

Fase 8 della risoluzione dei problemi del percorso dei dati di Firepower: Criteri di analisi della rete

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Risoluzione dei problemi relativi alla funzionalità dei criteri di analisi della rete](#)

[Utilizzo dello strumento "trace" per individuare le perdite del preprocessore \(solo FTD\)](#)

[Verifica configurazione di Protezione accesso alla rete](#)

[Visualizza impostazioni di Protezione accesso alla rete](#)

[Impostazioni di Protezione accesso alla rete che possono causare interruzioni invisibili all'utente](#)

[Verifica della configurazione back-end](#)

[Creazione di un Protezione accesso alla rete di destinazione](#)

[Analisi falsi positivi](#)

[Fasi di mitigazione](#)

[Dati da fornire a TAC](#)

Introduzione

Questo articolo fa parte di una serie di articoli che spiegano come risolvere in modo sistematico i problemi relativi al percorso dei dati nei sistemi Firepower per determinare se i componenti di Firepower possono influire sul traffico. Per informazioni sull'architettura delle piattaforme Firepower e per i collegamenti agli altri articoli sulla risoluzione dei problemi relativi al percorso dei dati, consultare l'[articolo Panoramica](#).

In questo articolo viene descritta l'ottava fase della risoluzione dei problemi relativi al percorso dati di Firepower, la funzionalità Criteri di analisi della rete.



Prerequisiti

- Questo articolo è applicabile a tutte le piattaforme Firepower. La funzione **trace** è disponibile solo nella versione 6.2.0 e successive del software per la piattaforma Firepower Threat Defense (FTD).
- Conoscenza di Snort open source è utile, anche se non richiesto. Per informazioni su Snort open source, visitare il sito <https://www.snort.org/>

Risoluzione dei problemi relativi alla funzionalità dei criteri di

analisi della rete

I criteri di analisi della rete contengono le impostazioni del preprocessore snort che eseguono controlli sul traffico in base all'applicazione identificata. I preprocessori sono in grado di eliminare il traffico in base alla configurazione. In questo articolo viene descritto come verificare la configurazione di Protezione accesso alla rete e verificare la presenza di rilasci del preprocessore.

Nota: Le regole per il preprocessore hanno un ID generatore (GID) diverso da '1' o '3' (ovvero 129, 119, 124). Per ulteriori informazioni sui mapping tra il GID e il preprocessore, vedere le [Guide alla configurazione di FMC](#).

Utilizzo dello strumento "trace" per individuare le perdite del preprocessore (solo FTD)

Lo strumento **System Support Trace** (Traccia supporto sistema) può essere utilizzato per rilevare le cadute eseguite a livello di preprocessore.

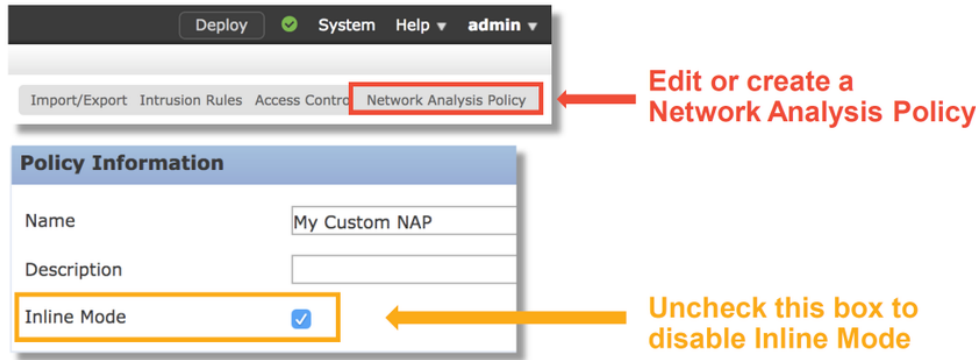
Nell'esempio seguente, il preprocessore di normalizzazione TCP ha rilevato un'anomalia. Di conseguenza, il traffico viene scartato in base alla regola **129:14**, che cerca i timestamp mancanti in un flusso TCP.

```
> system support trace
[omitted for brevity...]
172.16.111.226-51174 - 50.19.123.95-443 6 Packet: TCP, ACK, seq 3849839667, ack 1666843207
172.16.111.226-51174 - 50.19.123.95-443 6 Stream: TCP normalization error in timestamp, window, seq, ack, fin, flags, or unexpected data, drop
172.16.111.226-51174 - 50.19.123.95-443 6 ApplID: service unknown (0), application unknown (0)
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 I 0 Starting with minimum 3, 'block urls', 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
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
172.16.111.226-51174 > 50.19.123.95-443 6 AS 4 I 0 pending rule order 3, 'block urls', URL
172.16.111.226-51174 > 50.19.123.95-443 6 Firewall: pending rule-matching, 'block urls', pending URL
172.16.111.226-51174 > 50.19.123.95-443 6 Snort: processed decoder alerts or actions queue, drop
172.16.111.226-51174 > 50.19.123.95-443 6 IPS Event: gid 129, sid 14, drop
172.16.111.226-51174 > 50.19.123.95-443 6 NAP id 1, IPS id 0, Verdict BLOCK
172.16.111.226-51174 > 50.19.123.95-443 6 ==> Blocked by Stream
```

