

Déployez ERSPAN avec une sonde ExtraHop et un routeur virtuel Brocade 5600 dans AWS

Publié: 2024-02-16

Ce guide explique comment installer et configurer un exemple d'environnement au sein d'Amazon Web Services (AWS) grâce aux fonctionnalités ERSPAN intégrées à l'ExtraHop sonde et le vRouter Brocade 5600.

L'analyseur de port commuté à distance encapsulé (ERSPAN) vous permet de surveiller le trafic sur plusieurs interfaces réseau ou VLAN et d'envoyer le trafic surveillé vers une ou plusieurs destinations, y compris ExtraHop capteurs. Configuration d'ERSPAN sur le routeur Brocade 5600 avec l'ExtraHop sonde permet une analyse, une surveillance et une visibilité supplémentaires du trafic critiques sur AWS et d'autres plateformes cloud.

Références supplémentaires

Le document suppose un certain niveau de familiarité avec le réseautage. Pour suivre les étapes décrites dans ce guide, vous devez disposer d'un compte AWS. Si vous utilisez ExtraHop, Brocade ou Amazon Web Services pour la première fois, consultez les liens suivants pour obtenir des informations supplémentaires :

- Déployez l'ExtraHop sonde dans AWS
<https://docs.extrahop.com/current/install-ehv-de-aws/> 
- Utilisation du routeur Brocade 5600 vRouter 5600 dans AWS
<https://www.brocade.com/content/dam/common/documents/content-types/deployment-guide/brocade-vrouter-5600-amazon-aws-dp.pdf> 

Configuration d'un réseau de cloud privé virtuel AWS

Dans cette section, vous allez configurer un nouveau cloud privé virtuel (VPC), une passerelle Internet, des sous-réseaux et des services de routage.

Création d'un VPC

1. Connectez-vous à la console AWS.
2. Dans le Réseautage section, cliquez **VPC**.
3. Dans le Cloud privé virtuel section, cliquez **Vos VPC** puis cliquez sur **Création d'un VPC**.
4. Dans le Étiquette nominative dans ce champ, saisissez un nom pour le VPC.
5. Dans le Bloc CIDR champ, saisissez un bloc d'adresses IP pour le réseau, tel que 10.4.0.0/16.
6. Dans le Location champ, laissez l'option définie sur **Par défaut**.
7. Cliquez **Oui, créer**.



Note: Notez l'ID du VPC (vpc-nnnnnnnn), qui est nécessaire pour la procédure suivante.

Création d'une passerelle Internet

1. Dans le volet de navigation, cliquez sur **Passerelles Internet**, puis cliquez sur **Création d'une passerelle Internet**.
2. Dans le Étiquette nominative dans ce champ, saisissez un nom pour identifier la passerelle Internet. Ce paramètre autorise le trafic public entrant et sortant de votre cloud privé virtuel.
3. Cliquez **Oui, créer**.

Prenez note de l'ID de passerelle (igw-nnnnnnnn).

4. Cliquez **Joindre au VPC**.
5. Dans la liste déroulante, sélectionnez le VPC que vous avez créé, puis cliquez sur **Oui, joindre**.

Définissez des itinéraires

Avant que le trafic soit autorisé à entrer ou à sortir du nouveau VPC, les règles de routage et de sécurité du trafic doivent être configurées. Par défaut, tout le trafic sortant est autorisé, mais le trafic entrant est plus restrictif.

1. Dans le volet de navigation, cliquez sur **Tables de routage**.
2. Dans le tableau, cochez la case à côté de l'itinéraire associé au VPC que vous avez créé.
3. Cliquez sur **Itinéraires** onglet, puis cliquez sur **Modifier**.
4. Cliquez **Ajouter un autre itinéraire**.
5. Dans le champ Destination, tapez 0.0.0.0/0.
6. Dans le Cible dans ce champ, saisissez le nom que vous avez saisi pour la passerelle Internet.
7. Cliquez **Enregistrer**.



Destination	Target	Status	Propagated
10.4.0.0/16	local	Active	No
0.0.0.0/0	igw-7d126d18	Active	No

Création d'un sous-réseau

Cet exemple de réseau possède un sous-réseau public et privé dans le bloc CIDR que vous avez configuré précédemment. Vous allez configurer 10.4.0.0/24 en tant que sous-réseau public et 10.4.1.0/24 en tant que sous-réseau privé.

1. Dans le volet de navigation, cliquez sur **Sous-réseaux**, puis cliquez sur **Créer un sous-réseau**.
2. Dans l'Étiquette nominative dans ce champ, saisissez le nom du sous-réseau.
3. À partir du **VPC** liste déroulante, sélectionnez le VPC créé précédemment.
4. Optionnel : À partir du **Zone de disponibilité** dans la liste déroulante, sélectionnez la zone de disponibilité Amazon dans laquelle résidera le sous-réseau.
5. Dans le Bloc CIDR champ, saisissez le bloc CIDR public de 10.4.0.0/24.
6. Cliquez **Oui, créer**.

Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

Name tag ⓘ

VPC ⓘ

Availability Zone ⓘ

CIDR block ⓘ

7. Répétez les étapes 1 à 6 pour créer un sous-réseau privé avec 10.4.1.0/24 Bloc CIDR.

Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

Name tag ⓘ

VPC ⓘ

Availability Zone ⓘ

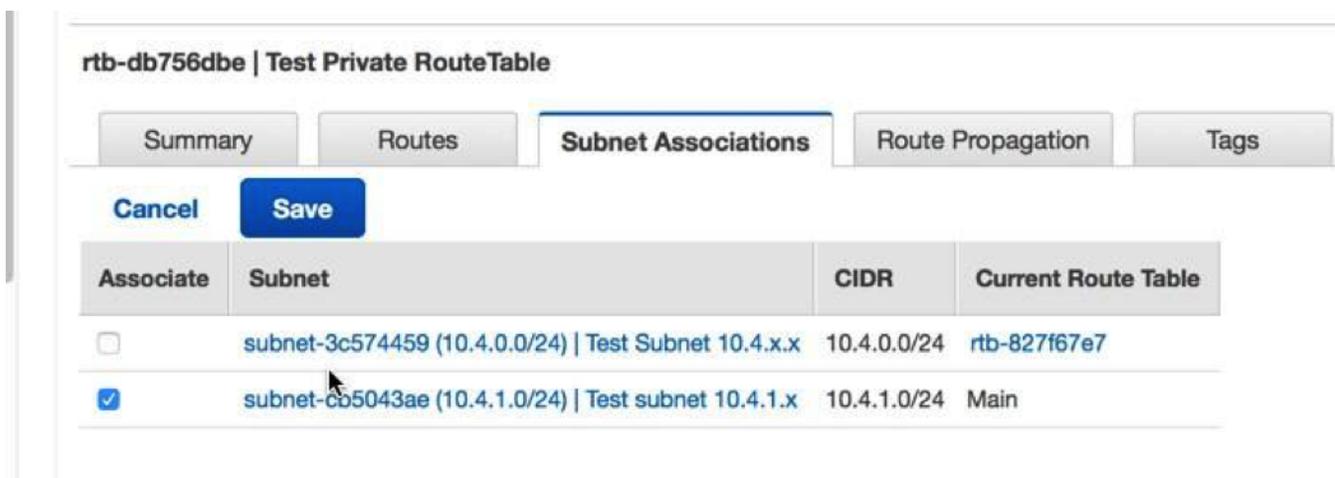
CIDR block ⓘ

Associer la table de routage au sous-réseau

1. Dans le volet de navigation, cliquez sur **Tables de routage**.
2. Vérifiez que la table de routage sélectionnée est la table contenant la passerelle Internet que vous avez créée précédemment.
3. Cliquez sur **Associations de sous-réseaux** onglet.
4. Cliquez **Modifier** et sélectionnez le sous-réseau public de 10.4.0.0/24, puis cliquez sur **Enregistrer**.



5. Cliquez **Créer une table de routage** pour créer une nouvelle table de routage pour le sous-réseau privé 10.4.1.0/24.
6. Dans le Étiquette nominative champ, tapez un nom pour la table de routage et sélectionnez le VPC que vous avez créé précédemment, puis cliquez sur **Oui, créer**.
7. Sélectionnez la table de routage créée pour le sous-réseau privé 10.4.1.0/24.
8. Sélectionnez le **Associations de sous-réseaux** onglet.
9. Cliquez **Modifier** et sélectionnez le sous-réseau privé 10.4.1.0/24 puis cliquez sur **Enregistrer**.
Prenez note de cette table de routage. Dans une étape suivante, une association est établie avec une route avec l'interface privée du Brocade vRouter.



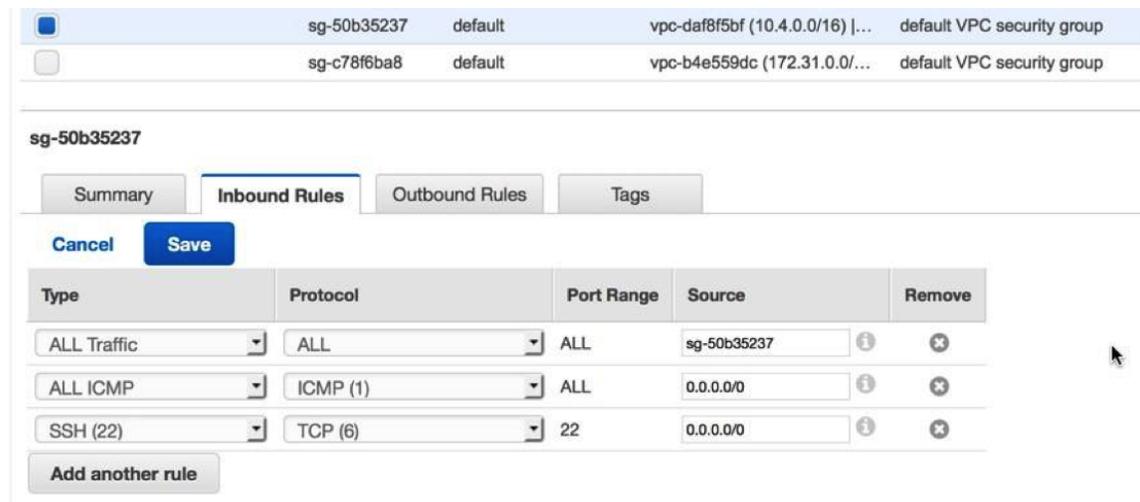
Ajouter des règles de trafic entrant au groupe de sécurité

1. Dans le volet de navigation, sélectionnez votre nouveau VPC dans **Filtrer par VPC** liste déroulante.
2. Dans le volet de navigation, cliquez sur **Groupes de sécurité**.
Le groupe de sécurité dispose de règles autorisant le trafic à entrer dans le VPC. La configuration initiale autorise tout le trafic provenant d'elle-même, tout ICMP (vous pouvez donc tester le ping de l'interface) et SSH sur le port 22.
3. Sélectionnez le groupe de sécurité par défaut pour votre nouveau VPC.
4. Cliquez sur le **Règles relatives au trafic entrant** onglet puis cliquez sur **Modifier**.
5. Cliquez **Ajouter une autre règle**.
6. Sélectionnez **Tous les ICMP** dans la liste déroulante et tapez 0.0.0.0/0 dans le La source champ.
7. Cliquez **Ajouter une autre règle**.

8. Sélectionnez **SSH (22)** dans la liste déroulante et tapez 0 . 0 . 0 . 0 / 0 dans le La source champ.
9. Cliquez **Enregistrer**.



