactive Block with reset		Permit	Intreset	Same as Interactive Block with the addition of a TCP RST in case of non-web traffic

Nota: A partire dal codice software 6.3 FTD L'offload dinamico del flusso può scaricare le connessioni che soddisfano criteri aggiuntivi, ad esempio i pacchetti attendibili che richiedono l'ispezione Snort. Per ulteriori dettagli, consultare la sezione "Offload di flussi di grandi dimensioni" nella Guida alla configurazione di Firepower Management Center.

Informazioni correlate

- [Regole della policy ACP nell'FTD](#)
- [Prefiltro e policy di prefiltro nell'FTD](#)
- [Analisi delle acquisizioni di Firepower Firewall per la risoluzione efficace dei problemi di rete](#)
- [Uso di capture e packet-tracer sui Firepower Threat Defense \(FTD\)](#)
- [Configurazione dei log sull'FTD tramite FMC](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)
- [Offload di flussi di grandi dimensioni](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).