

Implementazione di Snort IPS sui Cisco Integrated Services Router serie 4000

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Configurazione UTD piattaforma](#)

[Configurazione del piano di servizio e del piano dati](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Debug](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come distribuire la funzionalità Snort IPS e Snort IDS su Cisco Integrated Services Router (ISR) serie 4000 utilizzando il metodo IOx.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Integrated Services Router serie 4000 con almeno 8 GB di DRAM.
- Funzionalità di base del comando IOS-XE.
- Conoscenze base di snort.
- È necessario un abbonamento con firma annuale o triennale
- IOS-XE 16.10.1a e versioni successive.

Componenti usati

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

- ISR4331/K9 con versione 17.9.3a.

- UTD Engine TAR per release 17.9.3a.
- Licenza SecurityKey9 per ISR4331/K9.

Il metodo VMAN è obsoleto.

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

La funzione Snort IPS abilita Intrusion Prevention System (IPS) o Intrusion Detection System (IDS) per le filiali su Cisco serie 4000 Integrated Services Router e Cisco Cloud Services Router serie 1000v. Questa funzionalità utilizza lo snort open-source per abilitare le funzionalità IPS e IDS.

Lo snort è un IPS open-source che esegue analisi del traffico in tempo reale e genera avvisi quando vengono rilevate minacce sulle reti IP. Può inoltre eseguire analisi di protocollo, ricerche di contenuti o marce, nonché rilevare una varietà di attacchi e sonde, ad esempio sovraccarichi del buffer, scansioni di porte stealth e così via. Il motore Snort viene eseguito come servizio contenitore virtuale su Cisco Integrated Services Router serie 4000 e Cloud Services Router serie 1000v.

La funzione Snort IPS funziona come modalità di rilevamento o prevenzione delle intrusioni nella rete e fornisce funzionalità IPS o IDS su Cisco Integrated Services Router serie 4000 e Cloud Services Router serie 1000v.

- Esegue il monitoraggio del traffico di rete e l'analisi in base a un set di regole definito.
- Esegue la classificazione degli allegati.
- Richiama azioni in base a regole corrispondenti.

In base ai requisiti di rete. È possibile abilitare lo snort IPS come IPS o IDS. In modalità IDS, Snort controlla il traffico e segnala gli avvisi, ma non interviene per prevenirne gli attacchi. In modalità IPS, controlla il traffico e segnala gli avvisi come in modalità IDS, ma vengono intraprese azioni per prevenire gli attacchi.

Lo Snort IPS viene eseguito come servizio sui router ISR. I contenitori dei servizi utilizzano la tecnologia di virtualizzazione per fornire un ambiente host sui dispositivi Cisco per le applicazioni. L'ispezione del traffico di snort è abilitata su una base di interfaccia o a livello globale su tutte le interfacce supportate. Il sensore Snort richiede due interfacce VirtualPortGroup. Il primo VirtualPortGroup viene utilizzato per il traffico di gestione e il secondo per il traffico di dati tra il piano di inoltro e il servizio contenitore virtuale Snort. È necessario configurare gli indirizzi IP per queste interfacce VirtualPortGroup. La subnet IP assegnata all'interfaccia di gestione VirtualPortGroup deve essere in grado di comunicare con il server delle firme e il server di avviso/reporting.

Lo Snort IPS controlla il traffico e segnala gli eventi a un server di registro esterno o al syslog IOS.

