SDWAN Cisco IOS XE TLS Syslog-configuratie op syslog-ing server

Inhoud

Inleiding

Dit document beschrijft een uitgebreide handleiding voor het configureren van een TLS Syslog-server op SD-WAN Cisco IOS® XE-apparaten.

Voorwaarden

Zorg ervoor dat u aan de volgende vereisten voldoet voordat u overgaat tot de configuratie van een TLS Syslog-server op SD-WAN Cisco IOS XE-apparaten:

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SD-WAN controllers - Zorg ervoor dat uw netwerk is voorzien van correct geconfigureerde SD-WAN controllers.
- Cisco IOS XE SD-WAN router - Een compatibele router die het Cisco IOS XE SD-WAN beeld uitvoert.
- Syslog Server - Een op Ubuntu gebaseerde Syslog-server, zoals syslog-ng, om loggegevens te verzamelen en te beheren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- vManage: Versie 20.9.4
- Cisco IOS XE SD-WAN: Versie 17.9.4
- Ubuntu: Versie 2.04
- syslog-ng: Versie 3.27

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratie

1. Installatie van syslog-ng op Ubuntu Machine

Om syslog-ng op uw Ubuntu-server in te stellen, moet u deze stappen volgen om een juiste installatie en configuratie te waarborgen.

Stap 1. Netwerkinstellingen configureren

Na het installeren van Ubuntu Server, configureer een statisch IP-adres en DNS-server om er zeker van te zijn dat de machine toegang tot het internet heeft. Dit is cruciaal voor het downloaden van pakketten en updates.

Stap 2. Installeer syslog-ng

Open een terminal op uw Ubuntu-machine en voer:

```
sudo apt-get install syslog-ng sudo apt-get install syslog-ng openssl
```

2. Installeer de basiscertificeringsinstantie op de Syslog Server voor serververificatie

Maakt mappen en genereert toetsen

```
cd /etc/syslog-ng mkdir cert.d key.d ca.d cd cert.d openssl genrsa -out ca.key 2048 openssl req -new -x
```

Vingerafdruk berekenen

Voer de opdracht uit en kopieer de uitvoer:

openssl x509 -in PROXY-SIGNING-CA.ca -vingerafdruk -noout | wk -F "=" "{print $2}" | Gebruikt 's/://g' | T-vingerafdruk.txt
Voorbeeld uitvoer: 54F371C8E2BFB06E2C2D0944245C288FB07163

3. Syslog-ng serverconfiguratiebestand configureren

Bewerk het syslog-ng configuratiebestand:

```
sudo nano /etc/syslog-ng/syslog-ng.conf
```

Voeg de configuratie toe:

```
source s_src { network( ip(0.0.0.0) port(6514) transport("tls") tls( key-file("/etc/syslog-ng/key.d/ca.
```

4. Installeer de Root Certificate Authority op Cisco IOS XE SD-WAN apparaat voor serververificatie

Configureren vanaf CLI

1. Geef de configuratiemodus op:

```
config-t
```

2. Configureer het trustpoint:

<#root>

```
crypto pki trustpoint PROXY-SIGNING-CA enrollment url bootflash: revocation-check none rsakeypair PROXY
```

>> The fingerprint configured was obtained from the fingerprint.txt file above

```
 commit
```

3. Kopieert de PROXY-SIGNING-CA.ca bestand van uw syslog server naar de router bootflash met dezelfde naam.

4. Verifieer het trustpoint:

<#root>

```
crypto pki authenticate PROXY-SIGNING-CA
```

example:

Router#crypto pki authenticate PROXY-SIGNING-CA

```
Reading file from bootflash:PROXY-SIGNING-CA.ca
Certificate has the attributes:
Fingerprint MD5: 7A97B30B 2AE458FF D9E7D91F 66488DCF
Fingerprint SHA1: 21E0F09B B67B2E9D 706DBE69 856E5AA3 D39A268A
Trustpoint Fingerprint: 21E0F09B B67B2E9D 706DBE69 856E5AA3 D39A268A
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
```

