

Déployer ERSPAN avec un capteur ExtraHop et un vRouteur Brocade 5600 dans AWS

Publié: 2023-09-19

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

Encapsulated Remote Switched Port Analyzer (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 les capteurs ExtraHop. La configuration d'ERSPAN sur le Brocade 5600 vRouter avec le capteur ExtraHop permet de réaliser des analyses, une surveillance et une visibilité supplémentaires du trafic critique sur AWS et d'autres plates-formes en nuage.

Références supplémentaires

Ce document suppose un certain niveau de connaissance des réseaux. La réalisation des étapes de ce guide nécessite un compte AWS. Si vous ne connaissez pas ExtraHop, Brocade ou Amazon Web Services, consultez les liens suivants pour plus d'informations :

- Déployer le capteur ExtraHop dans AWS
<https://docs.extrahop.com/current/install-ehv-de-aws/> 
- Utilisation du vRouteur 5600 de Brocade dans AWS
<https://www.brocade.com/content/dam/common/documents/content-types/deployment-guide/brocade-vrouter-5600-amazon-aws-dp.pdf> 

Configurer un réseau de nuage privé virtuel AWS

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

Créer un VPC

1. Connectez-vous à la console AWS.
2. Dans la section Réseau, cliquez sur **VPC**.
3. Dans la section Cloud privé virtuel, cliquez sur **Vos VPC**, puis sur **Créer un VPC**.
4. Dans le champ Name tag, saisissez un nom pour le VPC.
5. Dans le champ Bloc CIDR, saisissez un bloc d'adresses IP pour le réseau, tel que 10.4.0.0/16.
6. Dans le champ Tenancy, laissez l'option définie sur **Default**.
7. Cliquez sur **Oui, Créer**.



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

Créer une passerelle Internet

1. Dans le volet de navigation, cliquez sur **Passerelles Internet**, puis sur **Créer une passerelle Internet**.
2. Dans le champ Balise de nom, saisissez un nom pour identifier la passerelle Internet.
Ce paramètre permet au trafic public d'entrer et de sortir de votre nuage privé virtuel.
3. Cliquez sur **Oui, Créer**.
Notez l'ID de la passerelle (igw-nnnnnnnn).

4. Cliquez sur **Attach to VPC (Attacher au VPC)**.
5. Dans la liste déroulante, sélectionnez le VPC que vous avez créé, puis cliquez sur **Oui, Attacher**.

Définir les itinéraires

Avant que le trafic ne 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 en regard de l'itinéraire associé au VPC que vous avez créé.
3. Cliquez sur l'onglet **Routes**, puis sur **Modifier**.
4. Cliquez sur **Ajouter un autre itinéraire**.
5. Dans le champ Destination, tapez 0.0.0.0/0.
6. Dans le champ Cible, tapez la balise de nom que vous avez saisie pour la passerelle Internet.
7. Cliquez sur **Enregistrer**.



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

Créer un sous-réseau

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

1. Dans le volet de navigation, cliquez sur **Sous-réseaux**, puis sur **Créer un sous-réseau**.
2. Dans le champ Balise de nom, saisissez un nom pour le sous-réseau.
3. Dans la liste déroulante **VPC**, sélectionnez le VPC créé précédemment.
4. Optionnel : Dans la liste déroulante **Zone de disponibilité**, sélectionnez la zone de disponibilité Amazon dans laquelle le sous-réseau résidera.
5. Dans le champ Bloc CIDR, saisissez le bloc CIDR public de 10.4.0.0/24.
6. Cliquez sur **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 le bloc CIDR 10.4.1.0/24.