Nota: Sebbene il preprocessore **TCP Stream Configuration** scarti il traffico, è in grado di farlo perché è abilitato anche il preprocessore **Inline Normalization**. Per ulteriori informazioni sulla normalizzazione in linea, leggere questo [articolo](#).

Verifica configurazione di Protezione accesso alla rete

Nell'interfaccia utente di Firepower Management Center (FMC), Protezione accesso alla rete può essere visualizzato in **Criteri > Controllo di accesso > Intrusione**. Fare quindi clic sull'opzione **Criteri di analisi della rete** in alto a destra. Sarà quindi possibile visualizzare i criteri di accesso alla rete, crearne di nuovi e modificare quelli esistenti.



Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
	172.16.111.226	50.19.123.95	51177 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAM5_NO_TIMESTAMP (129:14:2)

Inline Mode disabled = No Inline Result

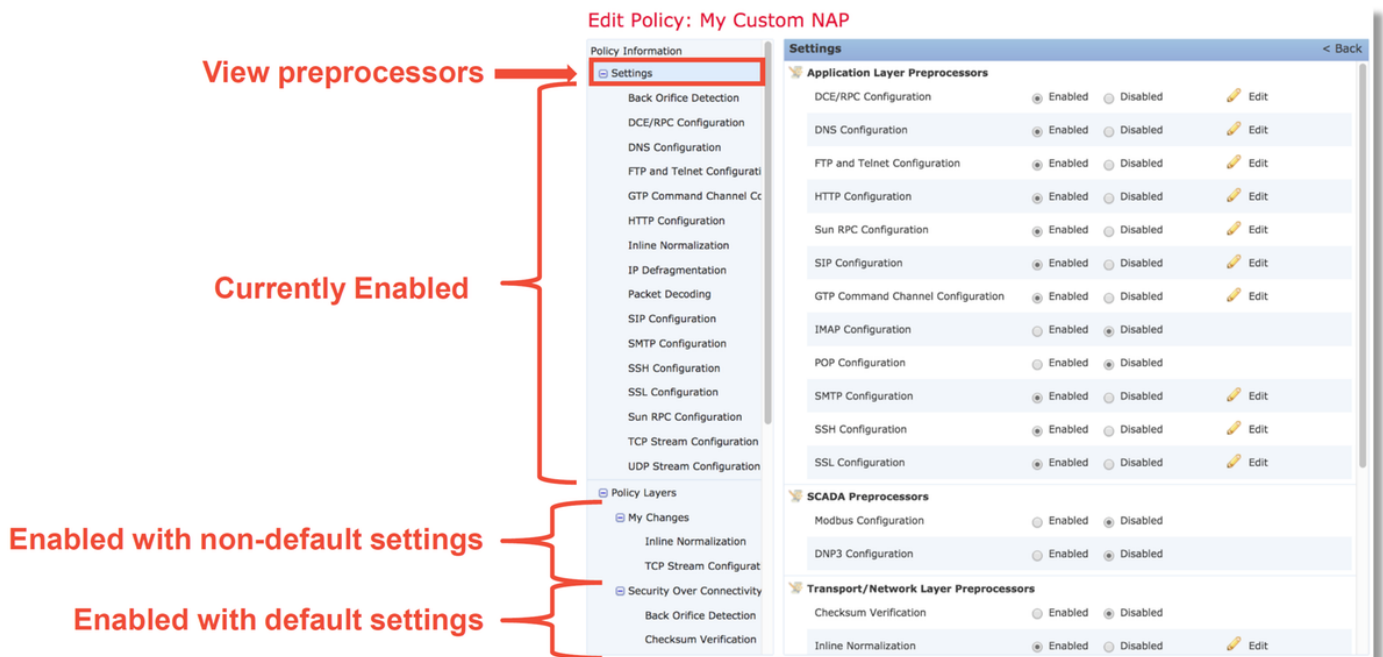
Inline Mode enabled = "Dropped" Inline Result

