# Stellen Sie ERSPAN mit einem ExtraHop-Sensor und einem Brocade 5600 vRouter in AWS bereit

Veröffentlicht: 2024-07-02

In diesem Handbuch wird erklärt, wie Sie eine Beispielumgebung innerhalb von Amazon Web Services (AWS) mithilfe der integrierten ERSPAN-Funktionen auf dem ExtraHop installieren und konfigurieren Sensor und der Brocade 5600 vRouter.

Mit Encapsulated RSPAN (ERSPAN) können Sie den Verkehr auf mehreren Netzwerkschnittstellen oder VLANs überwachen und den überwachten Verkehr an ein oder mehrere Ziele senden, einschließlich ExtraHop Sensoren. Konfiguration von ERSPAN auf dem Brocade 5600 vRouter mit dem ExtraHop Sensor ermöglicht zusätzliche geschäftskritische Datenverkehrsanalysen, Überwachung und Transparenz auf AWS und anderen Cloud-Plattformen.

## Zusätzliche Referenzen

Das Dokument setzt ein gewisses Maß an Vertrautheit mit Netzwerken voraus. Für die Ausführung der Schritte in diesem Handbuch ist ein AWS-Konto erforderlich. Wenn Sie neu bei ExtraHop, Brocade oder Amazon Web Services sind, finden Sie unter den folgenden Links weitere Informationen:

- Stellen Sie den ExtraHop bereit Sensor in AWS

  https://docs.extrahop.com/current/install-ehv-de-aws/
- Verwenden des Brocade 5600 vRouter 5600 in AWS

  https://www.brocade.com/content/dam/common/documents/content-types/deployment-guide/brocade-vrouter-5600-amazon-aws-dp.pdf

## Konfigurieren Sie ein AWS Virtual Private Cloud-Netzwerk

In diesem Abschnitt konfigurieren Sie eine neue Virtual Private Cloud (VPC), ein Internet-Gateway, Subnetze und Routing-Dienste.

### Eine VPC erstellen

1. Melden Sie sich bei der AWS-Konsole an.
2. In der Netzwerkbetrieb Abschnitt, klicken **VPC**.
3. In der Virtuelle private Cloud Abschnitt, klicken **Deine VPCs** und dann klicken **VPC erstellen**.
4. In der Namensschild Feld, geben Sie einen Namen für die VPC ein.
5. In der CIDR-Block Feld, geben Sie einen Block von IP-Adressen für das Netzwerk ein, z. B. `10.4.0.0/16`.
6. In der Mietverhältnis Feld, lassen Sie die Option auf gesetzt **Standard**.
7. klicken **Ja, Erstellen**.

   **Hinweis:** Notieren Sie sich die VPC-ID (vpc-nnnnnnnn), die für das nächste Verfahren benötigt wird.

### Ein Internet-Gateway erstellen

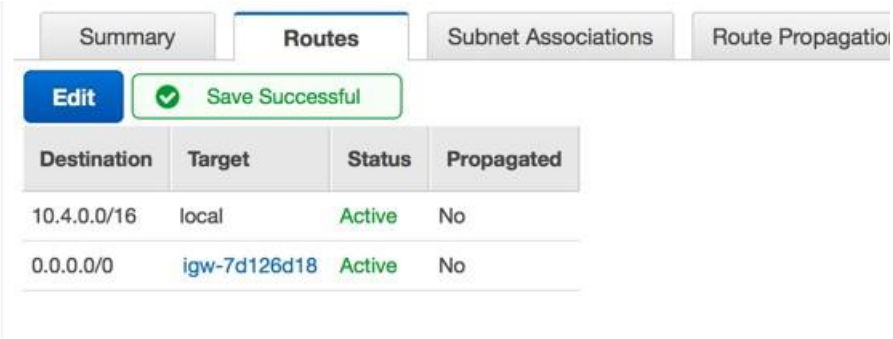
1. Klicken Sie im Navigationsbereich auf **Internet-Gateways**, und klicken Sie dann **Internet-Gateway erstellen**.

2. In der Namensschild Feld, geben Sie einen Namen zur Identifizierung des Internet-Gateways ein.
   Diese Einstellung ermöglicht öffentlichen Verkehr in und aus Ihrer Virtual Private Cloud.
3. klicken **Ja, Erstellen**.
   Notieren Sie sich die Gateway-ID (igw-nnnnnnnn).
4. klicken **An VPC anhängen**.
5. Wählen Sie in der Dropdownliste die VPC aus, die Sie erstellt haben, und klicken Sie dann auf **Ja, anhängen**.

## Routen festlegen

Bevor Datenverkehr in die neue VPC hinein oder aus ihr heraus zugelassen wird, müssen Routing- und Verkehrssicherheitsregeln konfiguriert werden. Standardmäßig ist der gesamte ausgehender Datenverkehr zulässig, eingehender Datenverkehr ist jedoch restriktiver .

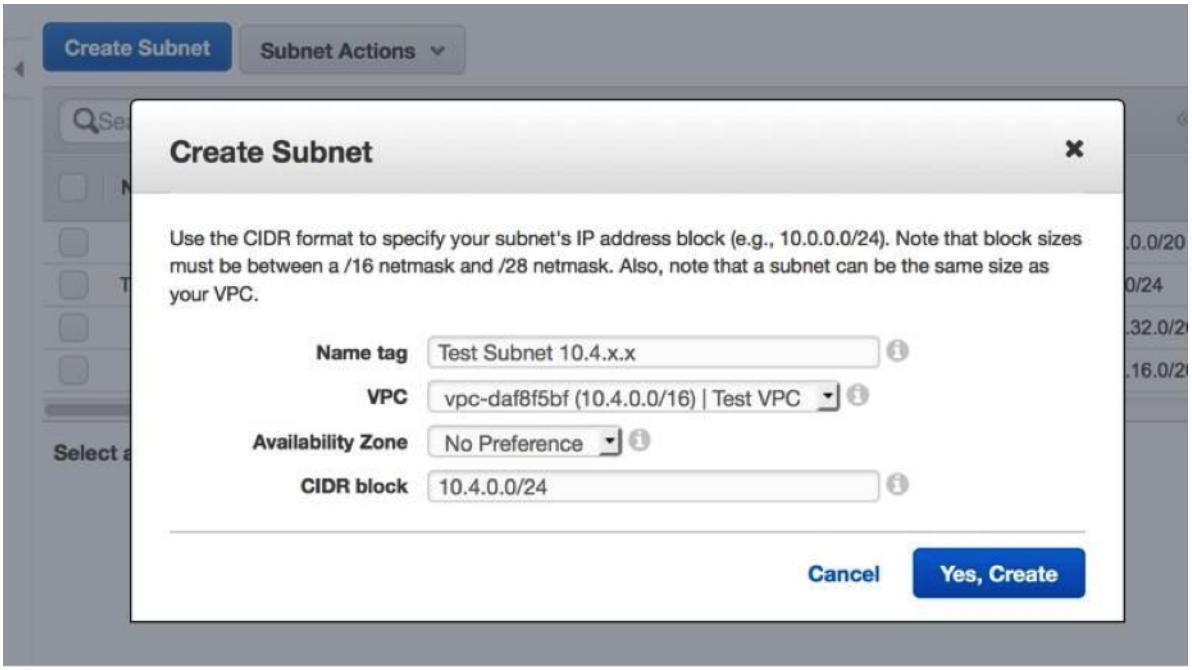
1. Klicken Sie im Navigationsbereich auf **Routentabellen**.
2. Wählen Sie in der Tabelle das Kontrollkästchen neben der Route aus, die mit der von Ihnen erstellten VPC verknüpft ist.
3. Klicken Sie auf **Strecken** Tabulatortaste, und klicken Sie dann auf **Bearbeiten**.
4. klicken **Eine weitere Route hinzufügen**.
5. Geben Sie im Feld Ziel Folgendes ein `0.0.0.0/0`.
6. In der Ziel Feld, geben Sie das Namensschild ein, das Sie für das Internet-Gateway eingegeben haben.
7. klicken **Speichern**.



