Stellen Sie den Intrusion Detection System 9380-Sensor bereit

Veröffentlicht: 2024-02-12

Die Sensoren des Intrusion Detection Systems (Intrusion Detection System) sind in Paketsensoren integriert, um Erkennungen auf der Grundlage branchenüblicher IDS-Signaturen zu generieren. In dieser Anleitung wird erklärt, wie der Intrusion Detection System 9380 im Rack montiert wird Sensor.

Voraussetzungen für die Installation

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

Fühler

2 HE Rackfläche und elektrische Anschlüsse für 2 x 800-W-Stromversorgungen.

Verwaltung

Ein 10/100/1000 BASE-T-Netzwerkanschluss oder ein 10G BASE-SR-Port für die Sensorverwaltung.

Überwachung (Erfassung)

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

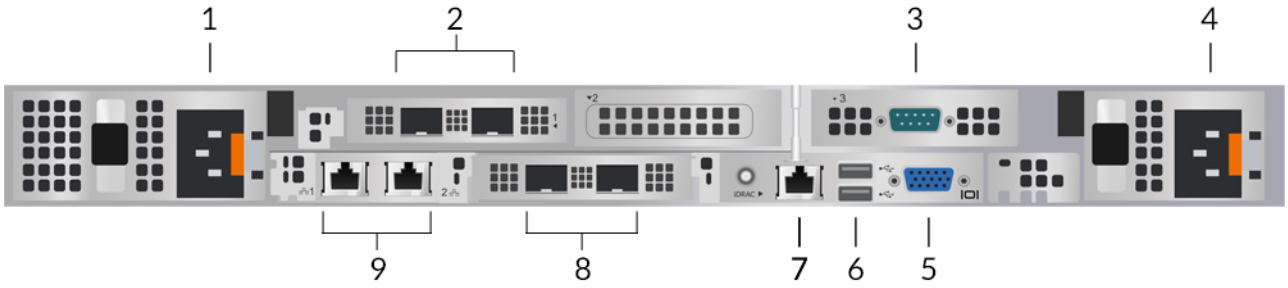
Zugriff auf das Netzwerk

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

Intrusion Detection System 980



1. Netzteil (PSU1) zum Anschluss des Sensor an eine Wechselstromquelle
2. Zwei 25-GbE-fähige Ports an zwei Netzwerkadaptern
3. Ein serieller RS-232-Anschluss zum Anschließen eines Konsolengeräts
4. Netzteil (PSU2) zum Anschluss des Sensor an eine Wechselstromquelle
5. Ein VGA-Anschluss zum Anschluss eines externen Displays
6. Zwei USB 3.0-Anschlüsse zum Anschließen von Eingabegeräten wie Tastatur und Maus

7. Ein iDRAC-Schnittstellenport
8. Zwei 10-GbE-Anschlüsse. Die Ports 3 und 4 können als Management-Port, Management- und Flow-Ziel oder Management und RPCAP/ERSPAN/VXLAN/GENEVE-Ziel konfiguriert werden.

   Hinweis: Diese Ports dienen auch als leistungsstarke Überwachungs- (oder Erfassungs-) Schnittstellen. Die Verarbeitung von RPCAP-, ERSPAN-, VXLAN- und GENEVE-Verkehr ist in den Modi „Management + RPCAP/ERSPAN/VXLAN/GENEVE“ auf 1 Gbit/s pro Schnittstelle begrenzt, aber die Ports unterstützen in den Zielmodi Monitoring und High-Performance ERSPAN/VXLAN/GENEVE bis zu 10 Gbit/s pro Schnittstelle.
9. Zwei 10/100/1000 BASE-T-Netzwerkanschlüsse. Die Ports 1 und 2 können als Management-Port, Management- und Flow-Ziel oder Management und RPCAP/ERSPAN/VXLAN/GENEVE-Ziel konfiguriert werden.

   Hinweis: In Umgebungen mit asymmetrischem Routing neben den Hochleistungsschnittstellen gelangen Ping-Antworten möglicherweise nicht an den Absender zurück.