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 ⓘ

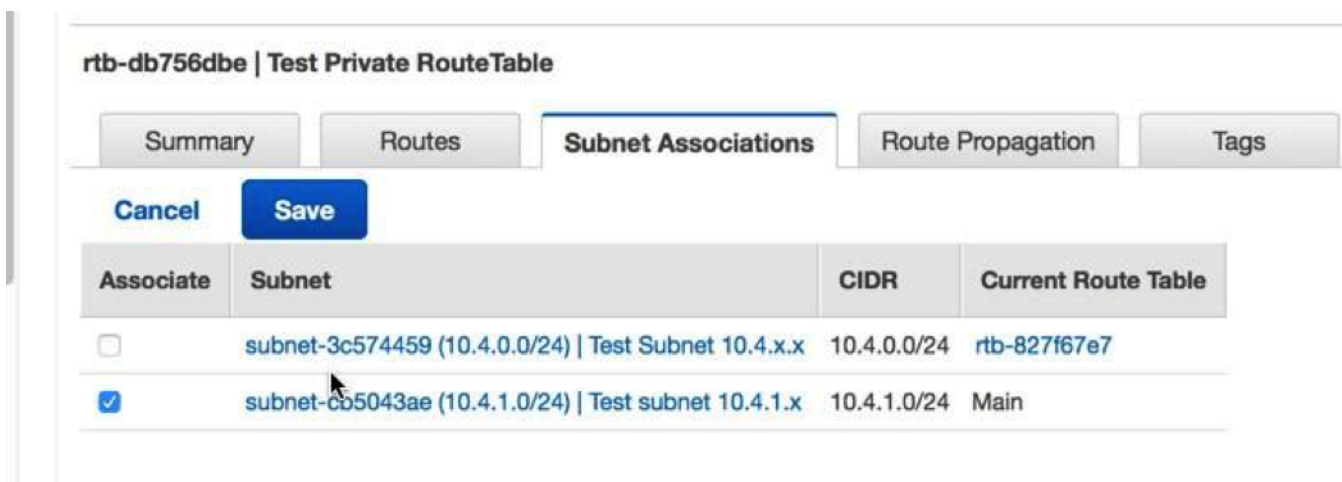
CIDR block ⓘ

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 celle qui contient la passerelle Internet que vous avez créée précédemment.
3. Cliquez sur l'onglet **Associations de sous-réseaux**.
4. Cliquez sur **Modifier** et sélectionnez le sous-réseau public de 10.4.0.0/24, puis cliquez sur **Enregistrer**.




5. Cliquez sur **Créer une table de rout** age pour créer une nouvelle table de routage pour le sous-réseau privé 10.4.1.0/24.
6. Dans le champ Balise de nom, saisissez 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 l'onglet **Subnet Associations (Associations de sous-réseau)**.
9. Cliquez sur **Edit** et sélectionnez le sous-réseau privé 10.4.1.0/24, puis cliquez sur **Save**.
Prenez note de cette table de routage, car dans une étape ultérieure, une association est faite à l'interface privée du vRouteur Brocade avec un routage.

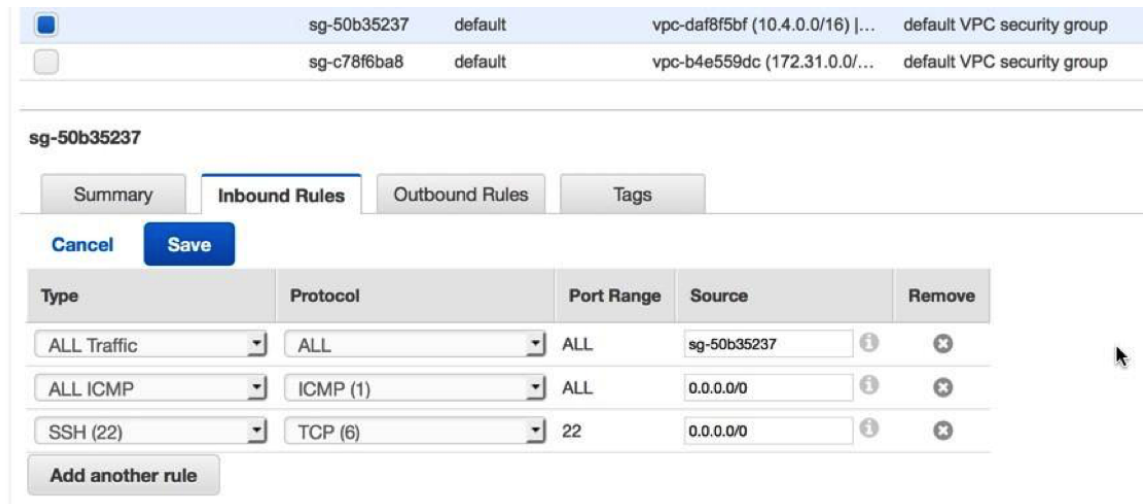


Ajouter des règles de réception au groupe de sécurité

1. Dans le volet de navigation, sélectionnez votre nouveau VPC dans le menu déroulant **Filtrer par VPC**.
2. Dans le volet de navigation, cliquez sur **Groupes de sécurité**.
Le groupe de sécurité comporte des règles autorisant le trafic à entrer dans le VPC. La configuration initiale autorise tout le trafic en provenance de lui-même, tous les ICMP (afin que vous puissiez 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 l'onglet **Règles d'entrée**, puis sur **Modifier**.
5. Cliquez sur **Ajouter une autre règle**.
6. Sélectionnez **All ICMP** dans la liste déroulante et tapez 0.0.0.0/0 dans le champ Source.
7. Cliquez sur **Ajouter une autre règle**.

8. Sélectionnez **SSH (22)** dans la liste déroulante et tapez `0.0.0.0/0` dans le champ Source.
9. Cliquez sur **Enregistrer**.

 **Note:** Il s'agit d'une configuration de non-production ; vous n'autoriserez généralement pas toutes les adresses IP à accéder à votre instance.