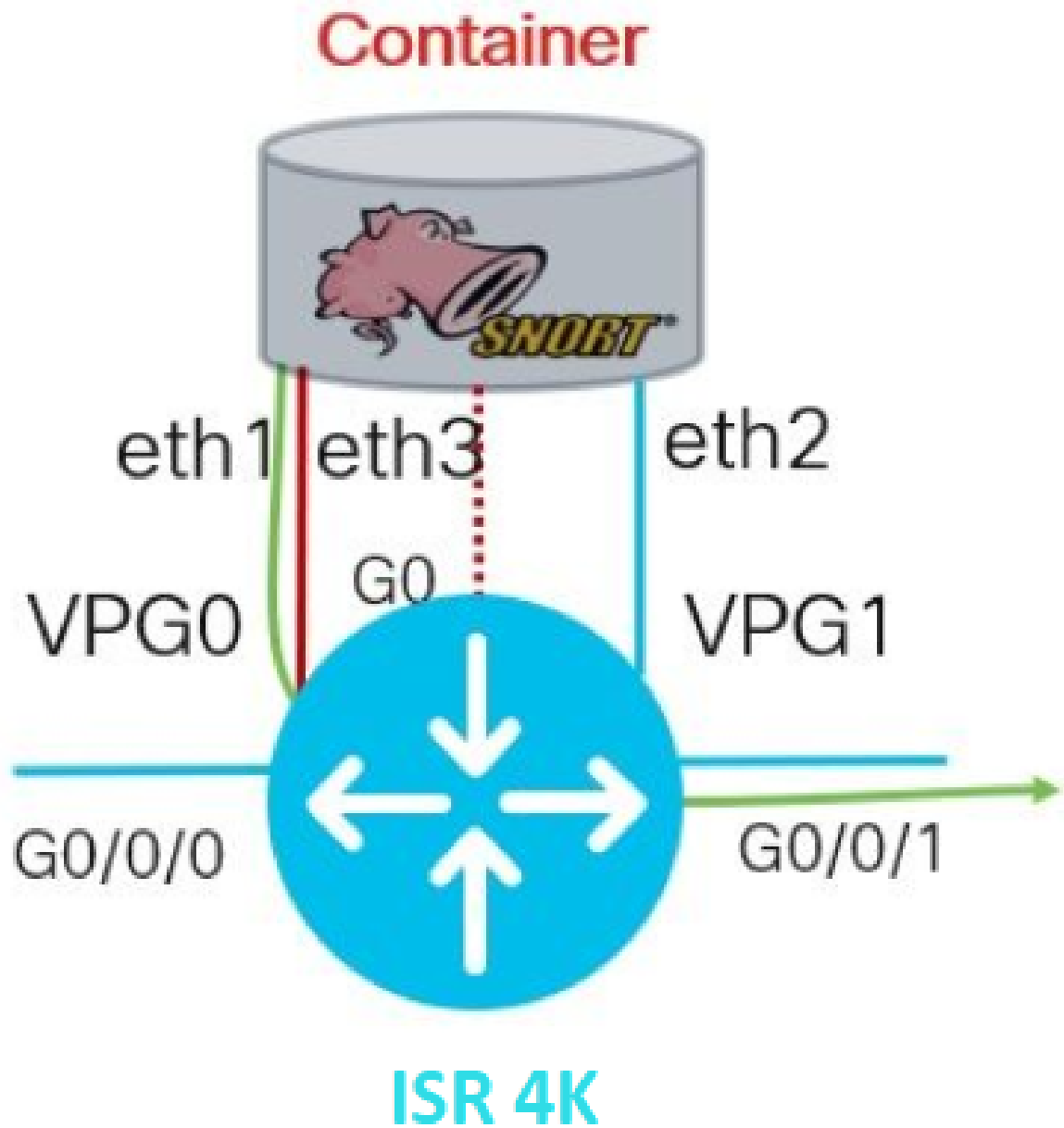
L'abilitazione dell'accesso al syslog IOS può influire sulle prestazioni a causa del volume potenziale dei messaggi di log. Per la raccolta e l'analisi dei log è possibile utilizzare strumenti di monitoraggio esterni di terze parti, che supportano i log Snort.

L'avvio di IPS su Cisco serie 4000 Integrated Services Router e Cisco Cloud Services Router serie 1000v è basato sul download del pacchetto Signature. Esistono due tipi di sottoscrizione:

- Pacchetto di firme della community.
- Pacchetto di firme basato sul sottoscrittore.

Il set di regole del pacchetto di firme della community offre una copertura limitata contro le minacce. Il set di regole del pacchetto di firma basato sul sottoscrittore offre la migliore protezione dalle minacce. Include la copertura in anticipo degli exploit e fornisce anche l'accesso più rapido alle firme aggiornate in risposta a un incidente di sicurezza o alla scoperta proattiva di una nuova minaccia. Questa sottoscrizione è completamente supportata da Cisco e il pacchetto verrà aggiornato su Cisco.com. Il pacchetto di firma può essere scaricato da software.cisco.com. Le informazioni sulle firme degli snort sono disponibili all'indirizzo snort.org.