5. Neem het trustpoint in:

<#root>

```
crypto pki enroll PROXY-SIGNING-CA
```

example:

vm32#crypto pki enroll PROXY-SIGNING-CA

```
Start certificate enrollment ..
The subject name in the certificate will include: cn=proxy-signing-cert
The fully-qualified domain name will not be included in the certificate
Certificate request sent to file system
The 'show crypto pki certificate verbose PROXY-SIGNING-CA' commandwill show the fingerprint.
```

6. Kopieert de PROXY-SIGNING-CA.req bestand van de router naar de syslog server.

Onderteken het certificaat op de Syslog-server

```
openssl x509 -in PROXY-SIGNING-CA.req -req -CA PROXY-SIGNING-CA.ca -CAkey ca.key -out PROXY-SIGNING-CA.
```

7. Het gegenereerde bestand kopiëren (PROXY-SIGNING-CA.crt) aan de router bootflash. scp kopiëren: bootflash:

8. Voer het certificaat in:

<#root>

```
crypto pki import PROXY-SIGNING-CA certificate
example:
```

Router# crypto pki import PROXY-SIGNING-CA certificate

```
% The fully-qualified domain name will not be included in the certificate
% Request to retrieve Certificate queued
```

De configuratie valideren

<#root>

```
show crypto pki trustpoint PROXY-SIGNING-CA status

example:
```

Router#show crypto pki trustpoint PROXY-SIGNING-CA status

```
Trustpoint PROXY-SIGNING-CA:
Issuing CA certificate configured:
Subject Name:
o=Internet Widgits Pty Ltd,st=Some-State,c=AU
Fingerprint MD5: 7A97B30B 2AE458FF D9E7D91F 66488DCF
Fingerprint SHA1: 21E0F09B B67B2E9D 706DBE69 856E5AA3 D39A268A
Router General Purpose certificate configured:
Subject Name:
cn=proxy-signing-cert
Fingerprint MD5: 140A1EAB FE945D56 D1A53855 FF361F3F
Fingerprint SHA1: ECA67413 9C102869 69F582A4 73E2B98C 80EFD6D5
Last enrollment status: Granted
State:
Keys generated ..... Yes (General Purpose, non-exportable)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Yes
```

5. TLS-systeemserver configureren op Cisco IOS XE SD-WAN router

Configureer de syslogserver met behulp van de opdrachten:

```
logging trap syslog-format rfc5424 logging source-interface GigabitEthernet0/0/0 logging tls-profile tl
```