The screenshot shows the AWS Management Console interface for configuring a security group. At the top, there is a table listing security groups: `sg-50b35237` (selected) and `sg-c78f6ba8`. Below this, the configuration for `sg-50b35237` is shown, with tabs for Summary, Inbound Rules, Outbound Rules, and Tags. The Inbound Rules tab is active, displaying a table of rules:

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	

Buttons for 'Cancel' and 'Save' are visible above the table. An 'Add another rule' button is at the bottom.

Résumé

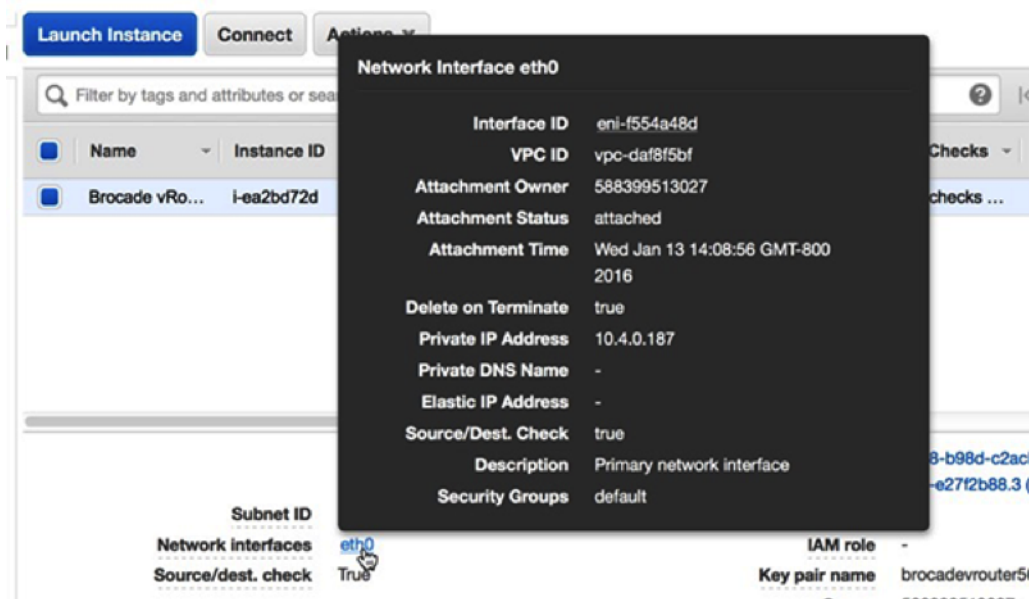
Dans cette section, vous avez créé un nuage public virtuel, un sous-réseau privé pour le réseau `10.4.1.0/24` et un sous-réseau public pour le réseau `10.4.0.0/24`. En outre, vous avez créé des tables de routage pour acheminer le trafic à l'intérieur des sous-réseaux VPC et vers l'extérieur par le biais d'une passerelle Internet. Les groupes de sécurité autorisent le trafic entrant ou sortant du VPC et vous avez configuré des règles d'entrée pour autoriser le trafic ICMP et 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 IP élastique pour configurer et tester la configuration via SSH.

1. Cliquez sur l'icône Console Home dans le coin supérieur gauche pour revenir à la page AWS Management Console.
2. Dans la section Compute, cliquez sur **EC2**.
3. Dans le volet de navigation, cliquez sur **Instances**.
4. Cliquez sur **Launch Instance** pour lancer l'assistant Amazon Machine Image (AMI).
5. Cliquez sur **AWS Marketplace** et tapez `5600` ou `Brocade vRouter` dans le champ Search AWS Marketplace Products, puis appuyez sur ENTER.
6. Cliquez sur le bouton **Select** en regard de **Brocade 5600 Virtual Router/Firewall/VPN**.
7. Pour cet exemple, sélectionnez le type d'instance **m4.large**, puis cliquez sur **Next : Configure Instance Details (Configurer les détails de l'instance)**.
8. Sur la page Configure Instance Details (Configurer les détails de l'instance), effectuez les étapes suivantes :
 - a) Tapez `1` dans le champ Nombre d'instances.
 - b) Dans la liste déroulante **Réseau**, sélectionnez le VPC que vous avez créé dans la première section de ce guide.
 - c) Dans la liste déroulante Subnet, sélectionnez le sous-réseau public, `10.4.0.0/24`.
 - d) Dans la section Interfaces réseau au bas de la page, tapez `10.4.0.187` dans le champ Primary IP.

