Setzen Sie den Intrusion Detection System 8280-Sensor ein

Veröffentlicht: 2024-02-12

Sensoren des Intrusion Detection Systems (Intrusion Detection System) lassen sich in Paketsensoren integrieren, um Erkennungen auf der Grundlage von IDS-Signaturen nach Industriestandard zu generieren. In dieser Anleitung wird erklärt, wie der im Rack montierte Intrusion Detection System 8280 installiert wird Sensor.

Voraussetzungen für die Installation

Um den Sensor zu installieren, muss Ihre Umgebung die folgenden Anforderungen erfüllen:

Fühler

1 HE Rackplatz und elektrische Anschlüsse für 2 x 750-W-Stromversorgungen.

Verwaltung

Ein 10/100/1000 BASE-T-Netzwerkanschluss für Sensor Verwaltung.

Überwachung (Erfassung)

Hochleistungsschnittstellen: Ein bis zwei Netzwerkanschlüsse für den Anschluss an 25-GbE- oder 10-GbE-Paketdatenquellen.
Verwaltungs- und Überwachungsschnittstellen: Ein bis drei Netzwerkanschlüsse für den Anschluss an 1-GbE-Paketdatenquellen.

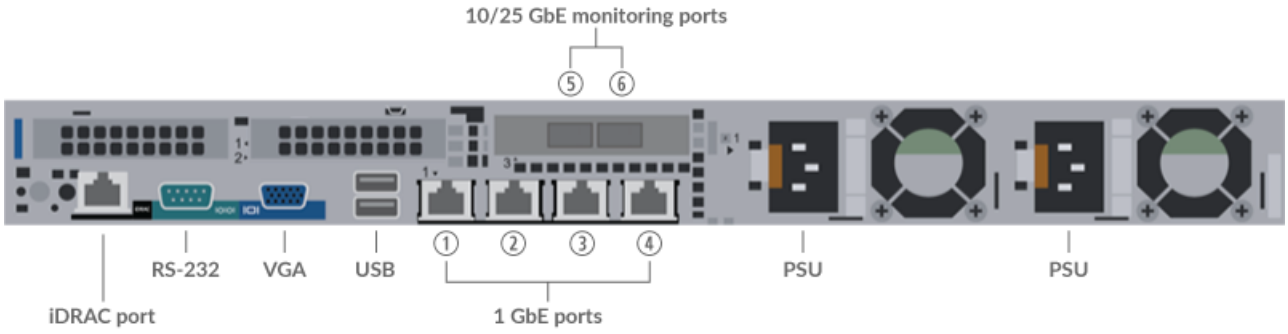
Zugriff auf das Netzwerk

Stellen Sie sicher, dass Administratoren auf die Administrationseinstellungen auf der Sensor über TCP-Port 443.

Weitere Informationen zu den Schnittstellen auf dem ExtraHop-System finden Sie in der Häufig gestellte Fragen zur ExtraHop Hardware.

Anschlüsse auf der Rückseite

VON 8280



- Ein iDRAC-Schnittstellenport
- Eine serielle RS-232-Schnittstelle zum Anschließen eines Konsolengeräts
- Ein VGA-Anschluss zum Anschließen eines externen Displays
- Zwei USB 3.0-Anschlüsse zum Anschließen von Eingabegeräten wie Tastatur und Maus
- Zwei Stromanschlüsse zum Anschließen der Sensor an eine Wechselstromquelle
- Vier 10/100/1000 BASE-T-Netzwerkanschlüsse. Port 1 ist der primäre Management-Port. Die Ports 2-4 sind die Management + Monitor-Ports.

- Zwei 25-GBE-fähige Ports an einem Netzwerkadapter. Die Ports 5 und 6 sind die Hochleistungsschnittstellen zur Überwachung (Erfassung).

Unterstützte Paketquellenkonnektivität

Der Intrusion Detection System 8280 kann Pakete über die Monitoring-Ports 2 bis 6 annehmen. Die Anschlüsse können gemäß der folgenden Tabelle angeschlossen werden.