Note: Il s'agit d'une configuration hors production ; vous n'autorisez généralement pas toutes les adresses IP à accéder à votre instance.



Type	Protocol	Port Range	Source	Remove
ALL Traffic	ALL	ALL	sg-50b35237	 
ALL ICMP	ICMP (1)	ALL	0.0.0.0/0	 
SSH (22)	TCP (6)	22	0.0.0.0/0	 

Résumé

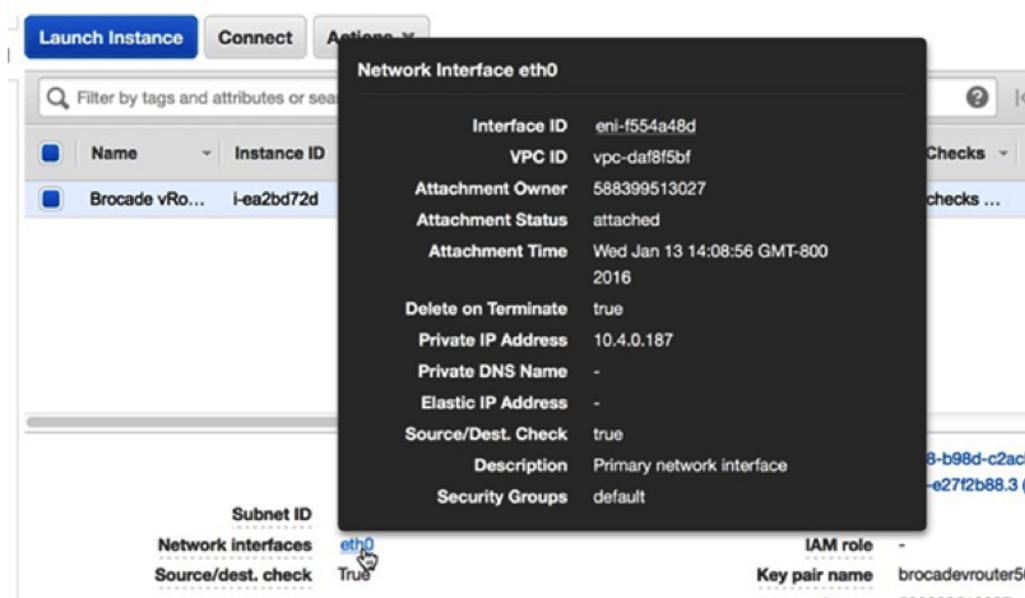
Dans cette section, vous avez créé un cloud public virtuel, un sous-réseau privé pour le réseau 10.4.1.0/24 et un sous-réseau public pour le réseau 10.4.0.0/24. En outre, vous avez créé des tables de routage pour acheminer le trafic au sein des sous-réseaux VPC et en externe via une passerelle Internet. Les groupes de sécurité autorisent le trafic entrant ou sortant du VPC et vous avez configuré des règles entrantes pour autoriser ICMP et du trafic SSH.

Configuration du routeur Brocade 5600v

Dans cette section, vous allez configurer un nouveau routeur Brocade 5600v dans le sous-réseau public créé précédemment et attribuer une adresse IP élastique pour configurer et tester la configuration via SSH.

1. Cliquez sur l'icône d'accueil de la console dans le coin supérieur gauche pour revenir à la page AWS Management Console.
2. Dans la section Calculer, cliquez sur **EC2**.
3. Dans le volet de navigation, cliquez sur **Instances**.
4. Cliquez **Lancer une instance** pour démarrer l'assistant Amazon Machine Image (AMI).
5. Cliquez **AWS Marketplace** et tapez 5600 ou Routeur virtuel Brocade dans le Rechercher des produits AWS Marketplace champ, puis appuyez sur ENTER.
6. Cliquez sur le **Sélectionnez** bouton à côté de **Routeur virtuel/pare-feu/VPN Brocade 5600**.
7. Pour cet exemple, sélectionnez **m4.large** type d'instance, puis cliquez sur **Suivant : Configurer les détails de l'instance**.
8. Sur le Configurer les détails de l'instance page, effectuez les étapes suivantes :
 - a) Type 1 dans le Nombre d'instances champ.
 - b) À partir du **Réseau** dans la liste déroulante, sélectionnez le VPC que vous avez créé dans la première section de ce guide.
 - c) Dans la liste déroulante Sous-réseau, sélectionnez le sous-réseau public, 10 . 4 . 0 . 0 / 24.
 - d) Dans le Interfaces réseau section en bas de page, tapez 10 , 4 , 0 , 187 dans le IP principale champ.

9. Cliquez **Suivant : Ajouter de l'espace de stockage**. Conservez les paramètres de stockage par défaut, puis cliquez sur **Suivant : Tag Instance**.
10. Tapez n'importe quel nom dans Valeur champ pour **Nom** clé pour identifier l'instance. Ajoutez des balises supplémentaires pour identifier cette instance dans l'environnement, puis cliquez sur **Suivant : Configuration du groupe de sécurité**.
11. Choisissez **Sélectionnez un groupe de sécurité existant** puis sélectionnez l'ID de groupe de sécurité par défaut pour votre VPC.
Assurez-vous que les règles créées précédemment ont été appliquées. Par exemple, SSH et ICMP sont toujours listés et leurs adresses sources sont 0.0.0.0/0. Facultativement, un nouveau groupe de sécurité peut être créé spécifiquement pour cette instance.
12. Cliquez **Révision et lancement** pour lancer et installer le Brocade vRouter.
13. Vérifiez les sélections et les entrées, en particulier les adresses de sous-réseau et IP. Si les coûts sont un problème, assurez-vous que l'instance est restée dans les limites de l'essai gratuit. Cliquez **Lancement** pour lancer l'instance et enregistrer le Brocade vRouter.
14. Dans la boîte de dialogue de la paire de clés, sélectionnez **Création d'une nouvelle paire de clés** dans le menu déroulant, saisissez un nom convivial et cliquez sur **Télécharger Key Pair** bouton pour télécharger la paire de clés. Assurez-vous de prendre note de l'emplacement du téléchargement.
15. Cliquez **Instances de lancement** pour terminer le processus d'installation.
16. Cliquez **Afficher les instances** au bas du État du lancement écran ou sélectionnez **Instances** depuis le volet de navigation. Selon les sélections, l'instance peut prendre plusieurs minutes pour être entièrement en ligne.
17. Une fois l'instance complètement lancée et le Contrôles de statut sont complets, cliquez sur **Descriptif** onglet en bas de page. Dans le Interfaces réseau section, cliquez **eth0**. Vérifiez que l'adresse IP est 10.4.0.187 (ou l'adresse IP configurée précédemment).
18. Cliquez sur le lien associé au Identifiant de l'interface. Dans cet exemple, l'ID est eni-f554a48d.



