

Determinare la versione snort attiva in esecuzione su Firepower Threat Defense (FTD)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Determinare la versione attiva dello snort eseguita su FTD](#)

[CLI \(Command Line Interface\) FTD](#)

[FTD gestito da Cisco FDM](#)

[FTD gestito dal Cisco FMC](#)

[FTD gestito da Cisco CDO](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come confermare la versione snort attiva in esecuzione di Cisco Firepower Threat Defense (FTD) quando viene gestita da Cisco Firepower Device Manager (FDM), Cisco Firepower Management Center (FMC) o Cisco Defense Orchestrator (CDO).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firepower Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Cisco Firepower Device Manager (FDM)
- Cisco Defense Orchestrator (CDO)

Componenti usati

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

- Cisco Firepower Threat Defense (FTD) versione 6.7.0 e 7.0.0
- Cisco Firepower Management Center (FMC) versione 6.7.0 e 7.0.0
- Cisco Defense Orchestrator (CDO)

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.

Premesse

SNORT® Intrusion Prevention System ha ufficialmente lanciato Snort 3, un aggiornamento radicale che presenta miglioramenti e nuove funzionalità che migliorano le prestazioni, l'elaborazione più veloce, la scalabilità migliorata per la rete e una gamma di oltre 200 plug-in in modo che gli utenti possano creare una configurazione personalizzata per la propria rete.

I vantaggi di Snort 3 includono, tra l'altro:

- Prestazioni migliorate
- Ispezione SMBv2 migliorata
- Nuove funzionalità di rilevamento degli script
- Ispezione HTTP/2
- Gruppi di regole personalizzati
- Sintassi che semplifica la scrittura delle regole di intrusione personalizzate
- Motivi per la perdita dei risultati inline negli eventi di intrusione
- Nessun riavvio automatico quando vengono distribuite modifiche al database virtuale, ai criteri SSL, ai rilevatori di applicazioni personalizzati, alle origini di identità del portale captive e all'individuazione delle identità del server TLS
- Miglioramento dei servizi grazie all'invio dei dati di telemetria specifici di Snort 3 a Cisco Success Network e a una migliore risoluzione dei problemi dei log

Il supporto per Snort 3.0 è stato introdotto per Cisco Firepower Threat Defense (FTD) 6.7.0, proprio quando l'FTD è gestito tramite Cisco Firepower Device Manager (FDM).

Nota: per le nuove distribuzioni FTD 6.7.0 gestite da FDM, Snort 3.0 è il motore di ispezione predefinito. Se si aggiorna il FTD alla versione 6.7 da una release precedente, Snort 2.0 rimane il motore di ispezione attivo, ma è possibile passare alla versione 3.0.

Nota: per questa release, Snort 3.0 non supporta router virtuali, regole di controllo dell'accesso basate sul tempo o la decrittografia di connessioni TLS 1.1 o versioni precedenti. Attivate Snort 3.0 solo se queste funzioni non sono necessarie.

In seguito, Firepower versione 7.0 ha introdotto il supporto Snort 3.0 per i dispositivi Firepower Threat Defense gestiti da entrambi, Cisco FDM e Cisco Firepower Management Center (FMC).

Nota: per le nuove distribuzioni FTD 7.0, Snort 3 è ora il motore di ispezione predefinito. Le distribuzioni aggiornate continuano a utilizzare Snort 2, ma è possibile passare in qualsiasi momento.

Attenzione: è possibile passare liberamente da Snort 2.0 a Snort 3.0 e viceversa, in modo da poter annullare le modifiche se necessario. Il traffico viene interrotto ogni volta che si cambia versione.

Attenzione: prima di passare allo Snort 3, si consiglia di leggere e comprendere la [Guida alla configurazione dello Snort 3 di Firepower Management Center](#). Prestare particolare attenzione alle limitazioni delle funzionalità e alle istruzioni di migrazione. Sebbene l'aggiornamento allo Snort 3 sia

progettato per un impatto minimo, le funzionalità non vengono mappate esattamente. La pianificazione e la preparazione prima dell'aggiornamento consentono di verificare che il traffico venga gestito come previsto.

Determinare la versione attiva dello snort eseguita su FTD

CLI (Command Line Interface) FTD

Per determinare la versione snort attiva in esecuzione su un FTD, accedere alla CLI del FTD ed eseguire il comando **show snort3 status**:

Esempio 1: quando non viene visualizzato alcun output, l'FTD esegue Snort 2.

```
<#root>  
>  
show snort3 status  
  
>
```

Esempio 2: quando l'output mostra "**Current running Snort 2**", l'FTD esegue Snort 2.

```
<#root>  
>  
show snort3 status  
  
Currently running Snort 2
```

Esempio 3: quando l'output mostra "**Current running Snort 3**", l'FTD esegue Snort 3.