9. Cliquez sur **Suivant : Ajouter du stockage**. Conservez les paramètres de stockage par défaut, puis cliquez sur **Suivant : Tag Instance**.
10. Saisissez un nom quelconque dans le champ Value (Valeur) de la clé **Name (Nom)** pour identifier l'instance. Ajoutez des balises supplémentaires pour identifier cette instance dans l'environnement, puis cliquez sur **Next(Suivant) : Configure Security Group (Configurer le groupe de sécurité)**.
11. Choisissez **Select an existing security group (Sélectionner un groupe de sécurité existant)** et sélectionnez l'ID du 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. En option, un nouveau groupe de sécurité peut être créé spécifiquement pour cette instance.
12. Cliquez sur **Review and Launch** pour lancer et installer le vRouteur Brocade.
13. Examinez les sélections et les entrées, en particulier le sous-réseau et les adresses IP. Si les coûts sont une préoccupation, assurez-vous que l'instance est restée dans les limites de l'essai gratuit. Cliquez sur **Launch** pour lancer l'instance et enregistrer le Brocade vRouter.
14. Dans la boîte de dialogue de la paire de clés, sélectionnez **Créer une nouvelle paire de clés** dans le menu déroulant, tapez un nom convivial et cliquez sur le bouton **Télécharger la paire de clés** pour télécharger la paire de clés. Veillez à noter l'emplacement du téléchargement.
15. Cliquez sur **Launch Instances** pour terminer le processus d'installation.
16. Cliquez sur **View Instances** en bas de l'écran Launch Status ou sélectionnez **Instances** dans le volet de navigation. L'instance, en fonction des sélections, peut prendre plusieurs minutes avant d'être entièrement en ligne.
17. Une fois que l'instance est entièrement lancée et que les vérifications d'état sont terminées, cliquez sur l'onglet **Description** en bas de la page. Dans la section Interfaces réseau, cliquez sur **eth0**. Vérifiez que l'adresse IP est 10.4.0.187 (ou l'adresse IP configurée précédemment).
18. Cliquez sur le lien associé à l'ID de l'interface. Dans cet exemple, l'ID est eni-f554a48d.



19. L'interface privée du vRouteur Brocade étant sélectionnée, cliquez sur le menu déroulant **Actions** et sélectionnez **Change Source/Dest. Check (Vérifier)**.
20. Sélectionnez la case d'option **Disabled (Désactivé)**, puis cliquez sur **Save (Enregistrer)**.
21. Créez l'interface de sous-réseau privée pour le vRouteur Brocade en cliquant sur **Create Network Interface (Créer une interface réseau)**.
22. Dans la boîte de dialogue Create Network Interface, remplissez les champs suivants :

Description

Saisissez 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

Tapez 10.4.1.10.

Groupes de sécurité

Sélectionnez le groupe de sécurité VPS par défaut.

23. Cliquez sur **Oui, Créer** pour créer la nouvelle interface.
24. Sélectionnez l'interface privée, puis cliquez sur le menu déroulant **Actions** et sélectionnez **Change Source/Dest. Vérifier**.
25. Sélectionnez la case d'option **Désactivé**, puis cliquez sur **Enregistrer**.
Enregistrez ou notez l'ID de l'interface réseau 10.4.1.10.
26. L'interface privée étant toujours sélectionnée, cliquez sur **Attach**.
27. Sélectionnez votre instance dans la liste déroulante Instance ID, puis cliquez sur **Attach**.
28. Retournez au tableau de bord 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 l'onglet **Routes**, puis sur **Modifier**.
32. Cliquez sur **Ajouter une autre route**. Dans le champ Destination, tapez 0.0.0.0/0 et dans le champ cible, tapez l'ID d'interface noté à l'étape 23, puis cliquez sur **Enregistrer**. Cette table de routage doit être associée à l'ID d'interface privée du vRouteur Brocade et au sous-réseau privé 10.4.1.0/24.
33. Allouez une IP Élastique Amazon, une IP routée publique allouée dynamiquement, en sélectionnant **IP Élastiques** dans le volet de navigation. Cliquez sur **Attribuer une nouvelle adresse**, puis sur **Oui, attribuer**.
34. Dans le menu déroulant Actions, sélectionnez Associer l'adresse et définissez les champs suivants :
 - Associer à**
Interface réseau
 - Interface réseau**
Sélectionnez l'ID de l'interface publique du vRouteur Brocade. 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 de 10.4.0.187.
35. Cliquez sur **Yes, Associate**.

Connexion à votre instance de 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 client de terminal 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 de clé afin qu'il ne soit pas visible par le public :

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

c) Établissez la connexion :

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

Par exemple :

```
ssh -i brocadevrouters5600.pem vyatta@52.35.186.255
```

Si la connexion SSH aboutit, une sortie similaire à la suivante s'affiche :

```
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` à la commande `ssh` pour collecter la sortie de débogage, vérifiez les règles du groupe de sécurité pour vous assurer que SSH est autorisé, vérifiez que l'IP élastique est associée à l'interface publique et vérifiez que le ping vers l'IP élastique publique renvoie une réponse.

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

```
show interfaces
```

Une sortie similaire à la suivante s'affiche :

```
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 vRouteur Brocade en exécutant la commande `reboot`.