Come illustrato nella figura precedente, i criteri di protezione accesso alla rete contengono una funzionalità "Modalità in linea", che equivale all'opzione "Elimina quando in linea" del criterio di intrusione. Per evitare che Protezione accesso alla rete ignori il traffico, è possibile deselezionare **Modalità in linea**. Gli eventi di intrusione generati da Protezione accesso alla rete non vengono visualizzati nella scheda **Risultato in linea** con **Modalità in linea** disattivata.

Visualizza impostazioni di Protezione accesso alla rete

In Protezione accesso alla rete è possibile visualizzare le impostazioni correnti. Sono inclusi i preprocessori abilitati totali, seguiti dai

i preprocessori sono abilitati con impostazioni non predefinite (modificate manualmente) e con impostazioni predefinite, come mostrato nella figura seguente.



Impostazioni di Protezione accesso alla rete che possono causare interruzioni invisibili all'utente

Nell'esempio menzionato nella sezione di traccia, la regola di configurazione del flusso TCP 129:14 sta eliminando il traffico. Questo valore viene determinato analizzando l'output di **traccia del supporto di sistema**. Tuttavia, se la regola non è attivata nell'ambito della rispettiva politica sulle intrusioni, al CCP non viene inviato alcun evento di intrusione.

Questo problema si verifica a causa di un'impostazione del preprocessore di **normalizzazione in linea** denominata **Block Unresolvable TCP Header Anomalies** (Anomalie di intestazione TCP non risolvibili). Questa opzione consente a Snort di eseguire un'azione di blocco quando alcune regole GID 129 rilevano anomalie nel flusso TCP.

Se l'opzione **Blocca anomalie intestazione TCP non risolvibili** è abilitata, si consiglia di attivare le regole GID 129 come illustrato di seguito.

The screenshot displays the 'Intrusion Policy' configuration page for GID: "129". It shows 12 selected rules out of 19. A context menu is open over rule 129:14, with options: Generate Events, Drop and Generate Events, and Disable. The 'Inline Normalization' settings panel is also visible, with 'Block Unresolvable TCP Header Anomalies' checked.

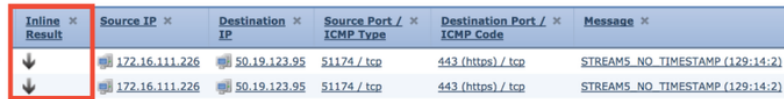
Rule ID	Rule Name	State
129 4	STREAM5_BAD_TIMESTAMP	Checked
129 5	STREAM5_BAD_SEGMENT	Unchecked
129 6	STREAM5_WINDOW_TOO_LARGE	Checked
129 7	STREAM5_EXCESSIVE_TCP_OVERLAPS	Unchecked
129 8	STREAM5_DATA_AFTER_RESET	Checked
129 9	STREAM5_SESSION_HIJACKED_CLIENT	Unchecked
129 10	STREAM5_SESSION_HIJACKED_SERVER	Unchecked
129 11	STREAM5_DATA_WITHOUT_FLAGS	Checked
129 12	STREAM5_SMALL_SEGMENT	Unchecked
129 13	STREAM5_4WAY_HANDSHAKE	Unchecked
129 14	STREAM5_NO_TIMESTAMP	Checked
129 15	STREAM5_BAD_RST	Checked
129 16	STREAM5_BAD_FIN	Checked
129 17	STREAM5_BAD_ACK	Checked
129 18	STREAM5_DATA_AFTER_RST_RCVD	Checked
129 19	STREAM5_WINDOW_SLAM	Checked