Esempio di rete



Configurazione

Configurazione UTD piattaforma

Passaggio 1. Configurare le interfacce VirtualPortGroups virtuali.

```
Router#configure terminal
Router(config)#interface VirtualPortGroup0
Router(config-if)#description Management Interface
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

```
Router(config)#interface VirtualPortGroup1
Router(config-if)#description Data Interface
Router(config-if)#ip address 192.168.2.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

Passaggio 2. Abilitare l'ambiente IOx in modalità di configurazione globale.

```
Router(config)#iox
```


Passaggio 3. Configurare l'hosting dell'app con la configurazione della vnic.

```
Router(config)#app-hosting appid UTD
Router(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.1.2 netmask 255.255.255.252
Router(config-app-hosting-gateway0)#exit
```

```
Router(config-app-hosting)#app-vnic gateway1 virtualportgroup 1 guest-interface 1
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.2.2 netmask 255.255.255.252
Router(config-app-hosting-gateway0)#exit
```


Passaggio 4 (facoltativo). Configurare il profilo della risorsa.

```
Router(config-app-hosting)#app-resource package-profile low [low,medium,high]
Router(config-app-hosting)#end
```

 Nota: Se non è definita, il sistema utilizzerà la configurazione predefinita app-resource (basso). Assicurarsi di disporre di risorse sufficienti sull'ISR se la configurazione predefinita del profilo verrà modificata.

Passaggio 5. Installare l'hosting dell'app utilizzando il file UTD.tar.

```
Router#app-hosting install appid UTD package bootflash:iox-iosxe-utd.16.12.08.1.0.24_SV2.9.16.1_XE16.12
```

 Nota: mantenere il file UTD.tar corretto su bootflash: per procedere con l'installazione. La versione dello snort è specificata nel nome file UTD.

```
Router#configure terminal
Router(config)#utd engine standard
```

Passaggio 2. Abilita la registrazione dei messaggi di emergenza in un server remoto.

```
Router(config-utd-eng-std)#logging host 192.168.10.5
```

Passaggio 3. Abilitare l'ispezione delle minacce per lo snort Engine.

```
Router(config-utd-eng-std)#threat-inspection
```

Passaggio 4. Configurazione del rilevamento delle minacce come IPS (Intrusion Prevention System) o IDS (Intrusion Detection System)

```
Router(config-utd-engstd-insp)#threat [protection,detection]
```



Nota: 'Protezione' viene utilizzato per IPS e 'Rilevamento' per IDS. 'Rilevamento' è l'impostazione predefinita.

Passaggio 5. Configurare i criteri di protezione.

```
Router(config-utd-engstd-insp)#policy [balanced, connectivity, security]
Router(config-utd-engstd-insp)#exit
Router(config-utd-eng-std)#exit
```




Nota: il criterio predefinito è 'quadrato'

Passaggio 6 (facoltativo). Creare l'elenco UTD consentito (Whitelist)

```
Router#configure terminal
Router(config)#utd threat-inspection whitelist
```

Passaggio 7 (facoltativo). Configurare gli Snort Signatures ID (Segnali di firma) da visualizzare nell'elenco.

```
Router(config-utd-whitelist)#generator id 40 signature id 54621 comment FILE-OFFICE traffic from network
Router(config-utd-whitelist)#end
```


 Nota: ad esempio viene utilizzato l'ID 40. Per controllare le informazioni Snort Signature, consultare la documentazione ufficiale Snort.


Passaggio 8 (facoltativo). Abilita elenco oggetti autorizzati nella configurazione di ispezione delle minacce.

```
Router#config terminal
Router(config)#utd engine standard
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#whitelist
```

Passaggio 9. Configurare l'intervallo di aggiornamento della firma per il download automatico delle firme personalizzate.


```
Router#config terminal
Router(config)#utd engine standard
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#signature update occur-at [daily, monthly, weekly] 0 0
```


 Nota: il primo numero definisce l'ora nel formato 24hr, mentre il secondo numero indica i minuti.

 Avviso: gli aggiornamenti della firma UTD generano una breve interruzione del servizio al momento dell'aggiornamento.

Passaggio 10. Configurare i parametri del server di aggiornamento della firma.

```
Router(config-utd-engstd-insp)#signature update server [cisco, url] username cisco password cisco12
```

 Nota: utilizzare 'cisco' per utilizzare il server Cisco o 'url' per definire un percorso

 personalizzato per il server di aggiornamento. Per il server Cisco, è necessario fornire un nome utente e una password personalizzati.

Passaggio 11. Abilita livello di registrazione.

```
Router(config-utd-engstd-insp)#logging level [alert,crit,debug,emerg,info,notice,warning]
Router(config-utd-engstd-insp)#exit
Router(config-utd-eng-std)#exit
```

Passaggio 12. Abilitare il servizio UTD.

```
Router#configure terminal
Router(config)#utd
```

Passaggio 13 (facoltativo). Reindirizza il traffico di dati dall'interfaccia VirtualPortGroup al servizio UTD.

```
Router#configure terminal
Router(config)#utd
Router(config-utd)#redirect interface virtualPortGroup
```

 Nota: se il reindirizzamento non è configurato, viene rilevato automaticamente.