19. Lorsque l'interface privée du Brocade vRouter est sélectionnée, cliquez sur **Actions** menu déroulant et sélectionnez **Modifier Source/Dest. Vérifiez**.
20. Sélectionnez le **Désactivé** bouton radio puis cliquez **Enregistrer**.
21. Créez l'interface de sous-réseau privé pour le Brocade vRouter en cliquant sur **Création d'une interface réseau**.
22. Dans le Création d'une interface réseau dans une boîte de dialogue, renseignez les champs suivants :

Descriptif

Entrez un nom pour identifier l'interface privée.

Sous-réseau

Dans la liste déroulante, sélectionnez le sous-réseau pour 10.4.1.0/24.

IP privée

Type 10.4.1.10.

Groupes de sécurité

Sélectionnez le groupe de sécurité VPS par défaut.

23. Cliquez **Oui, créer** pour créer la nouvelle interface.
24. Sélectionnez l'interface privée, puis cliquez sur **Actions** menu déroulant et sélectionnez **Modifier Source/Dest. Vérifiez**.
25. Sélectionnez le **Désactivé** bouton radio puis cliquez **Enregistrer**.
Enregistrez ou prenez note du 10.4.1.10 ID d'interface réseau.
26. L'interface privée étant toujours sélectionnée, cliquez sur **Joindre**.
27. Sélectionnez votre instance dans la liste déroulante Instance ID, puis cliquez sur **Joindre**.
28. Retournez au tableau de bord du VPC.
29. Dans le volet de navigation, sélectionnez **Tables de routage**.
30. Sélectionnez la table de routage associée au sous-réseau privé 10.4.1.0/24.
31. Cliquez sur le **Itinéraires** onglet puis cliquez sur **Modifier**.
32. Cliquez **Ajouter un autre itinéraire**. Dans le Destination champ, type 0.0.0.0/0 et dans le champ cible, saisissez l'ID d'interface indiqué à l'étape 23, puis cliquez sur **Enregistrer**. Cette table de routage doit être associée à l'ID d'interface privée du Brocade vRouter et associée au sous-réseau privé 10.4.1.0/24.
33. Allouez une adresse IP Amazon Elastic, une adresse IP routée publiquement allouée dynamiquement, en sélectionnant **IP élastiques** depuis le volet de navigation. Cliquez **Allouer une nouvelle adresse**, puis cliquez sur **Oui, allouez**.
34. Dans le menu déroulant Actions, sélectionnez Adresse associée et définissez les champs suivants :

Associez-vous à

Interface réseau

Interface réseau

Sélectionnez l'ID d'interface publique du Brocade vRouter. Dans cet exemple, l'ID est eni-f554a48d.

adresse IP privée

Sélectionnez l'adresse IP attribuée au sous-réseau public. Dans cet exemple, il s'agit 10.4.0.187.

35. Cliquez **Oui, associé**.

Connectez-vous à votre instance Brocade vRouter via SSH



Note: Les procédures suivantes ont été effectuées dans une application de terminal macOS. Vos commandes peuvent varier en fonction de votre choix de client.

1. Ouvrez un terminal client et exécutez les commandes suivantes :
 - a) Accédez au répertoire dans lequel vous avez téléchargé votre fichier de clé privée. Par exemple :

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

- b) Modifiez les autorisations du fichier clé afin qu'il ne soit pas accessible au public :

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

- c) Établissez la connexion :

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

Par exemple :

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

Si la connexion SSH est réussie, une sortie similaire à la suivante apparaît :

```
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
```



Note: Si la connexion échoue, ajoutez `-vvv` au `ssh` commande pour collecter les résultats de débogage, vérifier les règles du groupe de sécurité pour s'assurer que le SSH est autorisé, vérifier que l'adresse IP élastique est associée à l'interface publique et vérifier que le ping envoyé à l'adresse IP élastique publique renvoie une réponse.

2. Affichez la liste des interfaces configurées en exécutant la commande suivante :

```
show interfaces
```

Un résultat similaire à ce qui suit apparaît :

```
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
```



Note: Si une seule interface apparaît, redémarrez le Brocade vRouter en exécutant le `redémarrer` commande.

3. Deux interfaces doivent être visibles. Aucune interface n'est configurée et aucune adresse IP n'apparaît. Pour configurer l'interface, exécutez les commandes suivantes :

- a) Entrez en mode de configuration :

```
configure
```

- b) Configurez l'interface privée avec l'adresse IP privée précédemment attribuée. Dans cet exemple, `10.4.1.0.24` a été attribué dans l'instance dans AWS sur l'interface privée.