Intrusion Detection System 8280 Stecker	Peer-Connector für Paketquelle	Vom Kunden bereitgestellte Verkabelung	Unterstützte Betriebsgeschwindigkeiten
Transceiver-basierte Konnektivität			
25-GbE-SFP28-SR-Transceiver	25-GbE-SFP28-SR-Transceiver	Multimode-Glasfaser LC-Stecker	25 Gbit/s, 10 Gbit/s
	10-GbE-SFP+-SR-Transceiver	Multimode-Glasfaser LC-Stecker	10 Gbit/s
Direct Attach-Konnektivität			
Vom Kunden bereitgestelltes SFP28-DAC-Kabel, z. B. die Mellanox MCP2M00-Axxx-Serie			25 Gbit/s
Vom Kunden bereitgestelltes RJ45-Ethernet-Kabel			1 Gbit/s

Richtlinien zur Verkehrsverteilung

- Pakete aus demselben Fluss sollten auf derselben Schnittstelle oder auf Schnittstellen derselben Netzwerkschnittstellenkarte (NIC) empfangen werden.
- Wenn Ihr Datenfeed nicht beide Schnittstellen auf der NIC benötigt, deaktivieren Sie die unkonfigurierten Schnittstellen in den Administrationseinstellungen.
- Es wird erwartet, dass ein einzelnes Hochleistungs-ERSPAN-Target 20 bis 30 Gbit/s verarbeitet. Auf einem größeren Sensoren, verteilen Sie den ERSPAN-Verkehr auf mehr Schnittstellen, um die Datenaufnahme zu skalieren.

Richten Sie den Sensor ein

1. Montieren Sie den Sensor im Rack.

   Installieren Sie den Sensor mit dem mitgelieferten Rackmontagesatz in Ihrem Rechenzentrum. Das Montageset unterstützt die meisten Racks mit vier Pfosten und runden oder quadratischen Löchern.

   Richten Sie die Hardware so aus, dass ein ordnungsgemäßer Luftstrom gewährleistet ist. Der Kaltlufteinlass erfolgt durch die Vorderseite des Sensor.
2. Verbinden Sie Port 1 mit Ihrem Verwaltungsnetzwerk.

   Dieser Sensor hat zwei 10/100/1000 BASE-T-Netzwerkanschlüsse. Verbinden Sie den Management-Port mit einem Netzwerk-Patchkabel am Sensor zu Ihrem Management-Netzwerk. Port 1 ist der Standard-Management-Port.
3. Verbinden Sie den Überwachungsanschluss.

   Wichtig: Um die beste Leistung bei der ersten Gerätesynchronisierung zu gewährleisten, schließen Sie alle Sensoren an die Konsole an und konfigurieren Sie dann die Weiterleitung des Netzwerkverkehrs zu den Sensoren.

Verbinden Sie mit dem entsprechenden Netzwerkkabel einen Überwachungsanschluss am Sensor mit einem Netzwerk-Tap- oder Mirror-Anschluss am Switch.

Wichtig: Der Intrusion Detection System 8280 benötigt einen doppelten Feed des Datenverkehrs, der an den Paketsensor gesendet wird.

Hinweis: Die Verbindungsleuchten an den Anschlüssen der Überwachungsschnittstelle leuchten erst auf, wenn Sie den ExtraHop-Sensor, den Recordstore oder den Packetstore mit Ihrem Produktschlüssel registriert haben.

4. Optional: Verbinden Sie den iDRAC-Anschluss.

   Um die Remoteverwaltung der zu aktivieren Sensor, verbinden Sie Ihr Verwaltungsnetzwerk mit einem Netzwerk-Patchkabel mit dem iDRAC-Anschluss.

5. Montieren Sie die Frontblende.

   Sie müssen die Frontblende anbringen, wenn Sie den Sensor über das LCD-Display konfigurieren möchten.

   Stecken Sie den USB-Anschluss auf der rechten Seite der Blende in den USB-Anschluss an der Vorderseite des Sensor. Drücken und halten Sie die Auslösetaste am linken Ende der Blende und drücken Sie die Blende bündig mit dem Sensor, bis sie einrastet.

6. Schließen Sie die Netzkabel an.

   Verbinden Sie die beiden mitgelieferten Netzkabel mit den Netzteilen auf der Rückseite des Sensor und stecken Sie die Kabel dann in eine Steckdose. Wenn sich der Sensor nicht automatisch einschaltet, drücken Sie den Netzschalter ⏻ auf der Vorderseite rechts am Sensor.