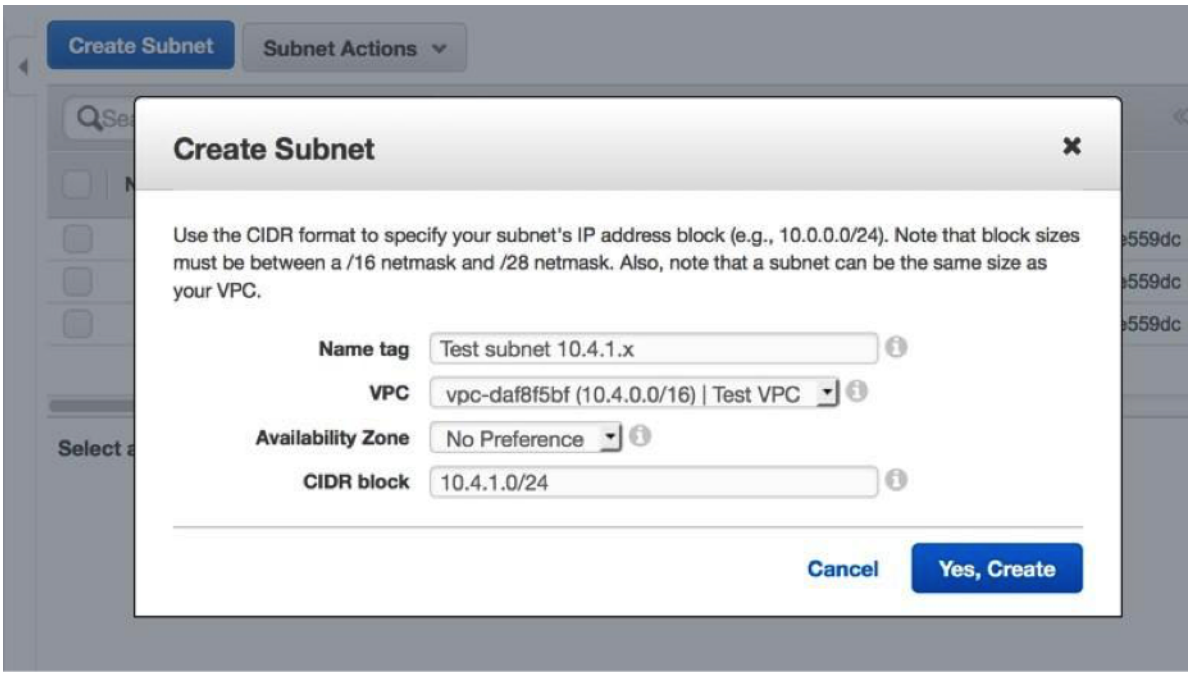

## Erstellen Sie ein Subnetz

Dieses Beispielnetzwerk hat ein öffentliches und ein privates Subnetz innerhalb des CIDR-Blocks, den Sie zuvor konfiguriert haben. Sie konfigurieren 10.4.0.0/24 als öffentliches Subnetz und 10.4.1.0/24 als privates Subnetz.

1. Klicken Sie im Navigationsbereich auf **Subnetze**, und klicken Sie dann **Subnetz erstellen**.
2. In der Namensschild Feld, geben Sie einen Namen für das Subnetz ein.
3. Aus dem **VPC** Wählen Sie in der Dropdownliste die zuvor erstellte VPC aus.
4. Optional: Aus dem **Verfügbarkeitszone** Wählen Sie in der Dropdownliste die Amazon-Verfügbarkeitszone aus, in der sich das Subnetz befinden soll.
5. In der CIDR-Block Feld, geben Sie den öffentlichen CIDR-Block von ein `10.4.0.0/24`.
6. klicken **Ja, Erstellen**.




7. Wiederholen Sie die Schritte 1—6, um ein privates Subnetz mit dem zu erstellen `10.4.1.0/24` CIDR-Block.

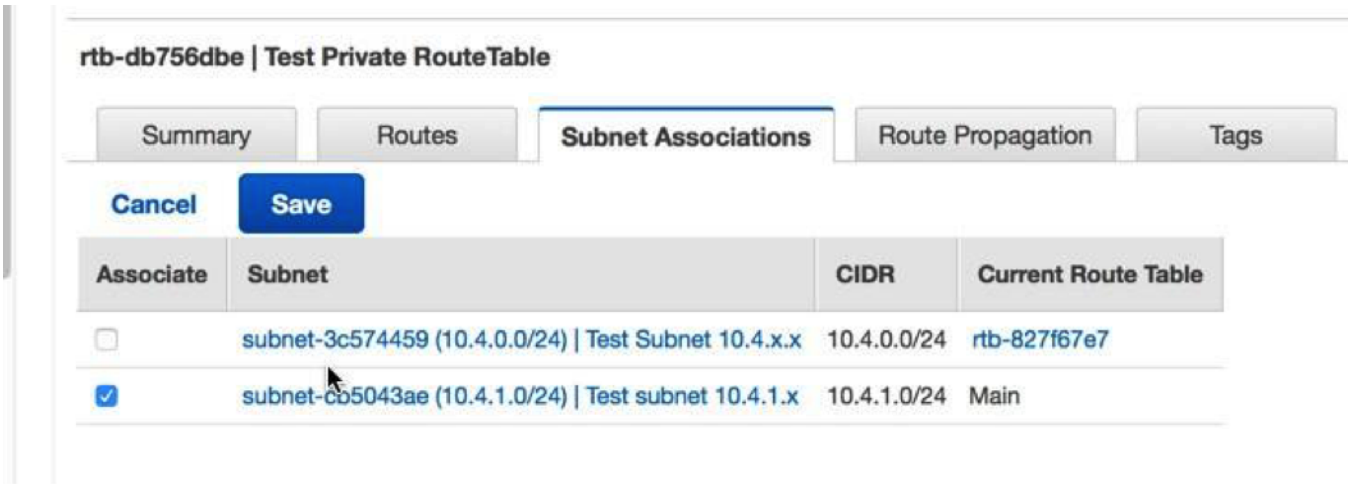



## Ordnen Sie die Routing-Tabelle dem Subnetz zu

1. Klicken Sie im Navigationsbereich auf **Routentabellen**.
2. Stellen Sie sicher, dass es sich bei der ausgewählten Routing-Tabelle um die Tabelle mit dem Internet-Gateway handelt, die Sie zuvor erstellt haben.
3. Klicken Sie auf **Subnetzzuordnungen** Registerkarte.
4. klicken **Bearbeiten** und wählen Sie das öffentliche Subnetz von `10.4.0.0/24`, und klicken Sie dann **Speichern**.


5. klicken **Routentabelle erstellen** um eine neue Routing-Tabelle für das private Subnetz zu erstellen `10.4.1.0/24`.
6. In der Namensschild Feld, geben Sie einen Namen für die Routentabelle ein, wählen Sie die VPC aus, die Sie zuvor erstellt haben, und klicken Sie dann auf **Ja, Erstellen**.
7. Wählen Sie die Routentabelle aus, die für das private Subnetz erstellt wurde `10.4.1.0/24`.
8. Wählen Sie den **Subnetzzuordnungen** Registerkarte.
9. klicken **Bearbeiten** und wählen Sie das private Subnetz `10.4.1.0/24` und dann klicken **Speichern**.

   Notieren Sie sich diese Routentabelle. In einem nachfolgenden Schritt wird eine Zuordnung zur privaten Schnittstelle des Brocade vRouters mit einer Route hergestellt.



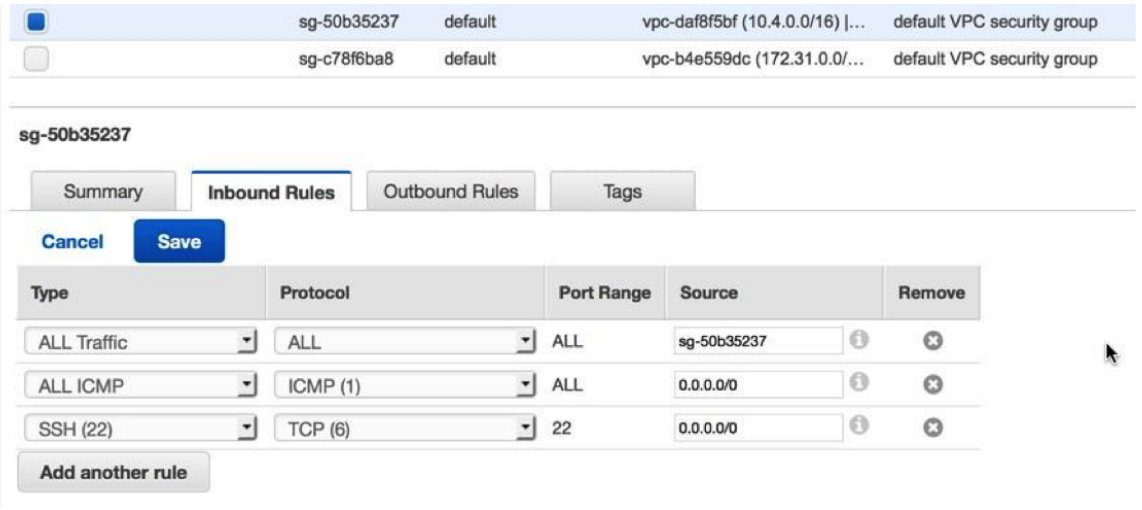

## Regeln für eingehenden Datenverkehr zur Sicherheitsgruppe hinzufügen

1. Wählen Sie im Navigationsbereich Ihre neue VPC aus der **Nach VPC filtern** Pulldown.
2. Klicken Sie im Navigationsbereich auf **Sicherheitsgruppen**.