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

- c) Définissez le nombre de demandes ARP (Address Resolution Protocol) gratuites à envoyer :

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

- d) Activez le filtre à chemin inversé sans validation de la source :

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

- e) Définissez le nombre de paquets NS à transmettre :

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

- f) Définit la taille de la MTU pour l'interface du plan de données :

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

- g) Définissez l'EtherType pour les trames VLAN :

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

4. Exécutez la commande `show interfaces` pour afficher les interfaces configurées. Un résultat similaire à ce qui suit s'affiche :

```
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
+ }
```

 **Note:** Le signe plus (+) indique les modifications non enregistrées.

5. Type `commettre` puis appuyez sur ENTER.
6. Type `sauver` puis appuyez sur ENTER pour enregistrer les modifications.
7. Optionnel : Définissez le port du service SSH sur 22 pour vous assurer que les ports sont correctement assignés sur le routeur Brocade dans le fichier de configuration :

```
set service ssh port 22
```

8. Type `commettre` puis appuyez sur ENTER.
9. Type `sauver` puis appuyez sur ENTER pour enregistrer les modifications.
10. Type `sortir` pour quitter le mode de configuration.
11. Exécutez le `afficher les interfaces` commande. Les deux interfaces doivent être opérationnelles et administrativement, comme dans le résultat suivant :

```
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

 **Note:** Laissez le shell vRouter ouvert pour exécuter des commandes supplémentaires ultérieurement dans cette procédure.

Résumé

Dans cette section, vous avez configuré le Brocade vRouter pour qu'il soit accessible et configurable depuis une machine distante. Vous avez également ajouté les interfaces appropriées pour la création de sous-réseaux supplémentaires.

(Facultatif) Configurer le client Linux pour la génération de trafic

Dans cette section et la suivante, vous allez configurer une nouvelle AMI Linux afin de vérifier la configuration de Brocade vRouter et d'ExtraHop Discover. Si d'autres sources de trafic sont disponibles, ces sections peuvent être ignorées.

 **Note:** Un client Linux est sélectionné dans l'exemple suivant.

1. Cliquez sur l'icône d'accueil de la console dans le coin supérieur gauche pour revenir à la page AWS Management Console.
2. Dans la section Calculer, cliquez sur **EC2**.
3. Dans le volet de navigation, cliquez sur **Instances**.
4. Cliquez **Lancer une instance** pour démarrer l'assistant Amazon Machine Image (AMI).
5. Localisez une image du serveur Ubuntu dans la liste, puis cliquez sur **Sélectionnez**.
6. Sélectionnez le **t2.micro** type d'instance, puis cliquez sur **Suivant : Configurer les détails de l'instance**.
7. Sur le Configurer les détails de l'instance page, effectuez les étapes suivantes :
 - a) Type 1 dans le Nombre d'instances champ.
 - b) À partir du **Réseau** dans la liste déroulante, sélectionnez le VPC que vous avez créé dans la première section de ce guide.
 - c) Dans la liste déroulante Sous-réseau, sélectionnez 10.4.1.0/24 sous-réseau.
Une adresse IP statique n'est pas nécessaire pour cette étape, mais notez l'adresse IP attribuée à l'instance. Dans cet exemple, l'adresse IP est 10.4.1.50.
 - d) Les autres paramètres peuvent être conservés à leurs valeurs par défaut.
8. Cliquez **Suivant : Ajouter de l'espace de stockage**. Aucune modification n'est nécessaire.
9. Cliquez **Suivant : Tag Instance**. Aucune modification n'est nécessaire.
10. Cliquez **Suivant : Configuration du groupe de sécurité**.
11. Sur le Configurer le groupe de sécurité page, effectuez les étapes suivantes :
 - a) Sélectionnez **Création d'un nouveau groupe de sécurité**.
 - b) Dans le **champ de nom du groupe de sécurité**, saisissez un nom descriptif. Par exemple, Ubuntu Linux.
 - c) Dans le Descriptif dans ce champ, saisissez une description pour ce groupe de sécurité.
 - d) Cliquez **Ajouter une règle**.
 - e) Sélectionnez **Tous les ICMP** depuis la liste déroulante.
 - f) Dans le La source colonne, sélectionnez **N'importe où** dans la liste déroulante et tapez 0.0.0.0/0 dans le champ.
 - g) Si SSH n'est pas répertorié, cliquez **Ajouter une règle**.
 - h) Dans le La source colonne, sélectionnez **N'importe où** dans la liste déroulante et tapez 0.0.0.0/0 dans le champ.
 - i) Cliquez **Révision et lancement**.

- j) Reconnaissez que votre groupe de sécurité est ouvert sur le monde, puis cliquez sur **Lancement**.
 -  **Note:** Il s'agit d'une configuration hors production. En règle générale, le trafic ne doit pas être configuré pour être ouvert sur le monde entier.
- k) Dans la boîte de dialogue de la paire de clés, sélectionnez **Création d'une nouvelle paire de clés** depuis la liste déroulante. Tapez un nom dans Nom de la paire de clés champ et cliquez **Télécharger Key Pair**. Notez l' emplacement du téléchargement, puis cliquez sur **Instances de lancement** pour terminer le processus d'installation.

(Facultatif) Configurer le NAT sur le vRouter pour le client Linux

Pour atteindre le client Linux sur le sous-réseau privé interne, à la fois entrant et sortant pour générer du trafic, le NAT doit être configuré sur le vRouter.

1. Revenez à l'invite du shell vRouter précédemment ouverte.
2. Ouvrez un port et masquez le trafic sortant en exécutant les commandes suivantes.
 - a) Entrez en mode de configuration :

```
configure
```

- b) Définissez le port de destination. Il s'agit d'un port arbitraire et 445 est spécifié dans cet exemple.

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

- c) Définissez l'interface entrante :

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

- d) Définissez le protocole :

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

- e) Définissez l'adresse de traduction, où `<client_instance_ip>` est l'adresse IP du client Linux :

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

Par exemple :

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

- f) Définissez le port de traduction :

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

- g) Type `commettre` puis appuyez sur ENTER.
 - h) Type `sauver` puis appuyez sur ENTER pour enregistrer les modifications.
 - i) Configurez le trafic sortant sur le vRouter pour masquer les adresses internes :