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

a) Entrez en mode configuration :

```
configure
```

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

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

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

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

d) Activer le filtre de chemin inverse sans validation de la source :

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

e) Définir le nombre de paquets NS à transmettre :

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

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


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


g) Définit le type d'échange (EtherType) pour les trames VLAN :

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

4. Exécutez la commande `show interfaces` pour afficher les interfaces configurées. Une sortie similaire à la suivante 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. Tapez `commit` et appuyez sur ENTER.
6. Tapez `save` et appuyez sur ENTER pour enregistrer les modifications.
7. Optionnel : Définissez le port de service SSH sur 22 pour vous assurer que les ports sont correctement attribués sur le Brocade vRouter dans le fichier de configuration :

```
set service ssh port 22
```

8. Tapez `commit` et appuyez sur ENTER.
9. Tapez `save` puis appuyez sur ENTER pour enregistrer les modifications.
10. Tapez `exit` pour quitter le mode configuration.
11. Exécutez la commande `show interfaces`. Les deux interfaces doivent être actives et administrativement actives, comme le montre la sortie suivante :

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


 **Note:** Laissez le shell du vRouter ouvert pour exécuter d'autres commandes plus tard dans cette procédure.

Résumé

Dans cette section, vous avez configuré le vRouteur Brocade pour qu'il soit accessible et configurable à partir d'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 du Brocade vRouter et de l'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 Console Home dans le coin supérieur gauche pour revenir à la page AWS Management Console.
2. Dans la section Compute, cliquez sur **EC2**.
3. Dans le volet de navigation, cliquez sur **Instances**.
4. Cliquez sur **Launch Instance (Lancer une instance)** pour lancer l'assistant Amazon Machine Image (AMI).

5. Localisez une image de serveur Ubuntu dans la liste, puis cliquez sur **Sélectionner**.
6. Sélectionnez le type d'instance **t2.micro** et cliquez sur **Suivant : Configurer les détails de l'instance**.
7. Sur la page Configurer les détails de l'instance, effectuez les étapes suivantes :
 - a) Tapez **1** dans le champ Nombre d'instances.
 - b) Dans la liste déroulante **Réseau**, 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 **10.4.1.0/24**.
Une 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 laissés à leurs valeurs par défaut.
8. Cliquez sur **Suivant : Ajouter le stockage**. Aucune modification n'est nécessaire.
9. Cliquez sur **Suivant : Tag Instance**. Aucune modification n'est nécessaire.
10. Cliquez sur **Suivant : Configure Security Group (Configurer le groupe de sécurité)**.
11. Sur la page Configurer le groupe de sécurité, effectuez les étapes suivantes :
 - a) Sélectionnez **Créer un nouveau groupe de sécurité**.
 - b) Dans le **champ Nom du groupe de sécurité**, saisissez un nom descriptif. Par exemple, Ubuntu Linux.
 - c) Dans le champ Description, saisissez une description pour ce groupe de sécurité.
 - d) Cliquez sur **Ajouter une règle**.
 - e) Sélectionnez **Tous les ICMP** dans la liste déroulante.
 - f) Dans la colonne Source, sélectionnez **Anywhere** dans la liste déroulante et tapez **0.0.0.0/0** dans le champ.
 - g) Si **SSH** ne figure pas dans la liste, cliquez sur **Add Rule (Ajouter une règle)**.
 - h) Dans la colonne Source, sélectionnez **Anywhere** dans la liste déroulante et tapez **0.0.0.0/0** dans le champ.
 - i) Cliquez sur **Review and Launch (Réviser et lancer)**.
 - j) Confirmez que votre groupe de sécurité est ouvert au monde, puis cliquez sur **Lancer**.



Note: Il s'agit d'une configuration de non-production. En règle générale, le trafic ne doit pas être configuré de manière ouverte au monde.
 - k) Dans la boîte de dialogue de la paire de clés, sélectionnez **Créer une nouvelle paire de clés** dans la liste déroulante. Saisissez un nom dans le champ Nom de la paire de clés et cliquez sur **Télécharger la paire de clés**. Notez l'emplacement du téléchargement, puis cliquez sur **Lancer les instances** 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 en entrée et en sortie pour la génération de trafic, le NAT doit être configuré sur le vRouter.

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

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

- d) Définissez le protocole :

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

- e) Définir 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, le service nat destination rule 10 translation address `<client_ip_address>` :

```
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) Tapez `commit` et appuyez sur ENTER.

- h) Tapez `save` 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) Tapez `commit` puis appuyez sur ENTER

- k) Tapez `save` et appuyez sur ENTER pour enregistrer les modifications.



Note: Les numéros de règle sont arbitraires ; toutefois, prévoyez 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 qui viennent d'être créées en exécutant la commande suivante :

```
show service
```

Une sortie similaire à la suivante s'affiche. Notez le port de destination, le port de traduction et l'adresse de l'instance Linux créée. En outre, assurez-vous 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 }
```

4. Retournez à la console AWS pour créer une règle de réception sur le groupe de sécurité par défaut afin de tester les règles NAT.