   Die Sicherheitsgruppe verfügt über Regeln, die den Datenverkehr in die VPC zulassen. Die Ersteinrichtung erlaubt den gesamten Verkehr von sich selbst, alles ICMP (damit Sie den Ping der Schnittstelle testen können) und SSH auf Port 22 testen.
3. Wählen Sie die Standardsicherheitsgruppe für Ihre neue VPC aus.
4. Klicken Sie auf **Regeln für eingehende Nachrichten** Tabulatortaste und dann klicken **Bearbeiten**.
5. klicken **Eine weitere Regel hinzufügen**.
6. Wählen **Alles ICMP** aus der Drop-down-Liste und tippe `0.0.0.0/0` in der Quelle Feld.
7. klicken **Eine weitere Regel hinzufügen**.

8. Wählen **SSH (22)** aus der Drop-down-Liste und tippe `0.0.0.0/0` in der Quelle Feld.
9. klicken **Speichern**.

**Hinweis:** Dies ist eine Konfiguration, die nicht für die Produktion bestimmt ist. Normalerweise würden Sie nicht allen IP-Adressen den Zugriff auf Ihre Instance gestatten.




### Zusammenfassung

In diesem Abschnitt haben Sie eine virtuelle öffentliche Cloud, ein privates Subnetz für das 10.4.1.0/24-Netzwerk und ein öffentliches Subnetz für das 10.4.0.0/24-Netzwerk erstellt. Darüber hinaus haben Sie Routingtabellen für das Routing des Datenverkehrs innerhalb der VPC-Subnetze und extern über ein Internet-Gateway erstellt. Sicherheitsgruppen lassen Datenverkehr in oder aus der VPC zu, und Sie haben die Regeln für eingehenden Datenverkehr so konfiguriert, dass ICMP und SSH-Verkehr.

## Den Brocade 5600v-Router konfigurieren

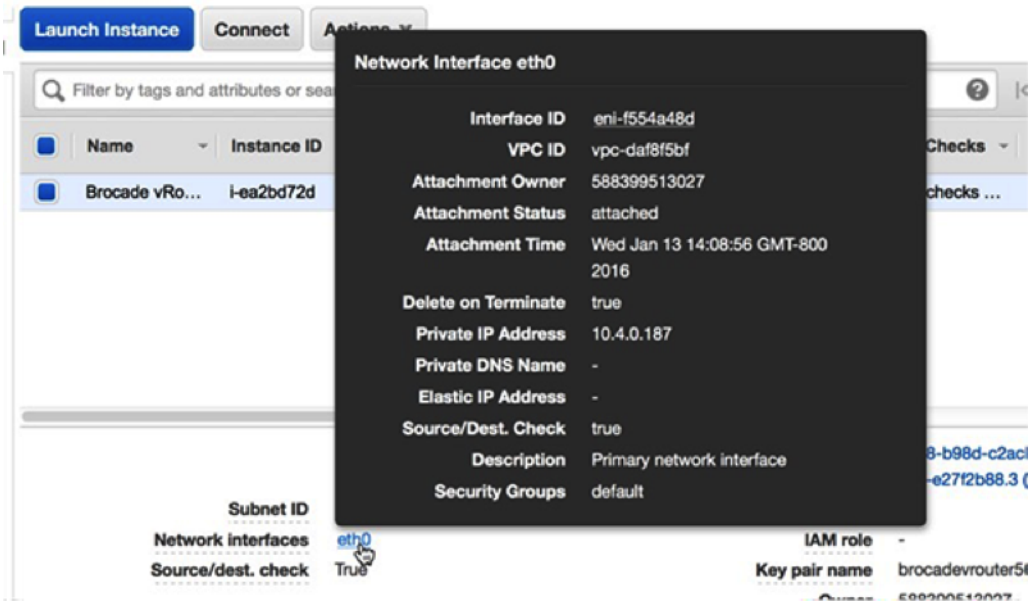
In diesem Abschnitt konfigurieren Sie einen neuen Brocade 5600v-Router innerhalb des zuvor erstellten öffentlichen Subnetzes und weisen eine Elastic IP zu, um das Setup über SSH zu konfigurieren und zu testen.

1. Klicken Sie in der oberen linken Ecke auf das Symbol Console Home, um zur Seite der AWS-Managementkonsole zurückzukehren.
2. Klicken Sie im Abschnitt Berechnen auf **EC2**.
3. Klicken Sie im Navigationsbereich auf **Instanzen**.
4. klicken **Instanz starten** um den Amazon Machine Image (AMI) -Assistenten zu starten.
5. klicken **AWS-Marktplatz** und tippe `5600` oder `Brocade vRouter` in der Suchen Sie nach AWS Marketplace-Produkten Feld und drücken Sie dann die EINGABETASTE.
6. Klicken Sie auf **Wählen** Schaltfläche neben **Brocade 5600 Virtueller Router/Firewall/VPN**.
7. Wählen Sie für dieses Beispiel die **m4. groß** geben Sie den Instanztyp ein und klicken Sie dann **Weiter: Instanzdetails konfigurieren**.
8. Auf dem Instanzdetails konfigurieren Seite, führe die folgenden Schritte aus:
   a) Typ `1` in der Anzahl der Instanzen Feld.
   b) Aus dem **Netzwerk** Wählen Sie in der Dropdownliste die VPC aus, die Sie im ersten Abschnitt dieses Handbuchs erstellt haben.
   c) Wählen Sie aus der Dropdownliste Subnetz das öffentliche Subnetz aus. `10.4.0.0/24`.

d) In der Netzwerkschnittstellen Abschnitt unten auf der Seite, geben Sie `10,4.0,187` in der Primäre IP Feld.

9. klicken **Weiter: Speicher hinzufügen**. Behalten Sie die Standardspeichereinstellungen bei und klicken Sie dann auf **Weiter: Tag-Instanz**.
10. Geben Sie einen beliebigen Namen in das Wert Feld für die **Name** Schlüssel zur Identifizierung der Instanz. Fügen Sie weitere Tags hinzu, um diese Instanz in der Umgebung zu identifizieren, und klicken Sie dann auf **Weiter: Sicherheitsgruppe konfigurieren**.
11. Wählen **Wählen Sie eine bestehende Sicherheitsgruppe** und wählen Sie dann die Standard-Sicherheitsgruppen-ID für Ihre VPC aus.

    Stellen Sie sicher, dass die zuvor erstellten Regeln angewendet wurden. Zum Beispiel SSH und ICMP sind immer noch aufgeführt und ihre Quelladressen sind 0.0.0.0/0. Optional könnte eine neue Sicherheitsgruppe speziell für diese Instanz erstellt werden.
12. klicken **Überprüfung und Markteinführung** um den Brocade vRouter zu starten und zu installieren.
13. Überprüfen Sie die Auswahlen und Einträge, insbesondere das Subnetz und die IP-Adressen. Wenn die Kosten ein Problem darstellen, stellen Sie sicher, dass die Instance innerhalb der Grenzen der kostenlosen Testversion geblieben ist. klicken **Starten** um die Instanz zu starten und den Brocade vRouter zu registrieren.
14. Wählen Sie im Schlüsselpaar-Dialogfeld **Neues Schlüsselpaar erstellen** geben Sie im Drop-down-Menü einen benutzerfreundlichen Namen ein und klicken Sie auf **Key Pair herunterladen** Schaltfläche zum Herunterladen des Schlüsselpaars. Stellen Sie sicher, dass Sie sich den Download-Speicherort notieren.
15. klicken **Instances starten** um den Installationsvorgang abzuschließen.
16. klicken **Instanzen anzeigen** am unteren Rand der Status der Markteinführung Bildschirm oder Auswahl **Instanzen** aus dem Navigationsbereich. Je nach Auswahl kann es einige Minuten dauern, bis die Instanz vollständig online ist.
17. Nachdem die Instance vollständig gestartet wurde und Statusprüfungen sind abgeschlossen, klicken Sie auf **Beschreibung** Tab unten auf der Seite. In der Netzwerkschnittstellen Abschnitt, klicken **eth0**. Stellen Sie sicher, dass die IP-Adresse `10.4.0.187` (oder die zuvor konfigurierte IP-Adresse).
18. Klicken Sie auf den Link zum Schnittstellen-ID. In diesem Beispiel lautet die ID `eni-f554a48d`.




19. Wenn die private Schnittstelle des Brocade vRouters ausgewählt ist, klicken Sie auf **Aktionen** Drop-down-Menü und wählen **Quelle/Ziel ändern. Prüfen**.
20. Wählen Sie den **Deaktiviert** Optionsfeld und dann klicken **Speichern**.
21. Erstellen Sie die private Subnetzschnittstelle für den Brocade vRouter, indem Sie auf **Netzwerkschnittstelle erstellen**.