6. Verificaties

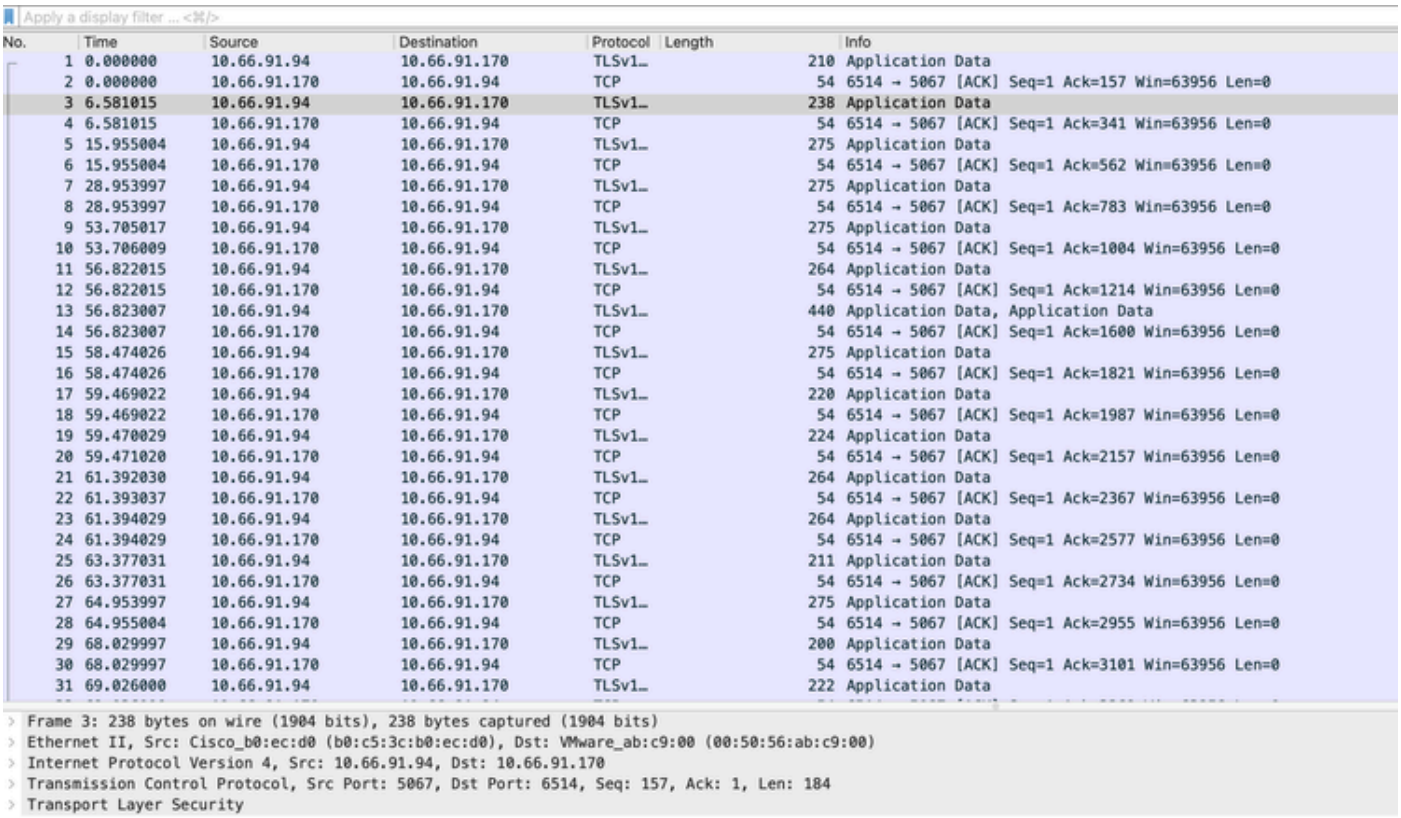
Logbestanden op de router controleren

```
show logging

Showing last 10 lines
Log Buffer (512000 bytes):
Apr 9 05:59:48.025: %DMI-5-CONFIG_I: R0/0: dmiauthd: Configured from NETCONF/RESTCONF by admin, transac
Apr 9 05:59:48.709: %DMI-5-AUTH_PASSED: R0/0: dmiauthd: User 'vmanage-admin' authenticated successfully
Apr 9 05:59:50.015: %LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to administratively
Apr 9 05:59:51.016: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state
Apr 9 05:59:52.242: %SYS-5-CONFIG_P: Configured programmatically by process iosp_dmiauthd_conn_100001_v
```

Logbestanden op de Syslog-server controleren

```
tail -f /var/log/syslog

root@server1:/etc/syslog-ng# tail -f /var/log/syslog
Apr 9 15:51:14 10.66.91.94 188 <189>1 2024-04-09T05:51:51.037Z - - - - - BOM%DMI-5-AUTH_PASSED: R0/0: d
Apr 9 15:59:10 10.66.91.94 177 <189>1 2024-04-09T05:59:47.463Z - - - - - BOM%SYS-5-CONFIG_P: Configured
Apr 9 15:59:10 10.66.91.94 177 <189>1 2024-04-09T05:59:47.463Z - - - - - BOM%SYS-5-CONFIG_P: Configured
Apr 9 15:59:10 10.66.91.94 143 <189>1 2024-04-09T05:59:47.463Z - - - - - BOM%DMI-5-CONFIG_I: R0/0: dmia
Apr 9 15:59:11 10.66.91.94 188 <189>1 2024-04-09T05:59:48.711Z - - - - - BOM%DMI-5-AUTH_PASSED: R0/0: d
Apr 9 15:59:13 10.66.91.94 133 <189>1 2024-04-09T05:59:50.016Z - - - - - BOM%LINK-5-CHANGED: Interface
Apr 9 15:59:13 10.66.91.94 137 <189>1 2024-04-09T05:59:50.016Z - - - - - BOM%LINEPROTO-5-UPDOWN: Line p
Apr 9 15:59:15 10.66.91.94 177 <189>1 2024-04-09T05:59:52.242Z - - - - - BOM%SYS-5-CONFIG_P: Configured
Apr 9 15:59:15 10.66.91.94 177 <189>1 2024-04-09T05:59:52.242Z - - - - - BOM%SYS-5-CONFIG_P: Configured
Apr 9 15:59:18 10.66.91.94 188 <189>1 2024-04-09T05:59:55.286Z - - - - - BOM%DMI-5-AUTH_PASSED: R0/0: d
Apr 9 15:59:21 10.66.91.94 113 <187>1 2024-04-09T05:59:58.882Z - - - - - BOM%LINK-3-UPDOWN: Interface G
Apr 9 15:59:21 10.66.91.94 135 <189>1 2024-04-09T05:59:59.882Z - - - - - BOM%LINEPROTO-5-UPDOWN: Line p
Apr 9 15:59:28 10.66.91.94 177 <189>1 2024-04-09T06:00:05.536Z - - - - - BOM%SYS-5-CONFIG_P: Configured
Apr 9 15:59:43 10.66.91.94 188 <189>1 2024-04-09T06:00:20.537Z - - - - - BOM%DMI-5-AUTH_PASSED: R0/0: d
```