- a) Dans le volet de navigation, cliquez sur **Instances**.

- b) Sélectionnez le vRouter dans la liste des instances.

- c) Dans la zone de l'onglet **Description**, à côté de Security groups (Groupes de sécurité), cliquez sur **default (Par défaut)**.

- d) Sur la page du groupe de sécurité, cliquez sur l'onglet **Inbound (Entrant)**.

- e) Cliquez sur **Édit (Modifier)**.

- f) Cliquez sur **Add Rule (Ajouter une règle)**.

- g) Dans la liste déroulante **Type**, sélectionnez **Custom TCP Rule (Règle TCP personnalisée)**.

- h) Dans le champ Port Range (Plage de ports), tapez 445.

- i) Dans le champ Source, tapez 0.0.0.0/0.

(Facultatif) Tester la configuration du client Linux

1. Sur votre ordinateur client, ouvrez une nouvelle fenêtre de terminal.
2. 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, l'instance étant sélectionnée, cliquez sur **Connecter** pour savoir comment vous connecter à votre instance particulière. Les noms d'utilisateur et la connectivité sont propres à l'AMI sélectionnée.

3. Après avoir réussi à vous connecter au client, effectuez un ping des adresses IP publiques et privées que vous avez configurées précédemment et assurez-vous que vous pouvez atteindre les IP spécifiées. Par exemple, vous pouvez envoyer un ping aux adresses IP publiques et privées que vous avez configurées précédemment :

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

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

```
ping 10.4.1.50
```

6. Affichez la feuille de route en exécutant la commande suivante :

```
show ip route
```

Une sortie similaire à la suivante s'affiche :

```
Codes : K - noyau, C - connecté, S - statique, 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 externe type 2 i -
IS-IS, L1 - IS-IS niveau 1, L2 - IS-IS niveau 2, ia - IS-IS inter area >
- route sélectionnée, * - route FIB, p - stale info Table des routes IP
pour VRF "default" La passerelle de dernier recours est 10.4.0.1 vers le
réseau 0.0.0.0 K *> 0.0.0.0/0 via 10.4.0.1, dp0s0 C *> 10.4.0.0/24 est
directement connecté, dp0s0 C *> 10.4.1.0/24 est directement connecté,
dp0s1 C *> 127.0.0.0/8 est directement connecté, lo
```

7. Affichez la table ARP en exécutant la commande suivante :

```
show arp
```

Des résultats similaires à ceux qui suivent s'affichent :

```
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. Affichez les interfaces en exécutant la commande suivante :

```
show interface
```

Une sortie similaire à la suivante s'affiche :

```
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 un trafic de paquets de test.

Configuration d'un ExtraHop EDA 1000v

Dans cette section, vous allez configurer un nouveau capteur ExtraHop EDA 1000v.

1. Cliquez sur l'icône Accueil de la console dans le coin supérieur gauche pour revenir à la page de la console de gestion AWS.
2. Dans la section Compute, cliquez sur **EC2**.
3. Dans le volet de navigation, cliquez sur **Instances**.
4. Cliquez sur **Launch Instance (Lancer une instance)** pour lancer l'assistant Amazon Machine Image (AMI).
5. Cliquez sur **Community AMIs**.
6. Tapez `ExtraHop` dans le champ Search community AMIs, localisez le site `ExtraHop Discover appliance 1000v 5.x.x.x AMI` et cliquez sur **Select**.
7. Sélectionnez le type d'instance **t2.medium**, puis cliquez sur **Suivant : Configurer les détails de l'instance**.
8. Dans la page Configurer les détails de l'instance, effectuez les étapes suivantes :
 - a) Tapez `1` dans le champ Number of instances.
 - b) Dans la liste déroulante **Réseau**, sélectionnez le VPC créé dans la première partie de ce guide.
 - c) Dans la liste déroulante **Subnet**, sélectionnez le sous-réseau privé `10.4.1.0/24`.
 - d) Dans la section Interfaces réseau, tapez `10.4.1.15` dans le champ Primary IP, puis cliquez sur **Next : Ajouter du stockage**.
9. Laissez la taille de stockage par défaut sur le paramètre par défaut. Cliquez sur **Next : Tag Instance (Suivant : Marquer l'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 **Next (Suivant) : Configurer le groupe de sécurité**.
11. Sur la page Configurer le groupe de sécurité, effectuez les étapes suivantes :
 - a) Sélectionnez **Créer un nouveau groupe de sécurité**.
 - b) Dans le champ Security group name (Nom du groupe de sécurité), saisissez un nom descriptif. Par exemple, `EDA 1000v`.
 - c) Dans le champ Description, saisissez une description pour ce groupe de sécurité.
 - d) Cliquez sur **Ajouter une règle** 6 fois et configurez chaque type de protocole comme suit :