```
set service nat source rule 100 outbound-interface dp0s0
set service nat source rule 100 translation address masquerade
```

- j) Type `commettre` puis appuyez sur ENTER
 - k) Type `sauver` puis appuyez sur ENTER pour enregistrer les modifications.

 **Note:** Les numéros de règles sont arbitraires ; toutefois, laissez suffisamment d'espace entre les plages au cas où vous auriez besoin d'ajouter des règles connexes à l'avenir.

- Vérifiez que la configuration est mise à jour avec les règles que vous venez de créer en exécutant la commande suivante :

```
show service
```

Une sortie similaire à celle qui suit s'affiche. Notez le port de destination, le port de traduction et l'adresse de l'instance Linux créée. Assurez-vous également que l'interface des deux règles est l'interface externe du vRouter.

```
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
}
```

- Retournez à la console AWS pour créer une règle entrante sur le groupe de sécurité par défaut afin de tester les règles NAT.
 - Dans le volet de navigation, cliquez sur **Instances**.
 - Sélectionnez le vRouter dans la liste des instances.
 - Dans le **Descriptif** zone d'onglets, à côté de Groupes de sécurité, cliquez **défaut**.
 - Sur la page du groupe de sécurité, cliquez sur **Entrant** onglet.
 - Cliquez **Modifier**.
 - Cliquez **Ajouter une règle**.
 - Dans le **Type** liste déroulante, sélectionnez **Règle TCP personnalisée**.
 - Dans le Gamme de ports champ, type 445.
 - Dans le La source champ, type 0.0.0.0/0.

(Facultatif) Testez la configuration du client Linux

- Sur votre client ordinateur, ouvrez une nouvelle fenêtre de terminal.
- Connectez-vous au client AWS Linux ou Windows avec la paire de clés et le nom d'utilisateur appropriés.

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

Par exemple :

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



Note: Dans la console AWS, une fois l'instance sélectionnée, cliquez sur **Connecter** pour savoir comment vous connecter à votre instance spécifique. Les noms d'utilisateur et la connectivité sont propres à l'AMI sélectionnée.

- Une fois que vous vous êtes connecté avec succès au client, envoyez un ping aux adresses IP publiques et privées que vous avez configurées précédemment et assurez-vous que vous pouvez atteindre les adresses IP spécifiées. Par exemple :

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

- Ouvrez une nouvelle fenêtre de terminal et connectez-vous au Brocade vRouter avec le nom d'utilisateur et la paire de clés appropriés.
- Envoyez un ping à l'adresse IP du client Linux. Par exemple :

```
ping 10.4.1.50
```

- Affichez la feuille de route en exécutant la commande suivante :

```
show ip route
```

Un résultat similaire à ce qui suit s'affiche :

```
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
```

- Affichez le tableau ARP en exécutant la commande suivante :

```
show arp
```

Un résultat similaire au suivant apparaît :

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

- Affichez les interfaces en exécutant la commande suivante :

```
show interface
```

Un résultat similaire au suivant apparaît :

```
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
```

Résumé

Dans cette section, vous avez installé et configuré une instance Linux pour générer du trafic de paquets de test.

Configurer un ExtraHop EDA 1000v

Dans cette section, vous allez configurer une nouvelle sonde ExtraHop EDA 1000v.

1. Cliquez sur l'icône d'accueil de la console dans le coin supérieur gauche pour revenir à la page AWS Management Console.
2. Dans la section Calculer, cliquez sur **EC2**.
3. Dans le volet de navigation, cliquez sur **Instances**.
4. Cliquez **Lancer une instance** pour démarrer l'assistant Amazon Machine Image (AMI).
5. Cliquez **AMI communautaires**.
6. Type Hop supplémentaire dans le Rechercher des AMI communautaires champ et localisez le ExtraHop Discover appliance 1000v 5.x.x.x AMI et cliquez **Sélectionnez**.
7. Sélectionnez le **t2.medium** type d'instance, puis cliquez sur **Suivant : Configurer les détails de l'instance**.
8. Dans le Configurer les détails de l'instance page, effectuez les étapes suivantes :
 - a) Type 1 dans le Nombre d'instances champ.
 - b) Dans le **Réseau** dans la liste déroulante, sélectionnez le VPC créé dans la première partie de ce guide.
 - c) Dans le **Sous-réseau** liste déroulante, sélectionnez le sous-réseau privé 10.4.1.0/24.
 - d) Dans le Interfaces réseau type de section 10.4.1.15 dans le IP principale champ, puis cliquez sur **Suivant : Ajouter de l'espace de stockage**.
9. Conservez le paramètre par défaut pour la taille de stockage par défaut. Cliquez **Suivant : Tag Instance**.
10. Attribuez un nom à l'instance pour l'identifier. Ajoutez des balises supplémentaires pour identifier cette instance dans l'environnement, puis cliquez sur **Suivant : Configuration du groupe de sécurité**.
11. Sur le Configurer le groupe de sécurité page, effectuez les étapes suivantes :
 - a) Sélectionnez **Création d'un nouveau groupe de sécurité**.
 - b) Dans le Nom du groupe de sécurité champ, saisissez un nom descriptif. Par exemple, EDA 1000v.
 - c) Dans le Descriptif dans ce champ, saisissez une description pour ce groupe de sécurité.
 - d) Cliquez **Ajouter une règle** 6 fois et configurez chacune protocole tapez comme suit :

Type	Protocole	Gamme de ports	La source
SSH	TCP	22	N'importe où 0.0.0.0/0
HTTP	TCP	80	N'importe où 0.0.0.0/0
HTTPS	TCP	443	N'importe où 0.0.0.0/0
Règle TCP personnalisée	TCP	2003	N'importe où 0.0.0.0/0

Type	Protocole	Gamme de ports	La source
Règle UDP personnalisée	UDP	2003	N'importe où 0.0.0.0/0
Tout le trafic	TOUS	0-65535	IP personnalisée 10.4.0.0/16
Tous les ICMP	ICMP	0-65535	N'importe où 0.0.0.0/0

12. Cliquez **Révision et lancement**.



Note: Si un **Démarrage à partir d'un disque SSD (General Purpose)** une boîte de dialogue apparaît, sélectionnez la première option, puis cliquez sur **Suivant**.

13. Vérifiez la sélection d'instances, puis cliquez sur **Lancement**.

14. Dans le Sélectionnez une page de paire de clés existante boîte de dialogue, sélectionnez **Procéder sans paire de clés** depuis la liste déroulante. La majeure partie de la configuration est effectuée via les paramètres d'administration de la sonde, une paire de clés n'est donc pas nécessaire. Sélectionnez le **Je reconnais** case à cocher, puis cliquez sur **Instances de lancement**.

15. Accédez à votre liste d'instances dans AWS. Vérifiez que les vérifications d'état ont été effectuées avec succès et notez l'adresse IP de l'instance.

Configurer le NAT sur le vRouter pour accéder au système ExtraHop

Pour accéder au système ExtraHop, le NAT doit être configuré sur le vRouter.

1. Revenez à l'invite du shell vRouter précédemment ouverte.
2. Ouvrez un port et masquez le trafic sortant en exécutant les commandes suivantes.
 - a) Entrez en mode de configuration :