22. In der Netzwerkschnittstelle erstellen Füllen Sie im Dialogfeld die folgenden Felder aus:

    **Beschreibung**

    Geben Sie einen Namen ein, um die private Schnittstelle zu identifizieren.

    **Subnetz**

    Wählen Sie aus der Drop-down-Liste das Subnetz für `10.4.1.0/24`.

    **Private IP**

    Typ `10.4.1.10`.

    **Sicherheitsgruppen**

    Wählen Sie die Standard-VPS-Sicherheitsgruppe aus.
23. klicken **Ja, Create** um die neue Schnittstelle zu erstellen.
24. Wählen Sie die private Schnittstelle aus und klicken Sie dann auf **Aktionen** Drop-down-Menü und wählen **Quelle/Ziel ändern. Prüfen**.
25. Wählen Sie den **Deaktiviert** Optionsfeld und dann klicken **Speichern**.

    Nehmen Sie die auf oder notieren Sie sich `10.4.1.10` Netzwerkschnittstellen-ID.
26. Wenn die private Schnittstelle noch ausgewählt ist, klicken Sie auf **Anhängen**.
27. Wählen Sie Ihre Instance aus der Dropdownliste Instance-ID aus und klicken Sie dann auf **Anhängen**.
28. Kehren Sie zum VPC-Dashboard zurück.
29. Wählen Sie im Navigationsbereich **Routentabellen**.
30. Wählen Sie die Routing-Tabelle aus, die dem privaten Subnetz zugeordnet ist `10.4.1.0/24`.
31. Klicken Sie auf **Strecken** Tabulatortaste und dann klicken **Bearbeiten**.
32. klicken **Eine weitere Route hinzufügen**. In der Destination Feld, Typ `0.0.0.0/0` und geben Sie im Zielfeld die in Schritt 23 angegebene Schnittstellen-ID ein, und klicken Sie dann auf **Speichern**. Diese Routentabelle sollte mit der privaten Schnittstellen-ID des Brocade vRouters und dem privaten Subnetz verknüpft werden. `10.4.1.0/24`.
33. Weisen Sie eine Amazon Elastic IP zu, eine dynamisch zugewiesene, öffentlich geroutete IP, indem Sie **Elastische IPs** aus dem Navigationsbereich. klicken **Neue Adresse zuweisen**, und klicken Sie dann **Ja, zuordnen**.
34. Wählen Sie im Drop-down-Menü Aktionen die Option Partneradresse aus und legen Sie die folgenden Felder fest:

    **Assoziieren mit**

    Netzwerk-Schnittstelle

    **Netzwerk-Schnittstelle**

    Wählen Sie die öffentliche Schnittstellen-ID des Brocade vRouters aus. In diesem Beispiel lautet die ID `eni-f554a48d`.

    **Private IP-Adresse**

    Wählen Sie die dem öffentlichen Subnetz zugewiesene IP-Adresse aus. In diesem Beispiel ist es `10.4.0.187`.
35. klicken **Ja, Mitarbeiter**.

## Stellen Sie über SSH eine Verbindung zu Ihrer Brocade vRouter-Instanz her

**Hinweis:** Die folgenden Verfahren wurden in einer macOS-Terminalanwendung durchgeführt. Ihre Befehle können je nach Ihrer Wahl variieren Client.

1. Öffnen Sie einen Terminal-Client und führen Sie die folgenden Befehle aus:
   a) Wechseln Sie in das Verzeichnis, in das Sie Ihre private Schlüsseldatei heruntergeladen haben. Zum Beispiel:

   ```
   remote$ cd ~/Downloads
   ```

b) Ändern Sie die Berechtigungen der Schlüsseldatei so, dass sie nicht öffentlich sichtbar ist:

```
remote$ chmod 400 *.pem
```

c) Stellen Sie die Verbindung her:

```
remote$ ssh -i <vrouter_private_key.pm> vyatta@<elastic_IP>
```

Zum Beispiel:

```
ssh -i brocadevrouter5600.pem vyatta@52.35.186.255
```

Wenn die SSH-Verbindung erfolgreich ist, wird eine Ausgabe ähnlich der folgenden angezeigt:

```
Welcome to Brocade vRouter
Welcome to Brocade Vyatta Network OS
Version: 4.1R2B
Description: Brocade Vyatta Network OS 4.1 R2
Built on: Fri Dec 18 07:10:38 UTC 2015
```

**Hinweis:** Wenn die Verbindung fehlschlägt, fügen Sie hinzu `-vvv` zu der `ssh` Befehl zum Sammeln von Debug-Ausgaben, zum Überprüfen der Sicherheitsgruppenregeln, um sicherzustellen, dass SSH zulässig ist, um zu überprüfen, ob die Elastic IP mit der öffentlichen Schnittstelle verknüpft ist, und um zu überprüfen, ob Ping an die öffentliche Elastic IP eine Antwort zurückgibt.

2. Zeigen Sie eine Liste der konfigurierten Schnittstellen an, indem Sie den folgenden Befehl ausführen:

```
show interfaces
```

Es erscheint eine Ausgabe, die der folgenden ähnelt:

```
Codes: S - State, L - Link, u - Up, D - Down, A – Admin Down
  Interface        IP Address                     S/L  Description
  ---------        ----------                     ---  -----------
  dp0s0            10.4.0.187/24                  u/u
  dp0s1            10.4.1.10/24                  -A/D
```

**Hinweis:** Wenn nur eine Schnittstelle angezeigt wird, starten Sie den Brocade vRouter neu, indem Sie `Neustart` Befehl.

3. Zwei Schnittstellen sollten sichtbar sein. Eine Schnittstelle ist nicht konfiguriert und eine IP-Adresse wird nicht angezeigt. Um die Schnittstelle zu konfigurieren, führen Sie die folgenden Befehle aus:

a) Rufen Sie den Konfigurationsmodus auf:

```
configure
```

b) Konfigurieren Sie die private Schnittstelle mit der zuvor zugewiesenen privaten IP. In diesem Beispiel `10.4.1.0.24` wurde in der Instanz in AWS auf der privaten Schnittstelle zugewiesen.

```
set interfaces dataplane dp0s1 address 10.4.1.10/24
```

c) Legen Sie die Anzahl der unentgeltlichen ARP-Anfragen (Address Resolution Protocol) fest, die gesendet werden sollen:

```
set interfaces dataplane dp0s1 ip gratuitous-arp-count 1
```

d) Aktivieren Sie den Reverse-Path-Filter ohne Quellenvalidierung:

```
set interfaces dataplane dp0s1 ip rpf-check disable
```

e) Stellen Sie die Anzahl der zu übertragenden NS-Pakete ein:

```
set interfaces dataplane dp0s1 ipv6 dup-addr-detect-transmits 1
```

f) Legt die Größe der MTU für die Datenebenenschnittstelle fest:

```
set interfaces dataplane dp0s1 mtu 1500
```

g) Stellen Sie den EtherType für VLAN-Frames ein:

```
set interfaces dataplane dp0s1 vlan-protocol 0x8100
```

4. Führen Sie den Befehl show interfaces aus, um die konfigurierten Schnittstellen anzuzeigen. Es erscheint eine Ausgabe, die der folgenden ähnelt:

```
interfaces {
        dataplane dp0s0 {
                address dhcp
                ip {
                        gratuitous-arp-count 1
                        rpf-check disable
                }
                ipv6 {
                        dup-addr-detect-transmits 1
                }
                mtu 1500
                vlan-protocol 0x8100
        }
+       dataplane dp0s1 {
+                address 10.4.1.10/24
+                ip {
+                        gratuitous-arp-count 1
+                        rpf-check disable
+                }
+                ipv6 {
+                        dup-addr-detect-transmits 1
+                }
+                mtu 1500
+                vlan-protocol 0x8100
+        }
+        loopback lo
+ }
```

**Hinweis:** Das Pluszeichen (+) weist auf nicht gespeicherte Änderungen hin.

5. Typ `verpflichten` und drücken Sie dann die EINGABETASTE.
6. Typ `sparen` und drücken Sie dann die EINGABETASTE, um die Änderungen zu speichern.
7. Optional: Stellen Sie den SSH-Dienstport auf 22 ein, um sicherzustellen, dass die Ports auf dem Brocade vRouter in der Konfigurationsdatei ordnungsgemäß zugewiesen sind:

```
set service ssh port 22
```

8. Typ `verpflichten` und drücken Sie dann die EINGABETASTE.
9. Typ `sparen` und drücken Sie dann die EINGABETASTE, um die Änderungen zu speichern.
10. Typ `aussteigen` um den Konfigurationsmodus zu verlassen.
11. Führen Sie das aus `Schnittstellen einblenden` Befehl. Beide Schnittstellen sollten aktiv und administrativ aktiv sein, ähnlich der folgenden Ausgabe:

```
Codes: S - State, L - Link, u - Up, D - Down, A – Admin Down
  Interface        IP Address                     S/L  Description
```

```
---------       ----------                          ---  -----------
dp0s0           10.4.0.187/24                       u/u
dp0s1           10.4.1.10/24                        u/u
```

**Hinweis:** Lassen Sie die vRouter-Shell geöffnet, um später in diesem Verfahren weitere Befehle auszuführen.

### Zusammenfassung

In diesem Abschnitt haben Sie den Brocade vRouter so konfiguriert, dass er von einem Remote-Computer aus zugänglich und konfiguriert werden kann. Sie haben auch die entsprechenden Schnittstellen für die Erstellung zusätzlicher Subnetze hinzugefügt.