Inline Normalization Settings:

- Normalize IPv4:
- Normalize Don't Fragment Bit:
- Normalize Reserved Bit:
- Normalize TOS Bit:
- Normalize Excess Payload:
- Normalize IPv6:
- Normalize ICMPv4:
- Normalize ICMPv6:
- Normalize/Clear Reserved Bits:
- Normalize/Clear Option Padding Bytes:
- Clear Urgent Pointer if URG=0:
- Clear Urgent Pointer/URG on Empty Payload:
- Clear URG if Urgent Pointer Is Not Set:
- Normalize Urgent Pointer:
- Normalize TCP Payload:
- Remove Data on SYN:
- Remove Data on RST:
- Trim Data to Window:
- Trim Data to MSS:
- Block Unresolvable TCP Header Anomalies:

L'attivazione delle regole GID 129 determina l'invio degli eventi intrusione al FMC quando questi intervengono sul traffico. Tuttavia, se l'opzione **Blocca anomalie intestazione TCP non risolvibili** è abilitata, è comunque possibile eliminare il traffico anche se lo **stato** della **regola** nel criterio di intrusione è impostato su **Genera eventi** solo. Questo comportamento viene illustrato nelle guide alla configurazione del CCP.

Still drops after setting to generate



Inline Result	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Message
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAMS_NO_TIMESTAMP (129:14:2)
↓	172.16.111.226	50.19.123.95	51174 / tcp	443 (https) / tcp	STREAMS_NO_TIMESTAMP (129:14:2)

Check configuration guide for relative protocols/preprocessors:

Block Unresolvable TCP Header Anomalies

When you enable this option, the system blocks anomalous TCP packets that, if normalized, would be invalid and likely would be blocked by the receiving host. For example, the system blocks any SYN packet transmitted subsequent to an established session.

The system also drops any packet that matches any of the following TCP stream preprocessor rules, regardless of whether the rules are enabled:

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14 through 129:19

The Total Blocked Packets performance graph tracks the number of packets blocked in inline deployments and, in passive deployments and inline deployments in tap mode, the number that would have been blocked in an inline deployment.

La documentazione di cui sopra è disponibile in questo [articolo](#) (per la versione 6.4, la più recente al momento della pubblicazione di questo articolo).

Verifica della configurazione back-end

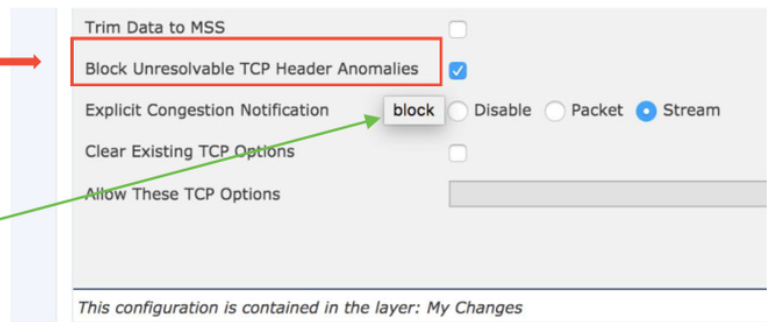
Al comportamento del preprocessore viene aggiunto un altro livello di complessità in quanto alcune impostazioni possono essere abilitate sul back-end, senza essere riflesse nel FMC. Queste sono alcune possibili ragioni.