Konfigurieren Sie die Verwaltungs-IP-Adresse

DHCP ist auf dem ExtraHop-System standardmäßig aktiviert. Wenn Sie das System einschalten, versucht Interface 1, eine IP-Adresse über DHCP abzurufen. Bei Erfolg wird die IP-Adresse auf dem Startbildschirm der LCD-Anzeige angezeigt.

Wenn Ihr Netzwerk DHCP nicht unterstützt, können Sie eine statische IP-Adresse über das LCD-Menü auf der Vorderseite oder über die Befehlszeilenschnittstelle (CLI) konfigurieren.

Wichtig: Wir empfehlen dringend Konfiguration eines eindeutigen Hostnamens. Wenn sich die System-IP-Adresse ändert, kann die ExtraHop-Konsole die Verbindung zum System einfach über den Hostnamen wiederherstellen.

Konfigurieren Sie eine statische IP-Adresse über das LCD

Gehen Sie wie folgt vor, um eine IP-Adresse manuell über die LCD-Bedienelemente an der Frontblende zu konfigurieren.

1. Stellen Sie sicher, dass die Standard-Verwaltungsschnittstelle mit dem Netzwerk verbunden ist und der Verbindungsstatus aktiv ist.
2. Drücken Sie die Auswahltaste (✓), um zu beginnen.
3. Drücken Sie die Abwärtspfeiltaste, um auszuwählen `Network`, und drücken Sie dann die Auswahltaste.
4. Drücken Sie den Abwärtspfeil, um auszuwählen `Set static IP`, und drücken Sie dann die Auswahltaste.
5. Drücken Sie die Links- oder Rechtspfeile, um die erste Ziffer auszuwählen, die geändert werden soll, und drücken Sie dann die Aufwärts- oder Abwärtspfeile, um die Ziffer in die gewünschte Zahl zu ändern. Wiederholen Sie diesen Schritt für jede Ziffer, die Sie ändern müssen. Nachdem Sie die gewünschte IP-Adresse konfiguriert haben, drücken Sie die Auswahltaste.
6. Auf dem `Network mask` Bildschirm, drücken Sie die Links- oder Rechtspfeile, um die erste Ziffer auszuwählen, die geändert werden soll, und drücken Sie dann die Aufwärts- oder Abwärtspfeile, um die Ziffer in die gewünschte Zahl zu ändern. Wiederholen Sie diesen Schritt für jede Ziffer, die Sie

ändern müssen. Nachdem Sie die gewünschte Netzwerkmaske konfiguriert haben, drücken Sie die Auswahltaste.

7. Auf dem `Default gateway` Bildschirm, drücken Sie die Links- oder Rechtspfeile, um die erste Ziffer auszuwählen, die geändert werden soll, und drücken Sie dann die Aufwärts- oder Abwärtspfeile, um die Ziffer in die gewünschte Zahl zu ändern. Wiederholen Sie diesen Schritt für jede Ziffer, die Sie ändern müssen. Nachdem Sie das gewünschte Standard-Gateway konfiguriert haben, drücken Sie die Auswahltaste.
8. Bestätigen Sie Ihre geänderten Netzwerkeinstellungen auf der `Settings saved` Bildschirm, und drücken Sie dann eine beliebige Taste, um zum `Network Menu`.
9. Drücken Sie den Abwärtspfeil und scrollen Sie zu `Set DNS servers`, und drücken Sie dann die Auswahltaste.
10. Drücken Sie die Links- oder Rechtspfeile auf der `DNS1` Bildschirm, um die erste Ziffer auszuwählen, die geändert werden soll, und drücken Sie dann die Aufwärts- oder Abwärtspfeile, um die Ziffer auf die gewünschte Zahl zu ändern. Wiederholen Sie diesen Schritt für jede Ziffer, die Sie ändern müssen, und drücken Sie dann die Auswahltaste, um mit der `DNS2` Bildschirm.
11. Konfigurieren Sie einen zweiten DNS-Server.
12. Bestätigen Sie die DNS-Einstellungen auf der `Settings saved` Bildschirm, und drücken Sie dann eine beliebige Taste, um zum `Network Menu`.
13. Drücken Sie zweimal den Abwärtspfeil bis ← `Back` erscheint, und drücken Sie dann die Auswahltaste.
14. Drücken Sie zweimal den Abwärtspfeil, um iDRAC auszuwählen. Konfigurieren Sie iDRAC DHCP, IP, Maske, Gateway und DNS auf die gleiche Weise wie die IP-Adresse.
15. Drücken Sie die `X` Taste, um zum Hauptmenü zurückzukehren.