Unterstützte Paketquellenkonnektivität

Der Sensor akzeptiert Pakete über die Ports 1 bis 8. Verbinden Sie die Anschlüsse gemäß der folgenden Tabelle.

Stecker	Peer-Connector für Paketquelle	Vom Kunden bereitgestellte Verkabelung	Unterstützte Betriebsgeschwindigkeiten
Transceiverbasierte Konnektivität			
2,5-GbE-SFP28-SR-Transceiver	2,5-GbE-SFP28-SR-Transceiver	Multimode-Glasfaser LC-Stecker	25 Gbit/s, 10 Gbit/s
	10GbE 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.
- Die Aufnahme auf jeder Netzwerkkarte sollte 75% des bewerteten Analysedurchsatzes für die Sensor um sicherzustellen, dass der Datenverkehr auf die Systemressourcen verteilt ist.
- Wenn Ihr Datenfeed nicht beide Schnittstellen auf der NIC benötigt, deaktivieren Sie die unkonfigurierten Schnittstellen in den Administrationseinstellungen. Konfigurieren Sie den Sensor beispielsweise mit einer einzigen Schnittstelle, um 50 Gbit/s auf jeder Netzwerkkarte aufzunehmen. Deaktivieren Sie die externen Ports auf jeder Netzwerkkarte. Diese Konfiguration optimiert die Leistung für 100 Gbit/s.
- 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 das im Rack Sensor.

   Installieren Sie den Sensor in Ihrem Rechenzentrum mit dem mitgelieferten Rackmontagesatz. 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 vier 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.

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

   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.

   Wichtig: Der IDS-Sensor 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 das konfigurieren möchten Sensor durch das LCD-Display.

   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 es einrastet.
6. Schließen Sie die Netzkabel an.

   Verbinden Sie die beiden mitgelieferten Netzkabel mit den Netzteilen (PSUs) auf der Rückseite des Sensor, und stecken Sie dann die Kabel in eine Steckdose. Wenn der Sensor schaltet sich nicht automatisch ein, drücken Sie den Netzschalter vorne rechts auf dem Sensor.

Konfiguration der 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-Steuerelemente auf der Vorderseite zu konfigurieren.

1. Stellen Sie sicher, dass die Standardverwaltungsschnittstelle 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 Pfeiltaste nach links oder rechts, um die erste zu ändernde Ziffer auszuwählen, und drücken Sie dann die Aufwärts- oder Abwärtspfeiltaste, um die Ziffer auf 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 Pfeiltaste nach links oder rechts, um die erste zu ändernde Ziffer auszuwählen, 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. Nachdem Sie die gewünschte Netzwerkmaske konfiguriert haben, drücken Sie die Auswahltaste.
7. Auf dem `Default gateway` Bildschirm, drücken Sie die Pfeiltaste nach links oder rechts, um die erste zu ändernde Ziffer auszuwählen, 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. 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`.

   Hinweis: Jeder Adresse ist ein Buchstabe vorangestellt, der angibt, ob es sich um die System-IP-Adresse (I), die Gateway-Adresse (G) oder die Netzmaske (N) handelt.
9. Drücken Sie den Abwärtspfeil und scrollen Sie zu `Set DNS servers`, und drücken Sie dann die Auswahltaste.
10. Drücken Sie die Pfeiltasten nach links oder rechts 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 dem `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.
15. Konfigurieren Sie iDRAC DHCP, IP, Maske, Gateway und DNS auf die gleiche Weise wie die IP-Adresse.
16. Drücken Sie die `X` Taste, um zum Hauptmenü zurückzukehren.

Konfigurieren Sie eine IP-Adresse über die CLI

Bevor Sie beginnen
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.
Sie können eine IP-Adresse manuell über die CLI konfigurieren.