Type	Protocole	Plage de ports	Source
SSH	TCP	22	N'importe où 0.0.0.0/0
HTTP	TCP	80	Partout 0.0.0.0/0
HTTPS	TCP	443	Partout 0.0.0.0/0

Type	Protocole	Plage de ports	Source
Règle TCP personnalisée	TCP	2003	Partout 0.0.0.0/0
Règle UDP personnalisée	UDP	2003	Partout 0.0.0.0/0
Tout le trafic	TOUS LES TRAFICS	0-65535	IP personnalisée 10.4.0.0/16
Tous ICMP	ICMP	0-65535	Partout 0.0.0.0/0

12. Cliquez sur **Review and Launch (Réviser et lancer)**.



Note: Si une boîte de dialogue **Boot from General Purpose (SSD)** apparaît, sélectionnez la première option, puis cliquez sur **Next (Suivant)**.

13. Examinez la sélection de l'instance, puis cliquez sur **Launch (Lancer)**.
14. Dans la boîte de dialogue **Select an existing key pair page (Sélectionner une paire de clés existante)**, sélectionnez **Proceed without a key pair (Procéder sans paire de clés)** dans la liste déroulante. La majeure partie de la configuration est effectuée par le biais des paramètres d'administration du capteur, une paire de clés n'est donc pas nécessaire. Cochez la case **J'accuse réception**, puis cliquez sur **Lancer les instances**.
15. Accédez à votre liste d'instances dans AWS. Confirmez que les contrôles d'état ont été effectués et notez l'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. Retournez 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 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 de réception :

```
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, le service nat destination rule 20 translation address `<extrahop_ip_address>` :

```
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) Configurer le trafic sortant sur le vRouter pour masquer les adresses internes (si ce n'est pas déjà fait) :

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

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



Note: Les numéros de règle 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 qui viennent d'être créées en exécutant la commande suivante :

```
show service
```

4. Retournez à la console AWS pour créer une règle de réception 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 la zone de l'onglet **Description**, à côté de Security groups (Groupes de sécurité), cliquez sur **default (Par défaut)**.
 - Sur la page du groupe de sécurité, cliquez sur l'onglet **Inbound (Entrant)**.
 - Cliquez sur **Edit (Modifier)**.
 - Cliquez sur **Add Rule (Ajouter une règle)**.
 - Dans la liste déroulante **Type**, sélectionnez **Règle TCP personnalisée**.
 - Dans le champ Port Range (Plage de ports), tapez 8443.
 - Dans le champ Source, tapez 0.0.0.0/0.
5. Dans votre navigateur, tapez l'adresse IP du système ExtraHop :

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

- Sur la page Licence, lisez les conditions générales d'ExtraHop, sélectionnez **J'accepte**, puis cliquez sur **Soumettre**.
- Sur l'écran de connexion, tapez `setup` 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. Saisissez les caractères qui suivent `i-` (mais pas `i-` lui-même), puis cliquez sur **Log In**.
- Sur la page Administration du capteur, dans la section Paramètres de l'appliance, cliquez sur **Licence**.
- Cliquez sur **Gérer la licence**, puis sur **Enregistrer**.
- Saisissez la clé de produit obtenue auprès d'ExtraHop dans le champ Clé de produit, puis cliquez sur **Enregistrer**.



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

- Cliquez sur **Terminé**.
- Retournez à la page d'**administration**.
- Dans la section Network Settings (Paramètres réseau), cliquez sur **Connectivity (Connectivité)**.
- Dans la section Interfaces, vérifiez que l'interface 1 est définie sur **Management + RPCAP/ERSPAN/VXLAN/GENEVE Target**.

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

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

1. Dans le volet de navigation dans AWS, cliquez sur **Volumes**.
2. Cliquez sur **Créer un volume**. Dans la boîte de dialogue Créer un volume, assurez-vous que la zone de disponibilité sélectionnée est la même que celle de l'instance Discover, puis cliquez sur **Créer**.
3. Sélectionnez le nouveau volume dans la liste Volumes, puis sélectionnez **Attacher le volume** dans le menu déroulant **Actions**. Dans le champ Instance, sélectionnez votre instance Discover, puis cliquez sur **Attacher**.
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 redevient opérationnelle, connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
7. Dans la section Appliance Settings (Paramètres de l'appareil), cliquez sur **Disks (Disques)** et vérifiez que le nouveau disque de capture de paquets apparaît dans la liste des disques directement connectés.
8. Cliquez sur **Enable (Activer)** sur le disque de capture de paquets pour l'activer.

Résumé

Dans cette section, vous avez configuré le système ExtraHop pour qu'il reçoive des paquets réseau et du trafic de l'interface ERSPAN. En option, un disque supplémentaire a été configuré pour permettre la capture de paquets avec déclenchement.

