SDWAN Cisco IOS XE TLS Syslog-Konfiguration auf einem Syslog-Server

Inhalt

Einleitung

Dieses Dokument beschreibt eine umfassende Anleitung für die Konfiguration eines TLS-Syslog-Servers auf Cisco IOS® XE SD-WAN-Geräten.

Voraussetzungen

Bevor Sie mit der Konfiguration eines TLS-Syslog-Servers auf Cisco IOS XE SD-WAN-Geräten fortfahren, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SD-WAN-Controller: Stellen Sie sicher, dass Ihr Netzwerk über ordnungsgemäß konfigurierte SD-WAN-Controller verfügt.
- Cisco IOS XE SD-WAN-Router - Ein kompatibler Router, auf dem das Cisco IOS XE SD-WAN-Image ausgeführt wird.
- Syslog Server - Ein Ubuntu-basierter Syslog-Server, z. B. syslog-ng, um Protokolldaten zu erfassen und zu verwalten.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- vManage: Version 20.9.4
- Cisco IOS XE SD-WAN: Version 17.9.4
- Ubuntu Version 22.04
- syslog-ng: Version 3.27

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfiguration

1. Installation von syslog-ng auf Ubuntu-Maschine

Um syslog-ng auf Ihrem Ubuntu-Server einzurichten, gehen Sie wie folgt vor, um die korrekte Installation und Konfiguration sicherzustellen.

Schritt 1: Netzwerkeinstellungen konfigurieren

Konfigurieren Sie nach der Installation von Ubuntu Server eine statische IP-Adresse und einen DNS-Server, um sicherzustellen, dass der Computer auf das Internet zugreifen kann. Dies ist entscheidend für das Herunterladen von Paketen und Updates.

Schritt 2: Installieren von syslog-ng

Öffnen Sie ein Terminal auf Ihrem Ubuntu-Computer, und führen Sie Folgendes aus:

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

2. Installation der Stammzertifizierungsstelle auf dem Syslog-Server für die Serverauthentifizierung

Verzeichnisse erstellen und Schlüssel generieren

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

Fingerabdruck berechnen

Führen Sie den Befehl aus, und kopieren Sie die Ausgabe:

openssl x509 -in PROXY-SIGNING-CA.ca -fingerprint -noout | awk -F "=" "{print $2}" | sed 's/://g' | T-Fingerprint.txt
Beispielausgabe: 54F371C8EE2BFB06E2C2D0944245C288FBB07163

3. Konfigurieren der Konfigurationsdatei für den Syslog-ng-Server

Bearbeiten Sie die Konfigurationsdatei syslog-ng:

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

Fügen Sie die Konfiguration hinzu:

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

4. Installation der Root Certificate Authority auf dem Cisco IOS XE SD-WAN-Gerät für die Serverauthentifizierung

Konfiguration über CLI

1. Wechseln Sie in den Konfigurationsmodus:

```
config-t
```

2. Konfigurieren Sie den Vertrauenspunkt:

<#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. Kopieren Sie PROXY-SIGNING-CA.ca Datei vom Syslog-Server auf den Router unter demselben Namen.
4. Authentifizierung des Vertrauenspunkts:

<#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. Registrieren Sie den Trustpoint:

<#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. Kopieren Sie PROXYSIGNIERUNG - CA.req Datei vom Router an den Syslog-Server.