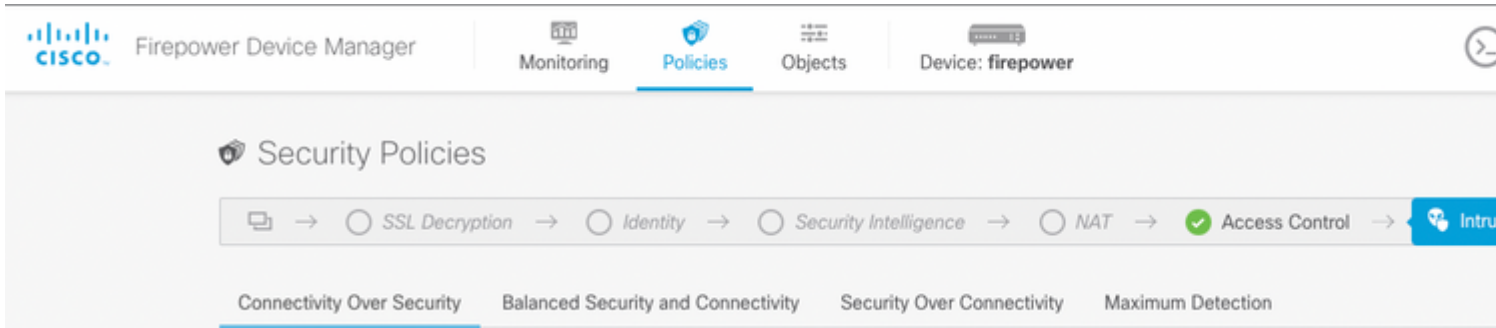
```
<#root>  
>  
show snort3 status  
  
Currently running Snort 3
```

FTD gestito da Cisco FDM

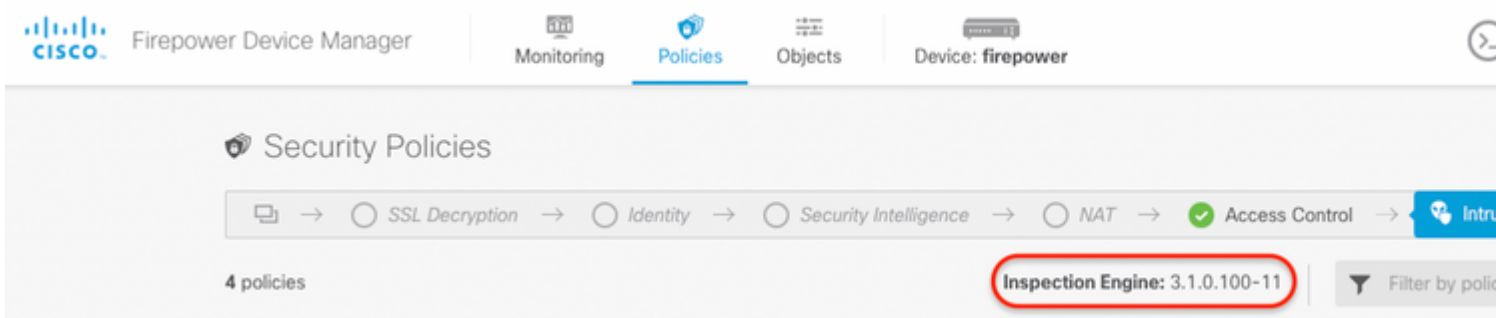
Per determinare la versione snort attiva in esecuzione su un FTD gestito da Cisco FDM, procedere con i passi successivi:

1. Accedere all'FTD Cisco tramite l'interfaccia Web FDM.
2. Dal menu principale, selezionare **Policy**.
3. Quindi, selezionate la scheda **Intrusione (Intrusion)**.
4. Cercare la sezione **Versione snort** o **Motore di ispezione** per confermare la versione snort attiva nell'FTD.

Esempio 1: l'FTD esegue snort versione 2.



Esempio 2: l'FTD esegue snort versione 3.



FTD gestito dal Cisco FMC

Per determinare la versione snort attiva in esecuzione su un FTD gestito da Cisco FMC, procedere con i passaggi seguenti:

1. Accedere all'interfaccia Web di Cisco FMC.
2. Dal menu **Dispositivi**, selezionare **Gestione dispositivi**.
3. Quindi, selezionare il dispositivo FTD appropriato.
4. Fare clic sull'icona **Modifica** matita.
5. Selezionare la scheda **Device** e cercare la sezione **Inspection Engine** per confermare la versione snort attiva nell'FTD:

Esempio 1: l'FTD esegue snort versione 2.

vFTD-1

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP

General

Name:	vFTD-1
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled

License

Performance Tier :	FTDv - Variable
Base:	Yes
Export-Controlled Features:	Yes
Malware:	Yes
Threat:	Yes
URL Filtering:	Yes
AnyConnect Apex:	No
AnyConnect Plus:	No
AnyConnect VPN Only:	No

System

Model:	
Serial:	
Time:	
Time Zone:	
Version:	
Time Zone setting based Rules:	

Inspection Engine

Inspection Engine: Snort 2

NEW Upgrade to our new and improved Snort 3

Snort 3 is the latest version of the most powerful, industry-standard inspection engine at the heart of Firepower Threat Defense devices. With significant improvements to performance and security efficacy, there is a lot to be excited about! [Learn more](#)

▲ Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be momentary traffic loss.