- Altre funzionalità abilitate consentono di forzare l'abilitazione delle impostazioni del preprocessore (la principale è Criteri file)
- Alcune regole dei criteri per le intrusioni richiedono alcune opzioni del preprocessore per eseguire il rilevamento
- Un difetto può causare il comportamento È stata rilevata un'istanza di questo problema: [CSCuz50295](#) - "Il blocco dei file con malware consente la normalizzazione TCP con flag di blocco"

Prima di esaminare la configurazione back-end, è possibile notare che le parole chiave Snort, utilizzate nei file di configurazione Snort back-end, possono essere visualizzate passando il mouse su un'impostazione specifica all'interno di Protezione accesso alla rete. Fare riferimento all'illustrazione seguente.

Hover over option to see backend snort configuration keyword

Snort config keyword is "block"



L'opzione **Blocca anomalie intestazione TCP non risolvibili** nella scheda Protezione accesso alla rete viene convertita nella parola chiave **block** nel back-end. Tenendo presenti queste informazioni, è possibile controllare la configurazione back-end dalla shell degli esperti.

```
root@ciscoasa:~# de_info.pl
-----
DE Name      : Primary Detection Engine (c9ef19d6-e187-11e6-ba76-99617d53da68)
DE Type      : ids
DE Description : Primary detection engine for device c9ef19d6-e187-11e6-ba76-99617d53da68
DE Resources  : 1
DE UUID      : 0d82120c-e188-11e6-8606-a4827d53da68
-----

root@ciscoasa:~# cd /var/sf/detection_engines/0d82120c-e188-11e6-8606-a4827d53da68/network_analysis/
root@ciscoasa: network_analysis# ls
b50f27b0-e31a-11e6-b866-dd9e65c01d56 object_b50f27b0-e31a-11e6-b866-dd9e65c01d56 snort.conf.b50f27b0-e31a-11e6-b866-
dd9e65c01d56 snort.conf.b50f27b0-e31a-11e6-b866-dd9e65c01d56.default
root@ciscoasa: network_analysis# cat b50f27b0-e31a-11e6-b866-dd9e65c01d56/normalize.conf
#
# generated from My Changes
#
preprocessor normalize_tcp: ips, rsv, pad, req_urg, req_pay, req_urp, block
```

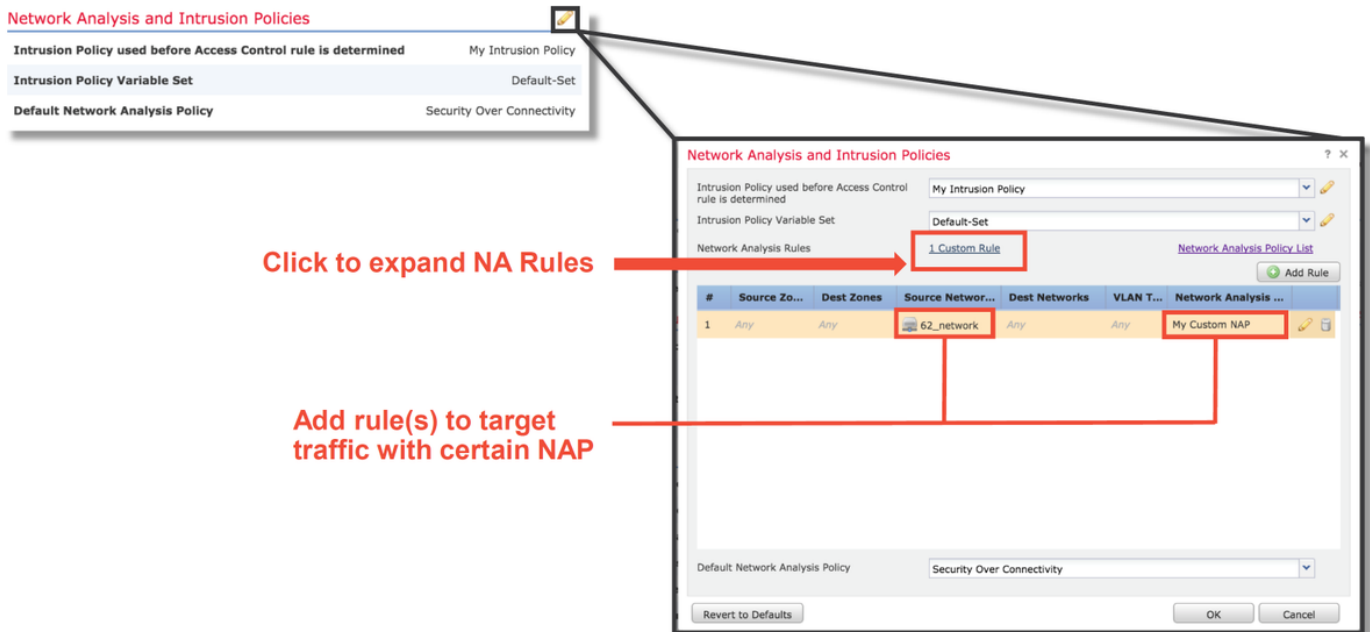
"block" option is enabled in normalize.conf