Signieren des Zertifikats auf dem Syslog-Server

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

7. Kopieren Sie die generierte Datei (PROXY-SIGNING-CA.crt) auf den Router bootflash. Kopie scp: Bootflash:

8. Zertifikat importieren:

<#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
```

Validierung der Konfiguration

<#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. Konfigurieren des TLS-Syslog-Servers auf dem Cisco IOS XE SD-WAN-Router

Konfigurieren Sie den Syslog-Server mithilfe der folgenden Befehle:

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

6. Überprüfungen

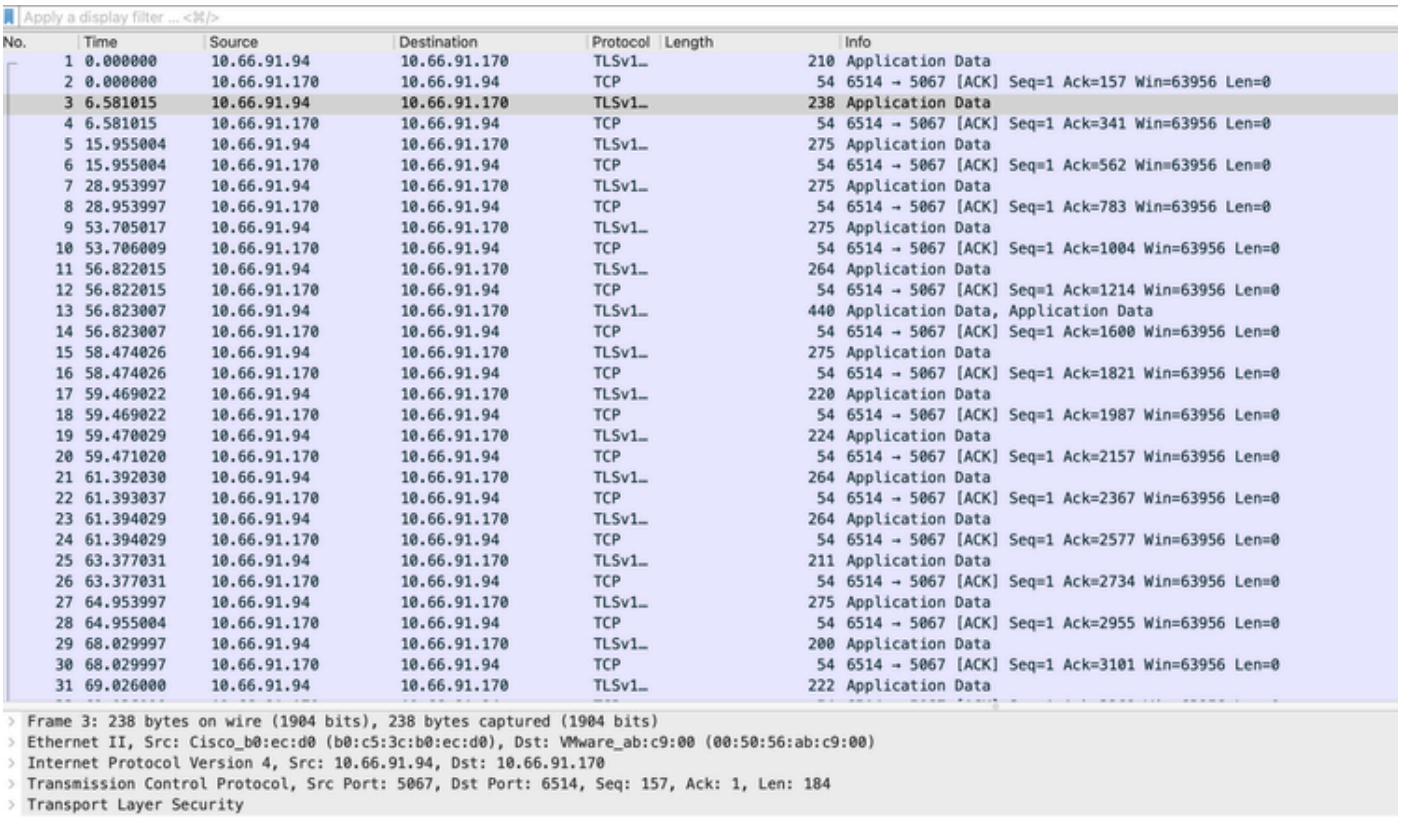
Protokolle auf dem Router überprüfen

```
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
```

Protokolle auf dem Syslog-Server überprüfen

```
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
```

Screenshot der Paketerfassung. Sie können sehen, wie verschlüsselte Kommunikation stattfindet:



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

```
> Frame 3: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits)
> Ethernet II, Src: Cisco_b0:ec:d0 (b0:c5:3c:b0:ec:d0), Dst: VMware_ab:c9:00 (00:50:56:ab:c9:00)
> Internet Protocol Version 4, Src: 10.66.91.94, Dst: 10.66.91.170
> Transmission Control Protocol, Src Port: 5067, Dst Port: 6514, Seq: 157, Ack: 1, Len: 184
> Transport Layer Security
```

ISR4331-branch-NEW_Branch#show logging

```
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
```

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung

verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.