Met Packet Capture screenshot kunt u versleutelde communicatie zien gebeuren:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.66.91.94	10.66.91.170	TLSv1…	210	Application Data
2	0.000000	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=157 Win=63956 Len=0
3	6.581015	10.66.91.94	10.66.91.170	TLSv1…	238	Application Data
4	6.581015	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=341 Win=63956 Len=0
5	15.955004	10.66.91.94	10.66.91.170	TLSv1…	275	Application Data
6	15.955004	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=562 Win=63956 Len=0
7	28.953997	10.66.91.94	10.66.91.170	TLSv1…	275	Application Data
8	28.953997	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=783 Win=63956 Len=0
9	53.705017	10.66.91.94	10.66.91.170	TLSv1…	275	Application Data
10	53.706009	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=1004 Win=63956 Len=0
11	56.822015	10.66.91.94	10.66.91.170	TLSv1…	264	Application Data
12	56.822015	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=1214 Win=63956 Len=0
13	56.823007	10.66.91.94	10.66.91.170	TLSv1…	440	Application Data, Application Data
14	56.823007	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=1600 Win=63956 Len=0
15	58.474026	10.66.91.94	10.66.91.170	TLSv1…	275	Application Data
16	58.474026	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=1821 Win=63956 Len=0
17	59.469022	10.66.91.94	10.66.91.170	TLSv1…	220	Application Data
18	59.469022	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=1987 Win=63956 Len=0
19	59.470029	10.66.91.94	10.66.91.170	TLSv1…	224	Application Data
20	59.471020	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=2157 Win=63956 Len=0
21	61.392030	10.66.91.94	10.66.91.170	TLSv1…	264	Application Data
22	61.393037	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=2367 Win=63956 Len=0
23	61.394029	10.66.91.94	10.66.91.170	TLSv1…	264	Application Data
24	61.394029	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=2577 Win=63956 Len=0
25	63.377031	10.66.91.94	10.66.91.170	TLSv1…	211	Application Data
26	63.377031	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=2734 Win=63956 Len=0
27	64.953997	10.66.91.94	10.66.91.170	TLSv1…	275	Application Data
28	64.955004	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=2955 Win=63956 Len=0
29	68.029997	10.66.91.94	10.66.91.170	TLSv1…	200	Application Data
30	68.029997	10.66.91.170	10.66.91.94	TCP	54	6514 → 5067 [ACK] Seq=1 Ack=3101 Win=63956 Len=0
31	69.026000	10.66.91.94	10.66.91.170	TLSv1…	222	Application Data

Vastlegging ISR4331-branch-NEW_Branch#show

```
Trap logging: level informational, 6284 message lines logged
    Logging to 10.66.91.170  (tls port 6514, audit disabled,
          link up),
          131 message lines logged,
          0 message lines rate-limited,
          0 message lines dropped-by-MD,
          xml disabled, sequence number disabled
          filtering disabled
          tls-profile: tls-proile
    Logging Source-Interface:       VRF Name:
    GigabitEthernet0/0/0
TLS Profiles:
    Profile Name: tls-proile
          Ciphersuites: Default
          Trustpoint: Default
          TLS version: TLSv1.2
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.