Passaggio 14. Abilitare UTD su tutte le interfacce di layer 3 su ISR.

```
Router(config-utd)#all-interfaces
```

Passaggio 15. Attivare lo standard del motore.


```
Router(config-utd)#engine standard
```

I messaggi syslog successivi devono essere visualizzati per indicare che l'UTD è stato abilitato correttamente.

```
*Jun 27 23:41:03.062: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0
*Jun 27 23:41:13.039: %IOSXE-2-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:0
*Jun 27 23:41:22.457: %IOSXE-5-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:0
```

Passaggio 16 (facoltativo). Definire l'azione per il guasto del motore UTD (UTD Data Plane)

```
Router(config-engine-std)#fail close
Router(config-engine-std)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
```

 Nota: l'opzione 'Fail close' elimina tutto il traffico IPS/IDS quando il motore UTD si guasta. L'opzione 'Fail open' consente tutto il traffico IPS/IDS in caso di errori UTD. L'opzione predefinita è 'fail-open'.

Verifica

Verificare l'indirizzo IP e lo stato dell'interfaccia di VirtualPortGroups.

```
Router#show ip interface brief | i VirtualPortGroup
VirtualPortGroup0 192.168.1.1 YES NVRAM up up
VirtualPortGroup1 192.168.2.1 YES NVRAM up up
```

Verificare la configurazione del gruppo porte virtuali.

```
Router#show running-config | b interface
interface VirtualPortGroup0
description Management Interface
ip address 192.168.1.1 255.255.255.252
!
interface VirtualPortGroup1
description Data Interface
ip address 192.168.2.1 255.255.255.252
!
```

Verificare la configurazione dell'hosting dell'app.

```
Router#show running-config | b app-hosting
app-hosting appid UTD
app-vnic gateway0 virtualportgroup 0 guest-interface 0
```

```
guest-ipaddress 192.168.1.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 1 guest-interface 1
guest-ipaddress 192.168.2.2 netmask 255.255.255.252
start
end
```

Verificare l'attivazione di iox.

```
Router#show running-config | i iox
iox
```

Verificare la configurazione del piano di servizio UTD.

```
Router#show running-config | b engine
utd engine standard
logging host 192.168.10.5
threat-inspection
threat protection
policy security
signature update server cisco username cisco password KcEDIO[gYafNZheBHBD`CC\g`_cSeFAAB
signature update occur-at daily 0 0
logging level info
whitelist
utd threat-inspection whitelist
generator id 40 signature id 54621 comment FILE-OFFICE traffic
utd
all-interfaces
redirect interface VirtualPortGroup1
engine standard
fail close
```

```
Router#show utd engine standard config
UTD Engine Standard Configuration:
```

IPS/IDS : Enabled

Operation Mode : Intrusion Prevention
Policy : Security

Signature Update:
Server : cisco
User Name : cisco
Password : KcEDIO[gYafNZheBHBD`CC\g`_cSeFAAB
Occurs-at : daily ; Hour: 0; Minute: 0

Logging:
Server : 192.168.10.5
Level : info
Statistics : Disabled
Hostname : router

System IP : Not set

Whitelist : Enabled
Whitelist Signature IDs:
54621, 40

Port Scan : Disabled

Web-Filter : Disabled

Verificare lo stato di hosting dell'app.

```
Router#show app-hosting list
App id                               State
-----
UTD                                   RUNNING
```

Verificare i dettagli di hosting dell'app.

```
Router#show app-hosting detail
App id : UTD
Owner : ioxm
State : RUNNING
Application
Type : LXC
Name : UTD-Snort-Feature
Version : 1.0.7_SV2.9.18.1_XE17.9
Description : Unified Threat Defense
Author :
Path : /bootflash/secapp-utd.17.09.03a.1.0.7_SV2.9.18.1_XE17.9.x86_64.tar
URL Path :
Multicast : yes
Activated profile name :
```

```
Resource reservation
Memory : 1024 MB
Disk : 752 MB
CPU :
CPU-percent : 25 %
VCPUs : 0
```

```
Platform resource profiles
Profile Name CPU(unit) Memory(MB) Disk(MB)
```

```
Attached devices
Type Name Alias
```

```
-----
Disk /tmp/xml/UtdLogMappings-IOX
Disk /tmp/xml/UtdIpsAlert-IOX
Disk /tmp/xml/UtdDaqWcapi-IOX
Disk /tmp/xml/UtdUr1f-IOX
Disk /tmp/xml/UtdTls-IOX
```