## (Optional) Linux-Client für die Generierung von Datenverkehr konfigurieren

In diesem und im nächsten Abschnitt konfigurieren Sie ein neues Linux-AMI, um die Brocade vRouter- und ExtraHop Discover-Konfiguration zu überprüfen . Wenn andere Verkehrsquellen verfügbar sind, können diese Abschnitte übersprungen werden.

**Hinweis:** Im folgenden Beispiel wird ein Linux-Client ausgewählt.

1. Klicken Sie in der oberen linken Ecke auf das Symbol Console Home, um zur Seite der AWS-Managementkonsole zurückzukehren.
2. Klicken Sie im Abschnitt Berechnen auf **EC2**.
3. Klicken Sie im Navigationsbereich auf **Instanzen**.
4. klicken **Instanz starten** um den Amazon Machine Image (AMI) -Assistenten zu starten.
5. Suchen Sie ein Ubuntu Server-Image in der Liste und klicken Sie dann auf **Wählen**.
6. Wählen Sie den **T2. Mikro** Instanztyp und dann klicken **Weiter: Instanzdetails konfigurieren**.
7. Auf dem Instanzdetails konfigurieren Seite, führe die folgenden Schritte aus:
   a) Typ `1` in der Anzahl der Instanzen Feld.
   b) Aus dem **Netzwerk** Wählen Sie in der Dropdownliste die VPC aus, die Sie im ersten Abschnitt dieses Handbuchs erstellt haben.
   c) Wählen Sie in der Dropdownliste Subnetz den `10.4.1.0/24` Subnetz.

      Eine statische IP ist für diesen Schritt nicht erforderlich. Notieren Sie sich jedoch die der Instanz zugewiesene IP-Adresse. In diesem Beispiel ist die IP `10.4.1.50`.
   d) Die übrigen Einstellungen können auf ihren Standardwerten belassen werden.
8. klicken **Weiter: Speicher hinzufügen**. Es sind keine Änderungen erforderlich.
9. klicken **Weiter: Tag-Instanz**. Es sind keine Änderungen erforderlich.
10. klicken **Weiter: Sicherheitsgruppe konfigurieren**.
11. Auf dem Sicherheitsgruppe konfigurieren Seite, führe die folgenden Schritte aus:
    a) Wählen **Eine neue Sicherheitsgruppe erstellen**.
    b) In der **Feld für den Namen der Sicherheitsgruppe**, geben Sie einen aussagekräftigen Namen ein. Zum Beispiel Ubuntu Linux.
    c) In der Beschreibung Feld, geben Sie eine Beschreibung für diese Sicherheitsgruppe ein.
    d) klicken **Regel hinzufügen**.
    e) Wählen **Alles ICMP** aus der Drop-down-Liste.
    f) In der Quelle Spalte, wählen **Irgendwo** aus der Drop-down-Liste und tippe `0.0.0.0/0` auf dem Feld.
    g) Wenn SSH ist nicht aufgeführt, klicken Sie **Regel hinzufügen**.
    h) In der Quelle Spalte, wählen **Irgendwo** aus der Drop-down-Liste und tippe `0.0.0.0/0` auf dem Feld.
    i) klicken **Überprüfung und Markteinführung**.

j) Bestätigen Sie, dass Ihre Sicherheitsgruppe weltweit geöffnet ist, und klicken Sie dann auf **Starten**.

**Hinweis** Dies ist eine Konfiguration, die nicht für die Produktion bestimmt ist. Normalerweise sollte der Verkehr nicht weltoffen konfiguriert werden.

k) Wählen Sie im Schlüsselpaar-Dialogfeld **Neues Schlüsselpaar erstellen** aus der Drop-down-Liste. Geben Sie einen Namen in das Name des Schlüsselpaars Feld und Klick **Key Pair herunterladen**. Notieren Sie sich den Download-Speicherort und klicken Sie dann auf **Instances starten** um den Installationsvorgang abzuschließen.

## (Optional) Konfigurieren Sie NAT auf dem vRouter für den Linux-Client

Um den Linux-Client im internen privaten Subnetz sowohl eingehend als auch ausgehend für die Generierung von Datenverkehr zu erreichen, muss NAT auf dem vRouter konfiguriert sein.

1. Kehren Sie zur zuvor geöffneten vRouter-Shell-Eingabeaufforderung zurück.
2. Öffnen Sie einen Port und maskieren Sie ausgehender Datenverkehr, indem Sie die folgenden Befehle ausführen.
   a) Rufen Sie den Konfigurationsmodus auf:

```
configure
```

   b) Stellen Sie den Zielport ein. Dies ist ein beliebiger Port und 445 ist in diesem Beispiel angegeben.

```
set service nat destination rule 10 destination port 445
```

   c) Stellen Sie die Eingangsschnittstelle ein:

```
set service nat destination rule 10 inbound-interface dp0s0
```

   d) Stellen Sie das Protokoll ein:

```
set service nat destination rule 10 protocol tcp
```

   e) Stellen Sie die Übersetzungsadresse ein, wobei *<client_instance_ip>* ist die IP-Adresse des Linux-Clients:

```
set service nat destination rule 10 translation address
 <client_ip_address>
```

   Zum Beispiel:

```
set service nat destination rule 10 translation address 10.4.1.50
```

   f) Stellen Sie den Übersetzungsport ein:

```
set service nat destination rule 10 translation port 22
```

   g) Typ `verpflichten` und drücken Sie dann die EINGABETASTE.
   h) Typ `sparen` und drücken Sie dann die EINGABETASTE, um die Änderungen zu speichern.
   i) Konfigurieren Sie den ausgehender Datenverkehr auf dem vRouter, um die internen Adressen zu maskieren:

```
set service nat source rule 100 outbound-interface dp0s0

set service nat source rule 100 translation address masquerade
```

   j) Typ `verpflichten` und drücken Sie dann ENTER
   k) Typ `sparen` und drücken Sie dann die EINGABETASTE, um die Änderungen zu speichern.

**Hinweis** Die Regelnummern sind willkürlich. Lassen Sie jedoch genügend Abstand zwischen den Bereichen, falls Sie in Zukunft verwandte Regeln hinzufügen müssen.

3. Stellen Sie sicher, dass die Konfiguration mit den gerade erstellten Regeln aktualisiert wurde, indem Sie den folgenden Befehl ausführen:

```
show service
```

Es erscheint eine Ausgabe, die der folgenden ähnelt. Notieren Sie sich den Zielport, den Übersetzungsport und die Adresse der erstellten Linux-Instanz. Stellen Sie außerdem sicher, dass es sich bei der Schnittstelle in beiden Regeln um die externe Schnittstelle des vRouters handelt.

```
nat {
 destination {
  rule 10 {
   destination {
    port 445
   }
   inbound-interface dp0s0
   protocol tcp
   translation {
    address 10.4.1.50
    port 22
   }
  }
 }
 source {
  rule 100 {
   outbound-interface dp0s0
   translation {
    address masquerade
   }
  }
 }
}
ssh {
 authentication-retries 3
 disable-password-authentication
 port 22
 timeout 120
}
```

4. Kehren Sie zur AWS-Konsole zurück, um eine eingehende Regel für die Standardsicherheitsgruppe zu erstellen, um die NAT-Regeln zu testen.
   a) Klicken Sie im Navigationsbereich auf **Instanzen**.
   b) Wählen Sie den vRouter in der Liste der Instanzen aus.
   c) In der **Beschreibung** Tab-Bereich, neben Sicherheitsgruppen, klicken **Standard**.
   d) Klicken Sie auf der Sicherheitsgruppenseite auf **Eingehend** Tabulatur.
   e) klicken **Bearbeiten**.
   f) klicken **Regel hinzufügen**.
   g) In der **Typ** Drop-down-Liste, wählen **Benutzerdefinierte TCP-Regel**.
   h) In der Portbereich Feld, Typ `445`.
   i) In der Quelle Feld, Typ `0.0.0.0/0`.