```
configure
```

- b) Définissez le port de destination. Il s'agit d'un port arbitraire et 8443 est spécifié dans cet exemple.

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

- c) Définissez l'interface entrante :

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

- d) Définissez le protocole :

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

- e) Définissez l'adresse de traduction, où <extrahop_instance_ip> est l'adresse IP du client Linux :

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

Par exemple :

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

- f) Définissez le port de traduction :

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

- g) Configurez le trafic sortant sur le vRouter pour masquer les adresses internes (si ce n'est déjà fait) :

```
set service nat source rule 100 outbound-interface dp0s0
set service nat source rule 100 translation address masquerade
```

- h) Tapez `commit`, puis appuyez sur ENTER.
 i) Type `save` puis appuyez sur ENTER pour enregistrer les modifications.



Note: Les numéros de règles sont arbitraires ; toutefois, laissez suffisamment d'espace entre les plages au cas où vous auriez besoin d'ajouter des règles connexes à l'avenir.

3. Vérifiez que la configuration est mise à jour avec les règles que vous venez de créer en exécutant la commande suivante :

```
show service
```

4. Retournez à la console AWS pour créer une règle entrante sur le groupe de sécurité par défaut afin de tester les règles NAT.
- Dans le volet de navigation, cliquez sur **Instances**.
 - Sélectionnez le vRouter dans la liste des instances.
 - Dans le **Description** zone d'onglets, à côté de Groupes de sécurité, cliquez **défaut**.
 - Sur la page du groupe de sécurité, cliquez sur le **Entrant** onglet.
 - Cliquez **Modifier**.
 - Cliquez **Ajouter une règle**.
 - Dans le **Type** liste déroulante, sélectionnez **Règle TCP personnalisée**.
 - Dans le Gamme de ports champ, type 8443.
 - Dans le La source champ, type 0.0.0.0/0.
5. Dans votre navigateur, saisissez l'adresse IP du système ExtraHop :

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

- Sur le Licences page, lisez les conditions générales d'ExtraHop, sélectionnez **Je suis d'accord**, puis cliquez sur **Soumettre**.
- Sur l'écran de connexion, tapez `installation` pour le nom d'utilisateur et l'ID d'instance pour le mot de passe. Vous trouverez l'ID d'instance sur la page Instances. Tapez les caractères suivants `i-` (mais pas `i-` lui-même), puis cliquez sur **Connectez-vous**.
- Sur le Administration des capteurs page, dans le Paramètres de l'appareil section, cliquez **Licence**.
- Cliquez **Gérer la licence** puis cliquez sur **S'inscrire**.
- Tapez la clé de produit obtenue auprès d'ExtraHop dans le champ Clé de produit, puis cliquez sur **S'inscrire**.



Note: Si l'enregistrement de licence échoue, assurez-vous que les règles de sécurité AWS autorisent le trafic sortant HTTP et trafic HTTPS.

- Cliquez **Terminé**.
- Retournez au **Administrateur** page.
- Dans le Réglages réseau section, cliquez **Connectivité**.
- Dans la section Interfaces, vérifiez que l'interface 1 est définie sur **Gestion + cible RPCAP/ERSPAN/VXLAN/GENEVE**.

(Facultatif) Créez un nouveau volume pour le stockage de capture de paquets

Créez un nouveau volume pour l'EDA 1000v afin de stocker les données de capture de paquets activées par le déclencheur.

- Dans le volet de navigation d'AWS, cliquez sur **Volumes**.

2. Cliquez **Créer un volume**. Dans le Boîte de dialogue Créer un volume boîte, assurez-vous que Zone de disponibilité sélectionné est la même zone que le Découvrir l'instance puis cliquez sur **Créer**.
3. Sélectionnez le nouveau volume dans la liste des volumes, puis sélectionnez **Joindre un volume** à partir du **Actions** menu déroulant. Dans le Instance champ, sélectionnez votre instance Discover , puis cliquez sur **Joindre**.
4. Dans le volet de navigation, cliquez sur **Instances**.
5. Sélectionnez l'instance Discover dans la liste, puis cliquez sur **Actions** > **État de l'instance** > **Redémarrer**.
6. Lorsque l'instance Discover revient à un état d'exécution, connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
7. Dans le Paramètres de l'appareil section, cliquez **Disques** et vérifiez que le nouveau disque de capture de paquets apparaît dans la liste des disques directement connectés.
8. Cliquez **Activer** sur le disque de capture de paquets pour l'activer.

Résumé

Dans cette section, vous avez configuré le système ExtraHop pour recevoir les paquets réseau et le trafic en provenance du ERSPAN interface. Facultativement, un disque supplémentaire a été configuré pour autoriser les captures de paquets activées par le déclencheur.

Configurer ERSPAN et la surveillance des ports sur le Brocade vRouter

Dans cette section, vous allez configurer le ERSPAN et des fonctionnalités de surveillance des ports sur le Brocade vRouter pour envoyer le trafic ERSPAN à la sonde ExtraHop.

1. Depuis une machine distante, SSH vers le vRouter.

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

2. Configurez l'interface ERSPAN en exécutant les commandes suivantes :

- a) Entrez en mode de configuration :