Creazione di un Protezione accesso alla rete di destinazione

Se determinati host attivano eventi del preprocessore, è possibile utilizzare Protezione accesso alla rete personalizzata per ispezionare il traffico da o verso tali host. All'interno di Protezione accesso alla rete personalizzata è possibile disattivare le impostazioni che causano problemi.

Di seguito sono riportati i passaggi per l'implementazione di un Protezione accesso alla rete mirato.

1. Creare Protezione accesso alla rete in base alle istruzioni indicate nella sezione Verifica configurazione di Protezione accesso alla rete di questo articolo.
2. Nella scheda **Avanzate** di Criteri di controllo di accesso passare alla sezione **Criteri di analisi della rete e intrusioni**. Fare clic su **Aggiungi regola** e creare una regola utilizzando gli host di destinazione e scegliere Protezione accesso alla rete appena creata nella sezione **Criteri di analisi della rete**.



Analisi falsi positivi

Il controllo dei falsi positivi negli eventi di intrusione per le regole del preprocessore è molto diverso da quello delle regole Snort utilizzate per la valutazione delle regole (che contengono un GID di 1 e 3).

Per eseguire un'analisi falsa positiva per gli eventi delle regole del preprocessore, è necessaria un'acquisizione di sessione completa per cercare le anomalie all'interno del flusso TCP.

Nell'esempio seguente viene eseguita l'analisi dei falsi positivi sulla regola **129:14**, che negli esempi precedenti mostra come il traffico stia diminuendo. Poiché **129:14** sta cercando i flussi TCP in cui mancano i timestamp, è possibile capire chiaramente perché la regola è stata attivata in base all'analisi di acquisizione dei pacchetti illustrata di seguito.

Full session pcap

```

> Internet Protocol Version 4, Src: 172.16.111.226, Dst: 50.19.123.95
  > Transmission Control Protocol, Src Port: 51174, Dst Port: 443, Seq: 3849839666, Len: 0
    Source Port: 51174
    Destination Port: 443
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 3849839666
    Acknowledgment number: 0
    Header Length: 40 bytes
    < b> Flags: 0x002 (SYN)
    Window size value: 8192
    [Calculated window size: 8192]
    Checksum: 0x70ba [correct]
    [Checksum Status: Good]
    [Calculated Checksum: 0x70ba]
    Urgent pointer: 0
    < b> Options: 20 bytes, Maximum segment size, No-Operation (NOP), Window scale, SACK permitted, Timestamps
      > Maximum segment size: 1380 bytes
      > No-Operation (NOP)
      > Window scale: 8 (multiply by 256)
      > TCP SACK Permitted Option: True
      > Timestamps: TSval 2054852, TSecr 0
  < b> Packet that triggered event
    > Internet Protocol Version 4, Src: 172.16.111.226, Dst: 50.19.123.95
      > Transmission Control Protocol, Src Port: 51174, Dst Port: 443, Seq: 3849839667, Ack: 1666843207, Len: 0
        Source Port: 51174
        Destination Port: 443
        [Stream index: 0]
        [TCP Segment Len: 0]
        Sequence number: 3849839667
        Acknowledgment number: 1666843207
        Header Length: 20 bytes
        < b> Flags: 0x010 (ACK)
        Window size value: 57
        [Calculated window size: 57]
        [Window size scaling factor: -1 (unknown)]
        Checksum: 0xed47 [correct]
        [Checksum Status: Good]
        [Calculated Checksum: 0xed47]
        Urgent pointer: 0
  < b> No TCP Timestamps in event packet (violates RFC)
  