## (Optional) Testen Sie die Linux-Client-Konfiguration

1. Auf deinem Client Computer, öffne ein neues Terminalfenster.
2. Stellen Sie mit dem entsprechenden Schlüsselpaar und Benutzernamen eine Verbindung zum AWS-Linux- oder Windows-Client her.

```
ssh –i <client.pem> <username>@<elastic_ip> -p 445
```

Zum Beispiel:

```
ssh -i ubuntulinux.pem ubuntu@52.35.186.255 -p 445
```

**Hinweis** Klicken Sie in der AWS-Konsole bei ausgewählter Instanz auf **Verbinde** um zu erfahren, wie Sie eine Verbindung zu Ihrer speziellen Instanz herstellen können. Benutzernamen und Konnektivität sind für das ausgewählte AMI einzigartig.

3. Nachdem Sie sich erfolgreich mit dem verbunden haben Client, pingen Sie die öffentlichen und privaten IP-Adressen, die Sie zuvor konfiguriert haben, und stellen Sie sicher, dass Sie die angegebenen IP-Adressen erreichen können. Zum Beispiel:

```
ubuntu@ip-10-4-1-50:~$ ping 10.4.0.187
ubuntu@ip-10-4-1-50:~$ ping 10.4.1.10
```

4. Öffnen Sie ein neues Terminalfenster und stellen Sie mit dem entsprechenden Benutzernamen und Schlüsselpaar eine Verbindung zum Brocade vRouter her.
5. Pingen Sie die IP-Adresse des Linux-Clients. Zum Beispiel:

```
ping 10.4.1.50
```

6. Zeigen Sie die Routenkarte an, indem Sie den folgenden Befehl ausführen:

```
show ip route
```

Es erscheint eine Ausgabe, die der folgenden ähnelt:

```
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
Gateway of last resort is 10.4.0.1 to network 0.0.0.0

K    *> 0.0.0.0/0 via 10.4.0.1, dp0s0
C    *> 10.4.0.0/24 is directly connected, dp0s0
C    *> 10.4.1.0/24 is directly connected, dp0s1
C    *> 127.0.0.0/8 is directly connected, lo
```

7. Zeigen Sie die ARP-Tabelle an, indem Sie den folgenden Befehl ausführen:

```
show arp
```

Es erscheint eine Ausgabe, die der folgenden ähnelt:

```
IP Address     HW address            Dataplane   Controller  Device
10.4.0.2       02:22:ef:75:6b:79     VALID       VALID       dp0s0
10.4.0.1       02:22:ef:75:6b:79     VALID       VALID       dp0s0
10.4.1.1       02:1f:68:6c:5c:81     VALID                   dp0s1
10.4.1.50      02:f2:d9:aa:fe:c5     VALID       VALID       dp0s1
```

8. Zeigen Sie die Schnittstellen an, indem Sie den folgenden Befehl ausführen:

```
show interface
```

Es erscheint eine Ausgabe, die der folgenden ähnelt:

```
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface       IP Address       S/L       Description
---------       ----------       --- -----------
dp0s0     10.4.0.187/24    u/u
dp0s1     10.4.1.10/24     u/u
```

### Zusammenfassung

In diesem Abschnitt haben Sie eine Linux-Instanz für die Generierung von Testpaketverkehr installiert und konfiguriert.

## Einen ExtraHop EDA 1000v konfigurieren

In diesem Abschnitt konfigurieren Sie einen neuen ExtraHop EDA 1000V-Sensor.

1. Klicken Sie in der oberen linken Ecke auf das Symbol Console Home, um zur Seite der AWS-Managementkonsole zurückzukehren.
2. Klicken Sie im Abschnitt Berechnen auf **EC2**.
3. Klicken Sie im Navigationsbereich auf **Instanzen**.
4. klicken **Instanz starten** um den Amazon Machine Image (AMI) -Assistenten zu starten.
5. klicken **AMIs der Gemeinschaft**.
6. Typ `ExtraHop` in der Community-AMIs durchsuchen Feld und lokalisieren Sie das `ExtraHop Discover appliance 1000v 5.x.x.x AMI` und klicken **Wählen**.
7. Wählen Sie den **t2. mittel** geben Sie den Instanztyp ein und klicken Sie dann **Weiter: Instanzdetails konfigurieren**.
8. In der Instanzdetails konfigurieren Seite, führe die folgenden Schritte aus:
   a) Typ `1` in der Anzahl der Instanzen Feld.
   b) In der **Netzwerk** Wählen Sie in der Dropdownliste die VPC aus, die im ersten Teil dieses Handbuchs erstellt wurde.
   c) In der **Subnetz** Drop-down-Liste, wählen Sie das private Subnetz `10.4.1.0/24`.
   d) In der Netzwerkschnittstellen Art des Abschnitts `10.4.1.15` in der Primäre IP Feld und dann klicken **Weiter: Speicher hinzufügen**.
9. Belassen Sie die Standardspeichergröße auf der Standardeinstellung. klicken **Weiter: Tag-Instanz**.
10. Kennzeichnen Sie die Instanz mit einem Namen, um die Instanz zu identifizieren. Fügen Sie weitere Tags zur Identifizierung dieser Instanz in der Umgebung hinzu und klicken Sie dann auf **Weiter: Sicherheitsgruppe konfigurieren**.
11. Auf dem Sicherheitsgruppe konfigurieren Seite, führe die folgenden Schritte aus:
    a) Wählen **Eine neue Sicherheitsgruppe erstellen**.
    b) In der Name der Sicherheitsgruppe Feld, geben Sie einen beschreibenden Namen ein. Zum Beispiel `EDA 1000v`.
    c) In der Beschreibung Feld, geben Sie eine Beschreibung für diese Sicherheitsgruppe ein.
    d) klicken **Regel hinzufügen** 6 mal und jeweils konfigurieren Protokoll tippe wie folgt:

| Typ | Protokoll | Portbereich | Quelle |
|---|---|---|---|
| SSH | TCP | 22 | Überall 0.0.0.0/0 |
| HTTP | TCP | 80 | Überall 0.0.0.0/0 |
| HTTPS | TCP | 443 | Überall 0.0.0.0/0 |

| Typ | Protokoll | Portbereich | Quelle |
|---|---|---|---|
| Benutzerdefinierte TCP-Regel | TCP | 2003 | Überall 0.0.0.0/0 |
| Benutzerdefinierte UDP-Regel | UDP | 2003 | Überall 0.0.0.0/0 |
| Gesamter Verkehr | ALLES | 0-65535 | Benutzerdefinierte IP 10.4.0.0/16 |
| Alles ICMP | ICMP | 0-65535 | Überall 0.0.0.0/0 |

12. klicken **Überprüfung und Markteinführung**.

    **Hinweis:** Wenn ein **Von General Purpose (SSD) booten** Das Dialogfeld wird angezeigt. Wählen Sie die erste Option aus und klicken Sie dann auf **Weiter**.
13. Überprüfen Sie die Instanzauswahl und klicken Sie dann auf **Starten**.
14. In der Wählen Sie eine vorhandene Schlüsselpaarseite aus Dialogfeld, wählen **Ohne Schlüsselpaar fortfahren** aus der Drop-down-Liste. Der Großteil der Konfiguration wird über die Administrationseinstellungen auf dem Sensor abgeschlossen, sodass kein Schlüsselpaar erforderlich ist. Wählen Sie den **Ich erkenne** Checkbox und dann klicken **Instances starten**.
15. Gehen Sie zu Ihrer Instance-Liste in AWS. Vergewissern Sie sich, dass die Statusprüfungen bestanden wurden, und notieren Sie sich die Instanz-IP.

## Konfigurieren Sie NAT auf dem vRouter für den Zugriff auf das ExtraHop-System

Um auf das ExtraHop-System zugreifen zu können, muss NAT auf dem vRouter konfiguriert sein.

1. Kehren Sie zur zuvor geöffneten vRouter-Shell-Eingabeaufforderung zurück.
2. Öffnen Sie einen Port und maskieren Sie ausgehender Datenverkehr, indem Sie die folgenden Befehle ausführen.
   a) Rufen Sie den Konfigurationsmodus auf:

   ```
   configure
   ```

   b) Stellen Sie den Zielport ein. Dies ist ein beliebiger Port und 8443 ist in diesem Beispiel angegeben.

   ```
   set service nat destination rule 20 destination port 8443
   ```

   c) Stellen Sie die Eingangsschnittstelle ein:

   ```
   set service nat destination rule 20 inbound-interface dp0s0
   ```

   d) Stellen Sie das Protokoll ein:

   ```
   set service nat destination rule 20 protocol tcp
   ```

   e) Stellen Sie die Übersetzungsadresse ein, wobei <extrahop_instance_ip> ist die IP-Adresse des Linux-Clients:

   ```
   set service nat destination rule 20 translation address
       <extrahop_ip_address>
   ```

   Zum Beispiel:

   ```
   set service nat destination rule 20 translation address 10.4.1.15
   ```

f) Stellen Sie den Übersetzungsport ein:

```
set service nat destination rule 20 translation port 443
```

g) Konfigurieren Sie den ausgehender Datenverkehr auf dem vRouter so, dass die internen Adressen maskiert werden (falls dies nicht bereits geschehen ist):

```
set service nat source rule 100 outbound-interface dp0s0

set service nat source rule 100 translation address masquerade
```

h) Geben Sie commit ein und drücken Sie dann die EINGABETASTE.

i) Typ `sparen` und drücken Sie dann die EINGABETASTE, um die Änderungen zu speichern.