Konfigurieren Sie eine IP-Adresse über die CLI

Sie können auf die CLI zugreifen, indem Sie eine USB-Tastatur und einen SVGA-Monitor an die Appliance anschließen oder über ein serielles RS-232-Kabel (Nullmodem) und ein Terminalemulatorprogramm. Stellen Sie den Terminalemulator auf 115200 Baud mit 8 Datenbits, ohne Parität, 1 Stoppbit (8N1) und deaktivierter Hardware-Flusskontrolle ein.

1. Stellen Sie eine Verbindung zum ExtraHop-System her.
2. Geben Sie in der Anmeldeaufforderung Folgendes ein `Schale` und drücken Sie dann die EINGABETASTE.
3. Geben Sie in der Passwortabfrage die Seriennummer des Systems ein, und drücken Sie dann die EINGABETASTE. Die Seriennummer ist auf einem Etikett auf der Rückseite des Geräts aufgedruckt. Die Seriennummer finden Sie auch auf dem LCD-Display an der Vorderseite des Geräts in der `Info` Abschnitt.
4. Aktiviere privilegierte Befehle:

   ```
   enable
   ```

5. Geben Sie in der Passwortabfrage die Seriennummer ein, und drücken Sie dann die EINGABETASTE.
6. Rufen Sie den Konfigurationsmodus auf:

   ```
   configure
   ```

7. Rufen Sie den Schnittstellenkonfigurationsmodus auf:

   ```
   interface
   ```

8. Starte den `ip` Befehl und geben Sie die IP-Adresse und die DNS-Einstellungen im folgenden Format an:
   `ip ipaddr <ip_adresse> <Netzmaske> <Tor> <DNS-Server>`

Zum Beispiel:

```
ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
```

9. Verlassen Sie den Schnittstellenkonfigurationsmodus:

```
exit
```

10. Speichern Sie die laufende Konfigurationsdatei:

```
running_config save
```

11. Typ y und drücken Sie dann ENTER.

Das System konfigurieren

Gehen Sie wie folgt vor, um den IDS-Sensor zu konfigurieren.

1. Registrieren Sie Ihr ExtraHop-System.
2. Stellen Sie eine Verbindung zu ExtraHop Cloud Services her.
3. Verbinde deine Konsole mit dem Sensor.
   - Informationen zum Herstellen einer Verbindung mit einer selbstverwalteten Konsole finden Sie unter Eine ExtraHop-Konsole mit einem ExtraHop-Sensor verbinden.
   - Informationen zum Herstellen einer Verbindung mit Reveal (x) 360 finden Sie unter Stellen Sie über selbstverwaltete Sensoren eine Verbindung zu Reveal (x) 360 her.
4. Verbinden Sie den IDS-Sensor mit einer Standort.
   - Für Reveal (x) Enterprise
     1. Klicken Sie auf der Seite „Verbundene Geräte verwalten“ der Konsole auf **Aktionen** neben dem IDS-Sensor und dann klicken **Seite beitreten** von der Appliance-Aktionen Drop-down-Liste.
     2. Aus dem Verbundene Seite Klicken Sie in der Dropdownliste auf den Namen der Standort, der Sie beitreten möchten. Sie müssen einer Standort beitreten, die denselben Netzwerk-Feed wie der IDS-Sensor hat.
     3. klicken **Seite beitreten**.
   - Für Reveal (x) 360
     1. Bei der Enthüllung (x) 360 **Verwaltung** > **Sensorik** Wählen Sie auf der Seite das Kontrollkästchen neben dem Namen des IDS-Sensors aus.
     2. Auf dem Einzelheiten zum Sensor Bereich, wählen Sie den Namen der Standort, der Sie beitreten möchten, aus dem **Verbundene Seite** Drop-down-Liste. Sie müssen einer Standort beitreten, die denselben Netzwerk-Feed wie der IDS-Sensor hat.
     3. klicken **Seite beitreten**.
5. Optional: Wählen Sie die IDS-Erkennungen Abstimmungsparameter um die Erkennung von eingehender Datenverkehr von externen Endpunkten zu ermöglichen.

   Standardmäßig generiert das ExtraHop-System nur Erkennungen für internen Datenverkehr.
6. Führen Sie die empfohlenen Verfahren in der Checkliste für die Zeit nach der Bereitstellung.