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 im `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 spezifizieren Sie die IP-Adresse und DNS Einstellungen im folgenden Format:
   `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 Konfigurationsmodus:

   ```
   exit
   ```
10. Speichern Sie die laufende Konfigurationsdatei:

    ```
    running_config save
    ```
11. Typ `y` und drücken Sie dann die EINGABETASTE.

    Hinweis: Das System aktualisiert die laufende Konfigurationsdatei und wendet die neuen Einstellungen an, wenn eine Verbindung auf der Schnittstelle erkannt wird.

(Optional) Konfigurieren Sie die 10-GbE-Verwaltungsschnittstelle

Sie können einen 10-GbE-Anschluss (Port 1 oder Port 2) konfigurieren, um das System zu verwalten.
Mit den folgenden Befehlen werden die Einstellungen von Port 3 auf Port 1 verschoben und dann Port 3 deaktiviert. Alternativ können Sie die 10-GbE-Verwaltungsschnittstelle in den Administrationseinstellungen konfigurieren.

1. Stellen Sie sicher, dass der Port 1 mit dem 10-GbE-Netzwerk verbunden ist.
2. Stellen Sie eine SSH-Verbindung zum ExtraHop-System her.
3. Geben Sie in der Anmeldeaufforderung Folgendes ein `shell` und drücken Sie dann ENTER.
4. 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 befindet sich auch auf dem LCD-Display an der Vorderseite des Geräts in der `Info` Abschnitt.

5. Aktiviere privilegierte Befehle:

```
enable
```

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

```
configure
```

8. Rufen Sie den Schnittstellenkonfigurationsmodus auf:

```
interface 1
```

9. Verschieben Sie die Schnittstelleneinstellungen:

   Warnung: Dieser Befehl überschreibt die Einstellungen für Interface 1 mit den Einstellungen von Interface 3. Die aktuellen Einstellungen für Interface 1 gehen verloren und Interface 3 wird deaktiviert.

```
take_settings 3
```

10. Typ `Y` um fortzufahren, und drücken Sie dann ENTER.

Den IDS-Sensor 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. Verbinden Sie Ihre ExtraHop-Konsole mit dem Sensor.
   - Informationen zum Herstellen einer Verbindung zu einer selbstverwalteten Konsole finden Sie unter Eine ExtraHop-Konsole mit einem ExtraHop-Sensor verbinden.
   - Informationen zum Herstellen einer Verbindung zu 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.

Option	Description
Für Reveal (x) Enterprise	1. Loggen Sie sich in den Administrationseinstellungen auf der Konsole über `https://<extrahop-hostname-or-IP-address>/admin`. 2. In der Verwaltung verbundener Appliances Abschnitt, klicken **Sensoren verwalten**. 3. Auf dem Verbundene Geräte verwalten Seite, klicken **Aktionen** neben dem IDS-Sensor und dann auf **Seite beitreten** von der Appliance-Aktionen Dropdownliste. 4. Aus dem Verbundene Seite In der Dropdownliste klicken Sie auf den Namen der Standort, der Sie beitreten möchten. Sie müssen einer Standort beitreten, die denselben Netzwerkfeed wie der IDS-Sensor hat. 5. Klicken Sie **Seite beitreten**.
Für Reveal (x) 360	1. Melden Sie sich bei den Verwaltungseinstellungen auf dem Reveal (x) 360-System an über `https://<extrahop-hostname-or-IP-address>/console`. 2. Klicken Sie **Fühler** im linken Bereich. 3. Markieren Sie das Kontrollkästchen neben dem Namen des IDS-Sensors.

Option	Description
	4. Auf dem Angaben zum Sensor Wählen Sie im Bereich den Namen der Standort, der Sie beitreten möchten, aus dem **Verbundene Seite** Dropdownliste. Sie müssen einer Standort beitreten, die denselben Netzwerkfeed wie der IDS-Sensor hat. 5. Klicken Sie **Seite beitreten**.

5. Optional: Wählen Sie die IDS-Erkennungen aus Tuning-Parameter um die Erkennung von eingehender Datenverkehr von externen Endpunkten zu ermöglichen.

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