**Hinweis:** Die Regelnummern sind willkürlich. Lassen Sie jedoch genügend Abstand zwischen den Bereichen, falls Sie in Zukunft verwandte Regeln hinzufügen müssen.

3. Stellen Sie sicher, dass die Konfiguration mit den gerade erstellten Regeln aktualisiert wurde, indem Sie den folgenden Befehl ausführen:

```
show service
```

4. Kehren Sie zur AWS-Konsole zurück, um eine eingehende Regel für die Standardsicherheitsgruppe zu erstellen, um die NAT-Regeln zu testen.
   a) Klicken Sie im Navigationsbereich auf **Instanzen**.
   b) Wählen Sie den vRouter in der Liste der Instanzen aus.
   c) In der **Beschreibung** Tab-Bereich, neben Sicherheitsgruppen, klicken **Standard**.
   d) Klicken Sie auf der Sicherheitsgruppenseite auf **Eingehend** Tabulatur.
   e) klicken **Bearbeiten**.
   f) klicken **Regel hinzufügen**.
   g) In der **Typ** Drop-down-Liste, wählen **Benutzerdefinierte TCP-Regel**.
   h) In der Portbereich Feld, Typ `8443`.
   i) In der Quelle Feld, Typ `0.0.0.0/0`.
5. Geben Sie in Ihrem Browser die IP-Adresse des ExtraHop-Systems ein:

```
https://<elastic_public_ip:8443>/admin
```

6. Auf dem Lizenzierung Seite, lesen Sie die Allgemeinen Geschäftsbedingungen von ExtraHop, wählen **Ich stimme zu**, und klicken Sie dann auf **Einreichen**.
7. Geben Sie auf dem Anmeldebildschirm Folgendes ein `Einrichten` für den Benutzernamen und die Instanz-ID für das Passwort. Sie finden die Instanz-ID auf der Instanzen-Seite. Geben Sie die folgenden Zeichen ein `i-` (aber nicht `i-` selbst), und klicken Sie dann **Einloggen**.
8. Auf dem Sensorverwaltung Seite, in der Geräteeinstellungen Abschnitt, klicken **Lizenz**.
9. klicken **Lizenz verwalten** und dann klicken **Registriere dich**.
10. Geben Sie den von ExtraHop erhaltenen Produktschlüssel in das Feld Product Key ein und klicken Sie dann auf **Registriere dich**.

**Hinweis:** Wenn die Lizenzregistrierung fehlschlägt, stellen Sie sicher, dass die AWS-Sicherheitsregeln ausgehenden Datenverkehr zulassen HTTP und HTTPS-Verkehr.

11. klicken **Erledigt**.
12. Kehren Sie zurück zum **Admin** Seite.
13. In der Netzwerk-Einstellungen Abschnitt, klicken **Konnektivität**.
14. Vergewissern Sie sich im Abschnitt Schnittstellen, dass Interface 1 auf eingestellt ist **Geschäftsleitung + RPCAP/ERSPAN/VXLAN/GENEVE Target**.

### (Optional) Erstellen Sie ein neues Volume für den Paketerfassungsspeicher

Erstellen Sie ein neues Volume für den EDA 1000v, um triggerfähige Paketerfassungsdaten zu speichern.

1. Klicken Sie im Navigationsbereich in AWS auf **Bände**.
2. klicken **Volumen erstellen**. In der Dialogfeld „Volumen erstellen“ Box, stellen Sie sicher, dass die Verfügbarkeitszone ausgewählt ist dieselbe Zone wie die Instanz entdecken und dann klicken **Erstellen**.
3. Wählen Sie das neue Volume in der Volumenliste aus und wählen Sie dann **Volumen anhängen** von der **Aktionen** Drop-down-Menü. In der Instanz Feld, wählen Sie Ihre Discover-Instanz aus und klicken Sie dann auf **Anhängen**.
4. Klicken Sie im Navigationsbereich auf **Instanzen**.
5. Wählen Sie die Discover-Instanz in der Liste aus und klicken Sie dann auf **Aktionen** > **Instanzstatus** > **Neustarten**.
6. Wenn die Discover-Instanz wieder in den laufenden Zustand zurückkehrt, melden Sie sich bei den Administrationseinstellungen auf dem ExtraHop-System an über `https://<extrahop-hostname-or-IP-address>/admin`.
7. In der Einstellungen der Appliance Abschnitt, klicken **Festplatten** und stellen Sie sicher, dass die neue Paketerfassungsdiskette in der Liste der direkt verbundenen Festplatten angezeigt wird.
8. klicken **Aktivieren** auf der Packet Capture-Diskette, um sie zu aktivieren.

### Zusammenfassung

In diesem Abschnitt haben Sie das ExtraHop-System für den Empfang von Netzwerkpaketen und Datenverkehr von der ERSPAN Schnittstelle. Optional wurde eine zusätzliche Festplatte konfiguriert, um triggerfähige Paketerfassungen zu ermöglichen.

## Konfiguration von ERSPAN und Portmonitoring auf dem Brocade vRouter

In diesem Abschnitt konfigurieren Sie die ERSPAN und Portüberwachungsfunktionen auf dem Brocade vRouter, um ERSPAN-Verkehr an den ExtraHop-Sensor zu senden.

1. Von einem Remote-Computer, SSH zum vRouter.

```
ssh -i <vrouter_private_key.pm> vyatta@<elastic_IP>
```

2. Konfigurieren Sie die ERSPAN-Schnittstelle, indem Sie die folgenden Befehle ausführen:
   a) Rufen Sie den Konfigurationsmodus auf:

```
configure
```

   b) Stellen Sie die lokale IP-Adresse für die ERSPAN-Schnittstelle ein:

```
set interfaces erspan erspan1 local-ip 10.4.1.10
```

   c) Stellen Sie die Remote-IP-Adresse für die ERSPAN-Schnittstelle ein:

```
set interfaces erspan erspan1 remote-ip 10.4.1.15
```

   d) Stellen Sie die folgende zusätzliche Konfiguration ein:

```
set interfaces erspan erspan1 ip tos inherit
set interfaces erspan erspan1 ip ttl 255
set interfaces erspan erspan1 mtu 1500
```

e) Zeigen Sie die Konfigurationsänderungen an:

```
show interfaces
```

f) Geben Sie commit ein und drücken Sie dann die EINGABETASTE.

g) Geben Sie Speichern ein und drücken Sie dann die EINGABETASTE, um die Änderungen zu speichern.

3. Konfigurieren Sie den Port Monitor und die ERSPAN-Quelle, indem Sie die folgenden Befehle ausführen:

**Hinweis** In diesem Beispiel ist die Quelle des Monitors die interne Schnittstelle des Brocade vRouters. Darüber hinaus sind die Sitzungs- und Identifikationsnummern willkürlich, sollten sich jedoch nicht mit anderen Sitzungs-IDs überschneiden.

a) Stellen Sie den Portmonitor-Sitzungstyp ein:

```
set service portmonitor session 25 type erspan-source
```

b) Stellen Sie die Quellschnittstelle für die Portüberwachung ein:

```
set service portmonitor session 25 source dp0s1
```

c) Stellen Sie die Zielschnittstelle für die Portüberwachung ein:

```
set service portmonitor session 25 destination erspan1
```

d) Legen Sie die Sitzungs-ID fest:

```
set service portmonitor session 25 erspan identifier 200
```

e) Stellen Sie den ERSPAN-Header-Typ ein:

```
set service portmonitor session 25 erspan header type-II
```

f) Stellen Sie die ERSPAN-Richtung ein:

```
set service portmonitor session 25 source dp0s1 direction both
```

g) Typ `verpflichten` und drücken Sie dann die EINGABETASTE.

h) Typ `sparen` und drücken Sie dann die EINGABETASTE, um die Änderungen zu speichern.

Die Portüberwachung für die Sitzung wird sofort aktiviert, wenn die Parameter Typ, Quelle, Ziel, ERSPAN-ID und ERSPAN-Headertyp korrekt konfiguriert sind.

i) Typ `aussteigen` um den Konfigurationsmodus zu verlassen.