```

SYN packet has TCP Timestamps

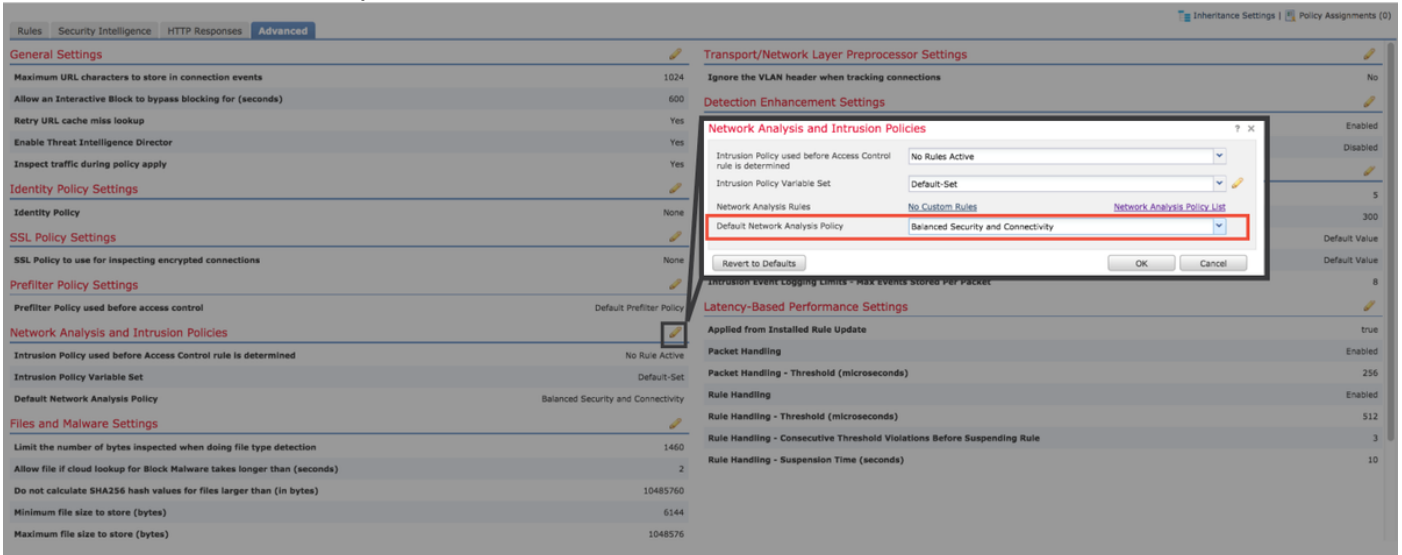
Packet that triggered event

No TCP Timestamps in event packet (violates RFC)