Note: If the device uses an Intrusion Policy that has custom Intrusion Rule, Snort 3 will not be able to migrate those rules.

[Upgrade](#)

Health

Status:	!
Policy:	Initial_Health_Policy 2018-02-28 14:46:00
Excluded:	None

Management

Host:	
Status:	
FMC Access Inter	

Esempio 2: l'FTD esegue snort versione 3.

FTD1010-1

Cisco Firepower 1010 Threat Defense

Device Routing Interfaces Inline Sets DHCP SNMP

General	
Name:	FTD1010-1
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled

License	
Base:	Yes
Export-Controlled Features:	Yes
Malware:	Yes
Threat:	Yes
URL Filtering:	Yes
AnyConnect Apex:	Yes
AnyConnect Plus:	Yes
AnyConnect VPN Only:	No

System	
Model:	
Serial:	
Time:	
Time Zone:	
Version:	
Time Zone setting:	
Rules:	
Inventory:	

Inspection Engine	
Inspection Engine:	Snort 3
Revert to Snort 2	

Health	
Status:	!
Policy:	Initial_Health_Policy 2018-02-28 14:46:00
Excluded:	None

Management	
Host:	
Status:	
FMC Access Inte	

significant improvements to performance and security efficacy, there is a lot to be excited about! [Learn more](#)

▲ Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be momentary traffic loss.

Note: If the device uses an Intrusion Policy that has custom Intrusion Rule, Snort 3 will not be able to migrate those rules.

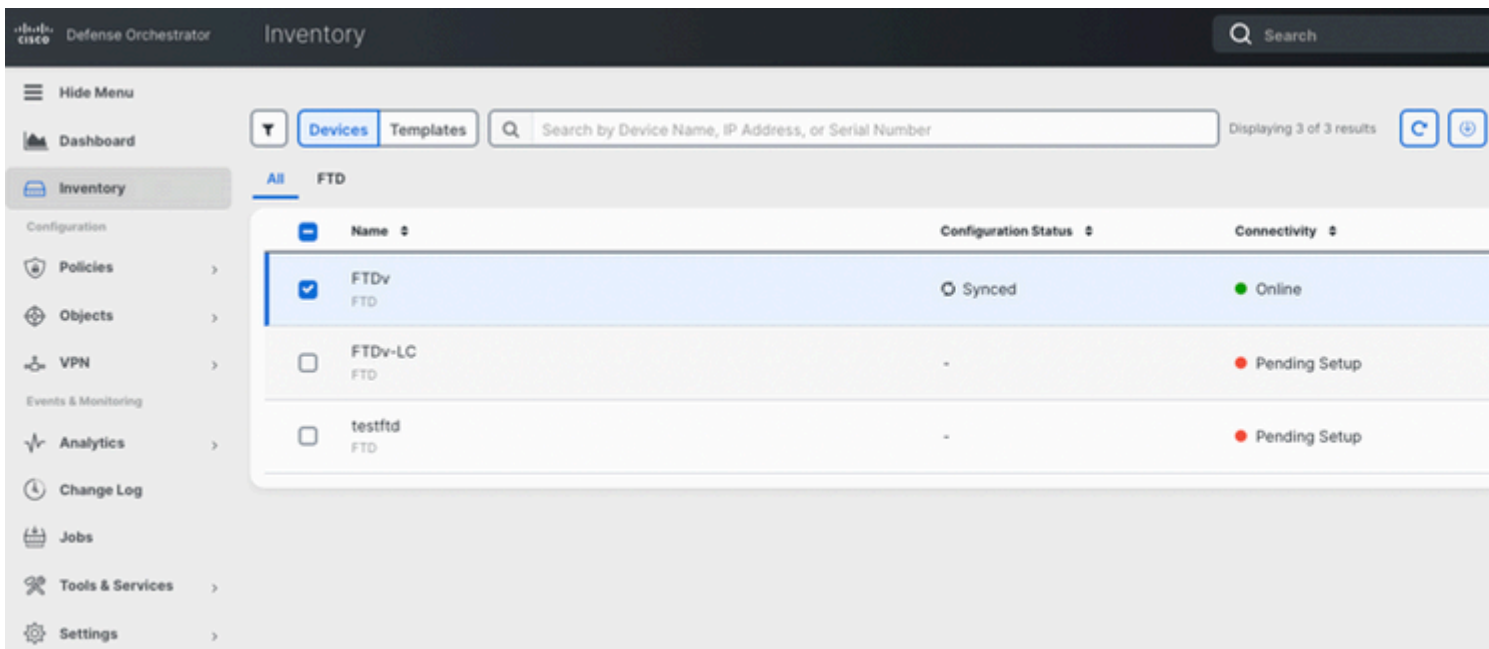
[Upgrade](#)