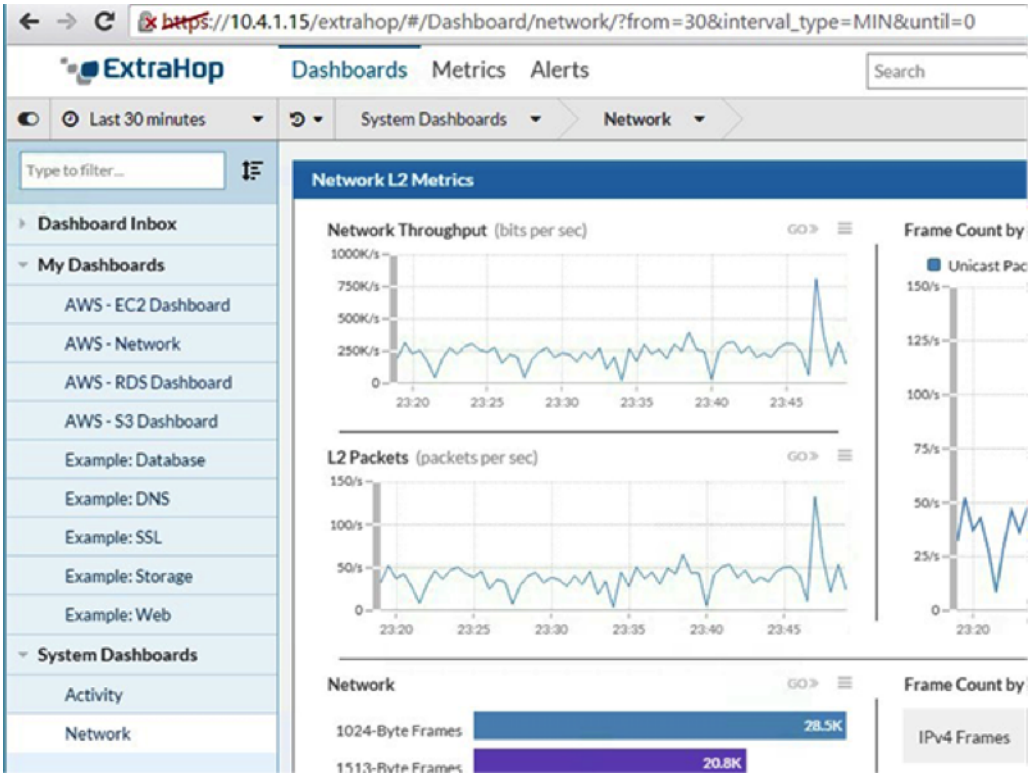
j) Typ `Konfiguration einblenden` um die neue Konfiguration anzuzeigen.

Es wird eine Ausgabe ähnlich der folgenden angezeigt (aus Gründen der Übersichtlichkeit gekürzt):

```
erspan erspan1 {
                ip {
                        tos inherit
                        ttl 255
                }
                local-ip 10.4.1.10
                mtu 1500
                remote-ip 10.4.1.15
        }
.
.
portmonitor {
                session 25 {
                        destination erspan1
                        erspan {
```

```
                                header type-II
                                identifier 200
                        }
                        source dp0s1 {
                                direction both
                        }
                        type erspan-source
                }
        }
```

4. Loggen Sie sich in das ExtraHop-System ein über `https://<elastic_public_ip:8443>/extrahop` und stellen Sie sicher , dass der ExtraHop ERSPAN-Verkehr vom vRouter empfängt von Armaturenbretter Schnittstelle.




## Zusammenfassung

In diesem Abschnitt haben Sie den Brocade vRouter zum Senden konfiguriert ERSPAN Datenverkehr zum ExtraHop-System, das die Analyse des Datenverkehrs innerhalb der virtuellen privaten Cloud von Amazon Web Services ermöglicht, ohne dass eine Installation erforderlich ist RPCAPD Kunden.

## Beispiel für eine Brocade vRouter-Konfiguration

```
vyatta@vyatta:~$ show configuration
interfaces {
        dataplane dp0s0 {
                address dhcp
                ip {
                        gratuitous-arp-count 1
                        rpf-check disable
                }
                ipv6 {
                        dup-addr-detect-transmits 1
                }
```

```
                mtu 1500
                vlan-protocol 0x8100
        }
        dataplane dp0s1 {
                address 10.4.1.10/24
                ip {
                        gratuitous-arp-count 1
                        rpf-check disable
                }
                ipv6 {
                        dup-addr-detect-transmits 1
                }
                mtu 1500
                vlan-protocol 0x8100
        }
        erspan erspan1 {
                ip {
                        tos inherit
                        ttl 255
                }
                local-ip 10.4.1.10
                mtu 1500
                remote-ip 10.4.1.15
        }
        loopback lo
}
protocols {
        ecmp {
                mode hrw
        }
        pim {
                register-suppression-timer 60
        }
        pim6 {
                register-suppression-timer 60
        }
}
security {
        firewall {
                all-ping enable
                broadcast-ping disable
                config-trap disable
                syn-cookies enable
        }
}
service {
        nat {
                destination {
                        rule 10 {
                                destination {
                                        port 445
                                }
                                inbound-interface dp0s0
                                protocol tcp
                                translation {
                                        address 10.4.1.50
                                        port 22
                                }
                        }
                        rule 20 {
                                destination {
                                        port 8443
                                }
                                inbound-interface dp0s0
```

```
                                protocol tcp
                                translation {
                                        address 10.4.1.15
                                        port 443
                                }
                        }
                }
                source {
                        rule 100 {
                                outbound-interface dp0s0
                                translation {
                                        address masquerade
                                }
                        }
                }
        }
        portmonitor {
                session 25 {
                        destination erspan1
                        erspan {
                                header type-II
                                identifier 200
                        }
                        source dp0s1 {
                                direction both
                        }
                        type erspan-source
                }
        }
        ssh {
                authentication-retries 3
                disable-password-authentication
                port 22
                timeout 120
        }
}
system {
        acm {
                create-default deny
                delete-default deny
                enable
                exec-default allow
                operational-ruleset {
                        rule 9977 {
                                action allow
                                command /show/tech-support/save
                                group vyattaop
                        }
                        rule 9978 {
                                action deny
                                command "/show/tech-support/save/*"
                                group vyattaop
                        }
                        rule 9979 {
                                action allow
                                command /show/tech-support/save-uncompressed
                                group vyattaop
                        }
                        rule 9980 {
                                action deny
                                command "/show/tech-support/save-
uncompressed/*"
                                group vyattaop
                        }
```

```
                        rule 9981 {
                                action allow
                                command /show/tech-support/brief/save
                                group vyattaop
                        }
                        rule 9982 {
                                action deny
                                command "/show/tech-support/brief/save/*"
                                group vyattaop
                        }
                        rule 9983 {
                                action allow
                                command /show/tech-support/brief/save-
uncompressed
                                group vyattaop
                        }
                        rule 9984 {
                                action deny
                                command "/show/tech-support/brief/save-
uncompressed/*"
                                group vyattaop
                        }
                        rule 9985 {
                                action allow
                                command /show/tech-support/brief/
                                group vyattaop
                        }
                        rule 9986 {
                                action deny
                                command /show/tech-support/brief
                                group vyattaop
                        }
                        rule 9987 {
                                action deny
                                command /show/tech-support
                                group vyattaop
                        }
                        rule 9988 {
                                action deny
                                command /show/configuration
                                group vyattaop
                        }
                        rule 9989 {
                                action allow
                                command "/clear/*"
                                group vyattaop
                        }
                        rule 9990 {
                                action allow
                                command "/show/*"
                                group vyattaop
                        }
                        rule 9991 {
                                action allow
                                command "/monitor/*"
                                group vyattaop
                        }
                        rule 9992 {
                                action allow
                                command "/ping/*"
                                group vyattaop
                        }
                        rule 9993 {
                                action allow
```

```
                        command "/reset/*"
                        group vyattaop
                }
                rule 9994 {
                        action allow
                        command "/release/*"
                        group vyattaop
                }
                rule 9995 {
                        action allow
                        command "/renew/*"
                        group vyattaop
                }
                rule 9996 {
                        action allow
                        command "/telnet/*"
                        group vyattaop
                }
                rule 9997 {
                        action allow
                        command "/traceroute/*"
                        group vyattaop
                }
                rule 9998 {
                        action allow
                        command "/update/*"
                        group vyattaop
                }
                rule 9999 {
                        action deny
                        command "*"
                        group vyattaop
                }
        }
        read-default allow
        ruleset {
                rule 9999 {
                        action allow
                        group vyattacfg
                        operation "*"
                        path "*"
                }
        }
        update-default deny
}
config-management {
        commit-revisions 20
}
console {
        device ttyS0 {
                speed 9600
        }
}
host-name vyatta
login {
        session-timeout 0
        user vyatta {
                authentication {
                        encrypted-password "********"
                        public-keys TestBrocade {
                                key xxx
                                type ssh-rsa
                        }
                }
```

```
                        level admin
                }
        }
        syslog {
                global {
                        archive {
                                files 5
                                size 250
                        }
                        facility all {
                                level warning
                        }
                }
        }
        time-zone GMT
}
```