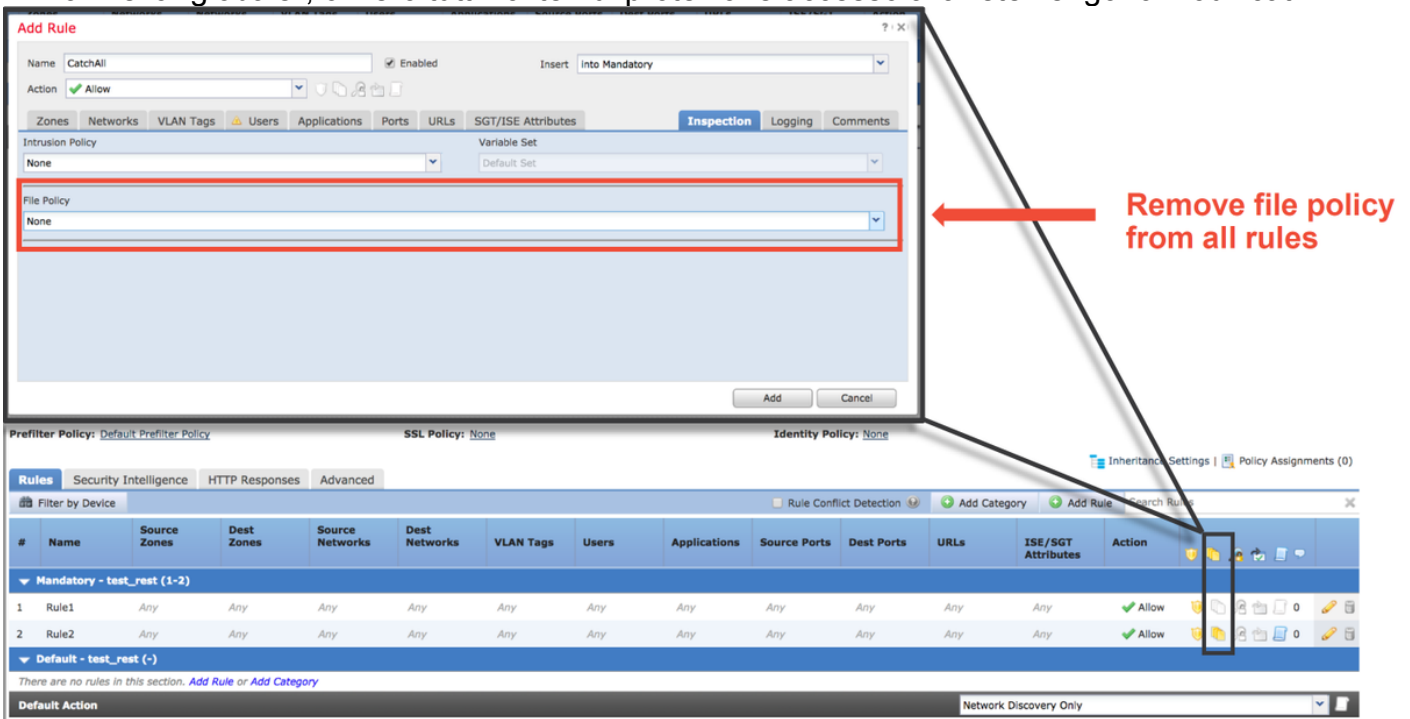
Fasi di mitigazione

Per ridurre rapidamente i possibili problemi di Protezione accesso alla rete, è possibile eseguire i passaggi seguenti.

- Se è in uso un criterio di Protezione accesso alla rete personalizzato e non si è certi che un'impostazione di Protezione accesso alla rete stia riducendo il traffico ma si sospetta che lo sia, è possibile provare a sostituirlo con un criterio "Protezione e connettività bilanciate" o "Connettività tramite protezione".



- Se vengono utilizzate "regole personalizzate", assicurarsi di impostare Protezione accesso alla rete su uno dei valori predefiniti sopra indicati
- Se una qualsiasi regola di controllo d'accesso utilizza un criterio file, potrebbe essere necessario provare a rimuoverlo temporaneamente in quanto un criterio file può abilitare le impostazioni del preprocessore sul back-end che non vengono riflesse nel FMC. Ciò avviene a livello "globale", ovvero tutti i criteri di protezione accesso alla rete vengono modificati.



Ogni protocollo ha un preprocessore diverso e la risoluzione dei problemi può essere molto specifica per il preprocessore. In questo documento non vengono illustrate tutte le impostazioni del preprocessore e i metodi di risoluzione dei problemi per ciascuno di essi.

È possibile consultare la documentazione di ogni preprocessore per avere un'idea più precisa della funzione di ogni opzione, il che risulta utile per la risoluzione dei problemi di un preprocessore specifico.

Dati da fornire a TAC

Dati

Istruzioni

Risoluzione
dei problemi
relativi al file
dalla

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn>

periferica

Firepower

Acquisizione

di pacchetti

in sessione

completa

<http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-series-applian>

dal

dispositivo

Firepower