Configuration des fonctions ERSPAN et portmonitoring sur le vRouter Brocade

Dans cette section, vous allez configurer les fonctions ERSPAN et portmonitoring sur le vRouter Brocade pour envoyer le trafic ERSPAN au capteur ExtraHop.

1. A partir d'une machine distante, connectez-vous en SSH au vRouter.

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

2. Configurez l'interface ERSPAN en exécutant les commandes suivantes :
 - a) Entrez dans le mode de configuration :

```
configure
```

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

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

- c) Définissez l'adresse IP distante de 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) Affichez les modifications de configuration :

```
show interfaces
```

- f) Tapez commit et appuyez sur ENTER.

- g) Tapez `save` et 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 vRouteur Brocade. En outre, les numéros de session et d'identifiant sont arbitraires, mais ne doivent pas chevaucher d'autres identifiants de session.

- a) Définissez le type de session du moniteur de port :

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

- b) Définissez l'interface source pour la surveillance de port :

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

- c) Définir l'interface de destination pour le contrôle de port :

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

- d) Définir l'identifiant de la session :

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

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

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

- f) Définir la direction de l'ERSPAN :

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

- g) Tapez `commit` et appuyez sur `ENTER`.

- h) Tapez `save` et appuyez sur `ENTER` pour enregistrer les modifications.

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

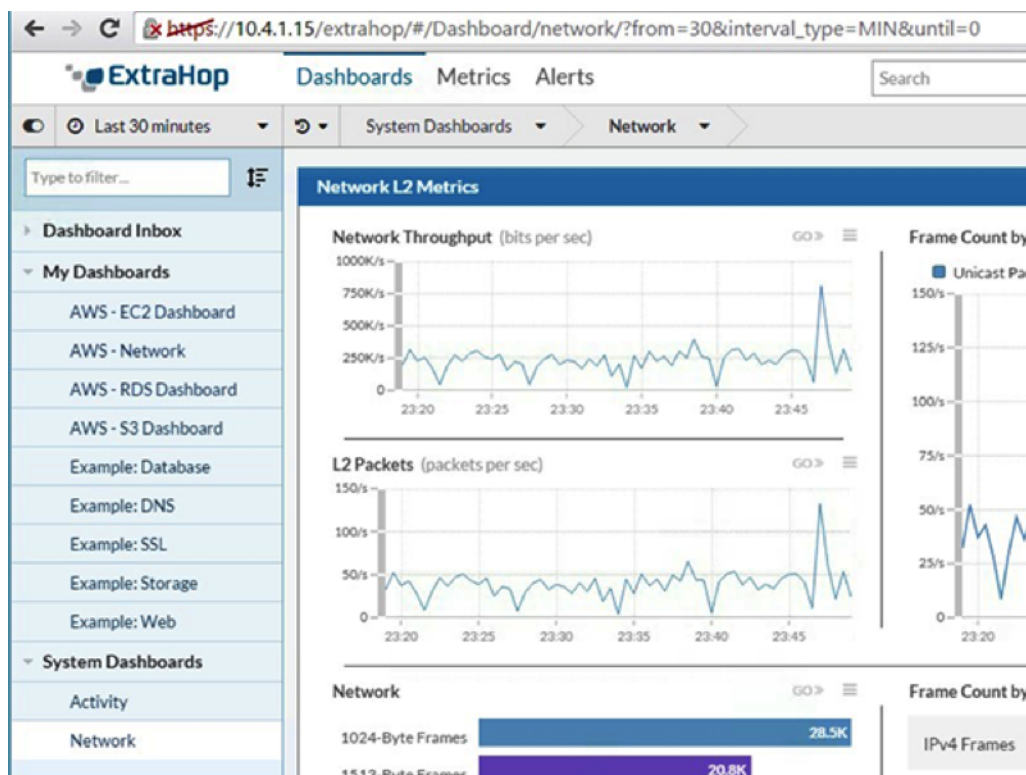
- i) Tapez `exit` pour quitter le mode de configuration.

- j) Tapez `show configuration` pour afficher la nouvelle configuration.

Une sortie similaire à la suivante apparaît (tronquée 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 } }
```

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



Résumé

Dans cette section, vous avez configuré le vRouteur Brocade pour qu'il envoie le trafic ERSPAN au système ExtraHop, ce qui permet d'analyser le trafic au sein du nuage privé virtuel Amazon Web Services sans installer de clients RPCAPD.

Exemple de configuration d'un vRouteur Brocade

```
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 { dest15 port 443 } } } source { rule
100 { outbound-interface dp0s0 translation { address masquerade } } }
portmonitor { session 25 { destination erspan1 erspan { header type-II
identifiant 200 } source dp0s1 { direction both } type erspan-source } } ssh
{ authentication-retries 3 disable-password-authentication port 22 timeout
12
```