```
configure
```

- b) Définissez l'adresse IP locale pour l'interface ERSPAN :

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

- c) Définissez l'adresse IP distante pour l'interface ERSPAN :

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

- d) Définissez la configuration supplémentaire suivante :

```
set interfaces erspan erspan1 ip tos inherit
```

```
set interfaces erspan erspan1 ip ttl 255
```

```
set interfaces erspan erspan1 mtu 1500
```

- e) Afficher les modifications de configuration :

```
show interfaces
```

- f) Tapez commit, puis appuyez sur ENTER.
 - g) Tapez enregistrer, puis appuyez sur ENTER pour enregistrer les modifications.
3. Configurez le moniteur de port et la source ERSPAN en exécutant les commandes suivantes :

 **Note:** Dans cet exemple, la source du moniteur est l'interface interne du Brocade vRouter. De plus, les numéros de session et d'identifiant sont arbitraires, mais ne doivent pas chevaucher les autres identifiants de session.

- a) Définissez le type de session portmonitor :

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

- b) Définissez l'interface source pour la surveillance des ports :

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

- c) Définissez l'interface de destination pour la surveillance des ports :

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

- d) Définissez l'identifiant de session :

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

- e) Définissez le type d'en-tête ERSPAN :

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

- f) Définissez la direction de l'ERSPAN :

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

- g) Type `commettre` puis appuyez sur ENTER.

- h) Type `sauver` puis appuyez sur ENTER pour enregistrer les modifications.

La surveillance des ports pour la session est immédiatement activée si les paramètres de type, de source, de destination, d'identifiant ERSPAN et de type d'en-tête ERSPAN sont correctement configurés.

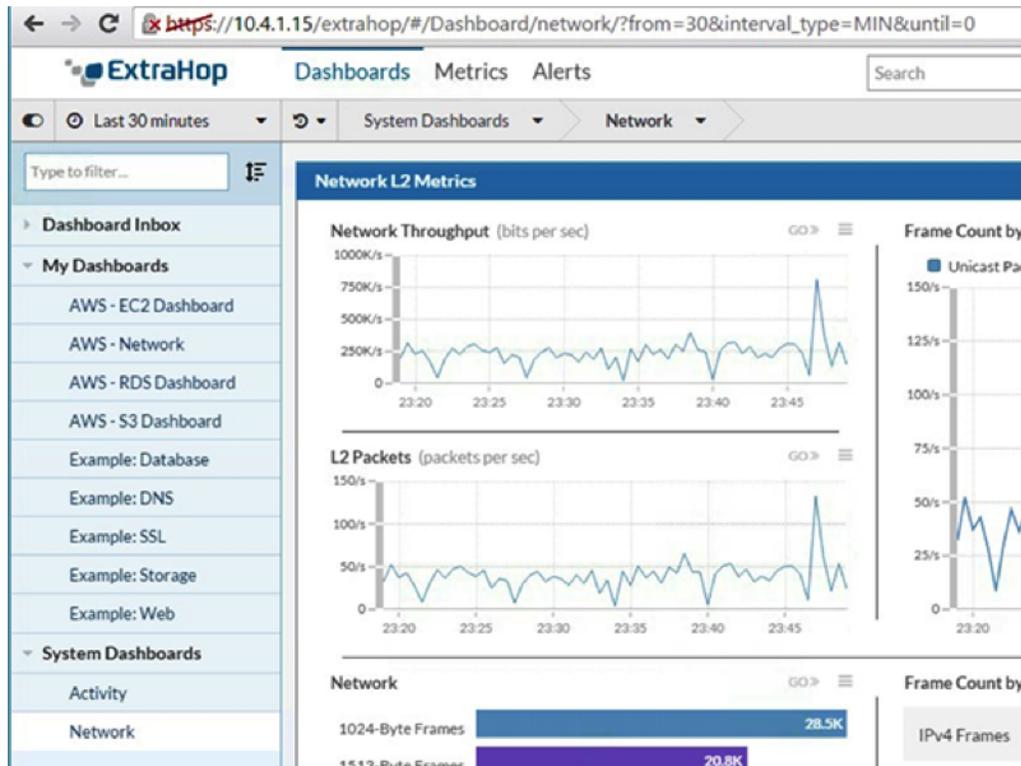
- i) Type `sortir` pour quitter le mode configuration.

- j) Type `afficher` la configuration pour afficher la nouvelle configuration.

Un résultat similaire au suivant apparaît (tronqué pour plus de clarté) :

```
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
    }
}
```

- Connectez-vous au système ExtraHop via `https://<elastic_public_ip>:8443/extrahop` et vérifiez que l'ExtraHop reçoit du trafic ERSPAN en provenance du vRouter depuis le Tableau de bord interface.



Résumé

Dans cette section, vous avez configuré le Brocade vRouter pour envoyer ERSPAN trafic vers le système ExtraHop permettant d'analyser le trafic au sein du cloud privé virtuel Amazon Web Services sans en installer RPCAPD clients.

Exemple de configuration de Brocade vRouter

```
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  
}
```