Disk /tmp/xml/UtdDaq-IOX
Disk /tmp/xml/UtdAmp-IOX
Watchdog watchdog-503.0
Disk /tmp/binos-IOX
Disk /opt/var/core
Disk /tmp/HTX-IOX
Disk /opt/var
NIC ieobc_1 ieobc
Disk _rootfs
NIC mgmt_1 mgmt
NIC dp_1_1 net3
NIC dp_1_0 net2
Serial/Trace serial3

Network interfaces

eth0:
MAC address : 54:0e:00:0b:0c:02
IPv6 address : ::
Network name :
eth:
MAC address : 6c:41:0e:41:6b:08
IPv6 address : ::
Network name :
eth2:
MAC address : 6c:41:0e:41:6b:09
IPv6 address : ::
Network name :
eth1:
MAC address : 6c:41:0e:41:6b:0a
IPv4 address : 192.168.2.2
IPv6 address : ::
Network name :

Process Status Uptime # of restarts

climgr UP 0Y 0W 0D 21:45:29 2
logger UP 0Y 0W 0D 19:25:56 0
snort_1 UP 0Y 0W 0D 19:25:56 0

Network stats:

eth0: RX packets:162886, TX packets:163855
eth1: RX packets:46, TX packets:65

DNS server:

domain cisco.com
nameserver 192.168.90.92

Coredump file(s): core, lost+found

Interface: eth2
ip address: 192.168.2.2/30
Interface: eth1
ip address: 192.168.1.2/30

Address/Mask Next Hop Intf.

0.0.0.0/0 192.168.2.1 eth2
0.0.0.0/0 192.168.1.1 eth1


Risoluzione dei problemi

1. Verificare che Cisco Integrated Services Router (ISR) esegua XE 16.10.1a e versioni successive (per il metodo IOx)
2. Verificare che Cisco Integrated Services Router (ISR) sia concesso in licenza con la funzionalità SecurityKey9 abilitata.
3. Verificare che il modello hardware dell'RCI sia conforme al profilo di risorse minimo.
4. Funzionalità non compatibile con SYN-cookie e Network Address Translation 64 (NAT64) del firewall basato su zone
5. Verificare che il servizio UTD sia stato avviato dopo l'installazione.
6. Durante il download manuale del pacchetto di firma, assicurarsi che il pacchetto abbia la stessa versione del motore Snort. L'aggiornamento del pacchetto di firma potrebbe non riuscire se le versioni non corrispondono.
7. In caso di problemi di prestazioni, usare le 'show app-hosting resource' e 'show app-hosting usage appid "UTD-NAME' per informazioni sull'utilizzo di CPU/memoria/spazio di archiviazione.

```
Router#show app-hosting resource
CPU:
Quota: 75(Percentage)
Available: 50(Percentage)
VCPU:
Count: 6
Memory:
Quota: 10240(MB)
Available: 9216(MB)
Storage device: bootflash
Quota: 4000(MB)
Available: 4000(MB)
Storage device: harddisk
Quota: 20000(MB)
Available: 19029(MB)
Storage device: volume-group
Quota: 190768(MB)
Available: 169536(MB)
Storage device: CAF persist-disk
Quota: 20159(MB)
Available: 18078(MB)
```

```
Router#show app-hosting utilization appid utd
Application: utd
CPU Utilization:
CPU Allocation: 33 %
CPU Used: 3 %
Memory Utilization:
Memory Allocation: 1024 MB
```

Memory Used: 117632 KB
Disk Utilization:
Disk Allocation: 711 MB
Disk Used: 451746 KB

 Avviso: se il livello di utilizzo della CPU, della memoria o del disco è elevato, contattare Cisco TAC.

Debug

Utilizzare i comandi di debug elencati di seguito per raccogliere informazioni su Snort IPS in caso di errore.

<#root>

```
debug virtual-service all
```

```
debug virtual-service virtualPortGroup
```

```
debug virtual-service messaging
```

```
debug virtual-service timeout
```

```
debug utd config level error [error, info, warning]  
debug utd engine standard all
```

Informazioni correlate

Ulteriori documenti relativi alla distribuzione di Snort IPS sono disponibili qui:

Guida alla configurazione della protezione IPS Snort

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html

Profilo risorse servizio virtuale

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html#id_31952

Avviare IPS sui router - configurazione dettagliata.

<https://community.cisco.com/t5/security-knowledge-base/router-security-snort-ips-on-routers-step-by-step-configuration/ta-p/3369186>

Risoluzione dei problemi relativi a Snort IPS

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html#concept_C3C869E633A6475890475931DF83EBCC

ISR4K Snort IPS non è distribuito perché il firmware non dispone di risorse di piattaforma sufficienti

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwf57595>

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).