FTD gestito dal Cisco CDO

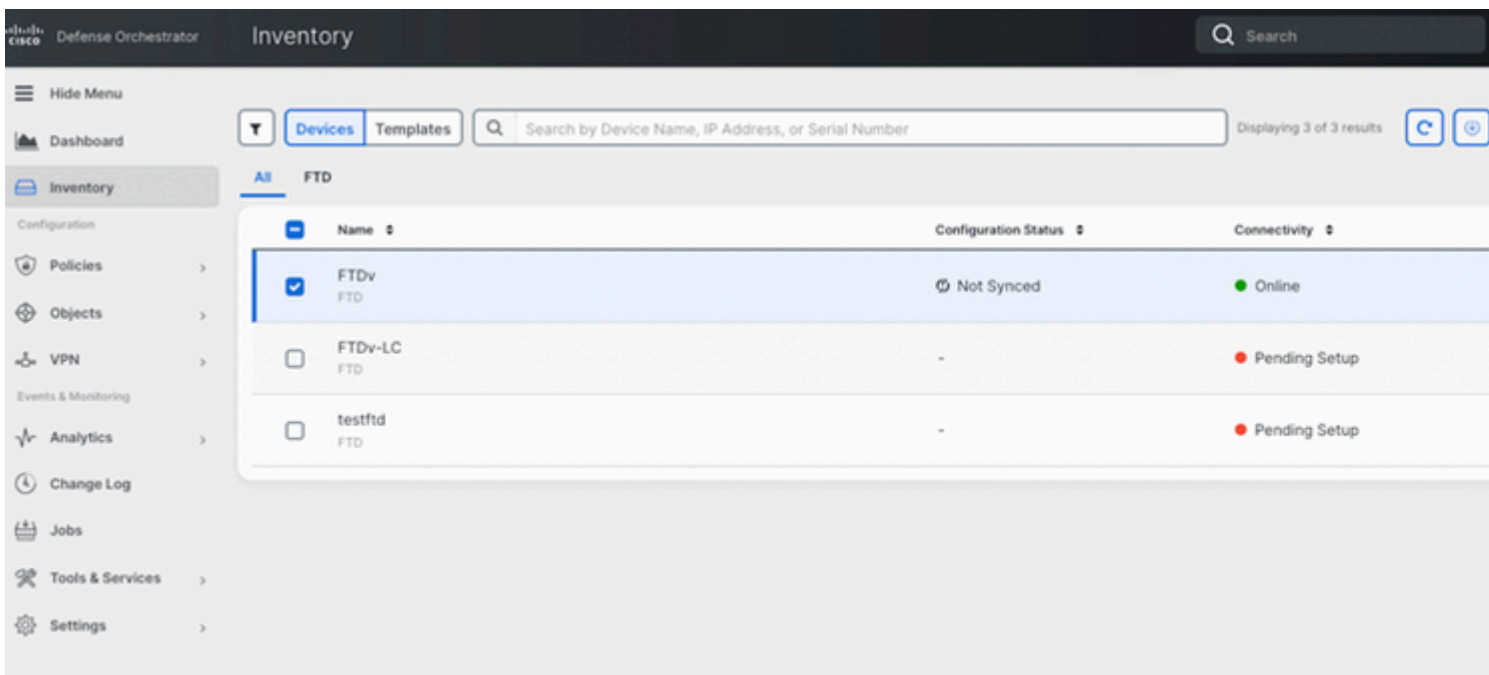
Per determinare la versione snort attiva in esecuzione su un FTD gestito da Cisco Defense Orchestrator, procedere con i passaggi seguenti:

1. Accedere all'interfaccia Web di Cisco Defense Orchestrator.
2. Dal menu **Inventory**, selezionare il dispositivo FTD appropriato.
3. Nella sezione **Dettagli dispositivo**, cercare **Versione snort**:

Esempio 1: l'FTD esegue snort versione 2.



Esempio 2: l'FTD esegue snort versione 3.



Informazioni correlate

- [Note sulla release di Cisco Firepower, versione 6.7.0](#)
- [Note sulla versione di Cisco Firepower, versione 7.0](#)
- [Sito Web Snort 3](#)
- [Documentazione e supporto tecnico â€“ Cisco Systems](#)

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).