

Configurer ERSPAN avec le Nexus 1000V

Publié: 2024-08-09


L'analyseur de port commuté à distance encapsulé (ERSPAN) vous permet de surveiller le trafic sur plusieurs interfaces réseau ou VLAN, puis d'envoyer le trafic surveillé vers une ou plusieurs destinations. Ce guide explique comment configurer ERSPAN sur un appareil ExtraHop Discover avec un commutateur Cisco Nexus 1000V exécuté sur un ordinateur Windows.

Ce guide part du principe que vous êtes familiarisé avec l'administration de base de Cisco.

Pour plus d'informations, consultez la documentation suivante :

- Cisco : *Configuration d'un profil de port ERSPAN*
- Hop supplémentaire : [Guide de l'interface utilisateur d'ExtraHop](#)

Configurer les paramètres de l'interface ExtraHop

 **Note:** Si vous sélectionnez **Interface 1** pour la gestion et **Interface 2** pour ERSPAN, vous ne pouvez pas configurer les deux interfaces sur le même sous-réseau.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Réglages réseau section, cliquez **Connectivité**.
3. Dans le Interfaces section, cliquez **Interface 1** ou **Interface 2**.
4. À partir du **Mode d'interface** liste déroulante, sélectionnez **Gestion + cible RPCAP/ERSPAN/VXLAN/GENEVE**.
5. Pour activer DHCP, cochez la case.
6. Dans le Adresse IP dans ce champ, saisissez l'adresse IP que vous souhaitez attribuer au port ExtraHop pour le trafic ERSPAN.
7. Dans le Masque réseau dans ce champ, saisissez le masque réseau du système ExtraHop .
8. Dans le Passerelle dans ce champ, saisissez l'adresse IP de la passerelle du système ExtraHop.
9. Cliquez **Enregistrer**.
10. Optionnel : Désactivez les autres interfaces, en fonction de vos besoins de configuration.

 **Note:** Pour plus d'informations sur la configuration des interfaces réseau, consultez [Connectivité](#) section du [Guide de l'interface utilisateur d'ExtraHop](#).

Configurer les paramètres du Nexus 1000V

1. Connectez-vous à votre module de supervision virtuelle (VSM).
2. Identifiez les hôtes Ethernet virtuels à surveiller en exécutant la commande suivante :

```
Switch# Show int virt
```

3. Passez en mode configuration en exécutant la commande suivante :

```
Switch# config terminal
```

4. Créez une nouvelle session de surveillance (également appelée session de port de duplication) en exécutant la commande suivante :

```
switch(config)# monitor session 1 type erspan-source
```

5. Configurez l'adresse IP cible ExtraHop ERSPAN en exécutant la commande suivante :

```
switch(config-erspan-src)# destination ip <ip-address>
```

où <ip-address> est l'adresse IP de destination de votre cible ERSPAN.

6. Définissez un ID ERSPAN en exécutant la commande suivante :

```
switch(config-erspan-src)# erspan-id <integer>
```

où <integer> est le numéro d'identification, tel que 1.

7. Définissez le MTU sur 9000 en exécutant la commande suivante :

```
switch(config-erspan-src)# mtu 9000
```



Note: Pour minimiser les risques de chutes, veillez à modifier le MTU par défaut du Nexus 1000V de 1500 à 9000. En outre, pensez à désactiver le déchargement par segmentation TCP sur les systèmes d'exploitation impliqués dans les communications transférées .

8. Ajoutez des sources de données en exécutant la commande suivante :

```
switch(config-erspan-src)# source <sources>
```

où se <sources> trouvent les sources de vos données.

1. Dans l'exemple suivant, les données proviennent d'un invité :

```
switch(config-erspan-src)# source interface vethernet 3-5 both
```

Dans cet exemple, `both` signifie que la machine virtuelle envoie et reçoit des données.

2. Dans l'exemple suivant, les données sont extraites de tout le trafic reçu par le VLAN :

```
switch(config-erspan-src)# source vlan 1010 rx
```

9. Activez la session de surveillance en exécutant la commande suivante :

```
switch(config-erspan-src)# no shut
```

10. Quittez la source ERSPAN et revenez au mode de configuration en exécutant la commande suivante :

```
switch(config-erspan-src)# exit
```

11. Quittez le mode de configuration et revenez à l'invite d'activation en exécutant la commande suivante :

```
switch(config)# exit
```

12. Enregistrez vos modifications en exécutant la commande suivante :

```
switch# copy running-config startup-config
```

13. Vérifiez les paramètres en exécutant la commande suivante :

```
switch# show monitor session 1
```

Dans l'exemple suivant, une session de surveillance fonctionnelle est

```

    session 1
    -----
    type           : erspan-source
    state          : up
    source intf    :
      rx           : Veth3      Veth4      Veth5
      tx           : Veth3      Veth4      Veth5
      both        : Veth3      Veth4      Veth5
    source VLANs  :
      rx           : 1010
      tx           :
      both        :
    source port-profile :
      rx           :
      tx           :
      both        :
    filter VLANs  : filter not specified
    destination IP : 10.10.247.93
    ERSPAN ID     : 1
    ERSPAN TTL    : 64
    ERSPAN IP Prec. : 0
    ERSPAN DSCP   : 0
    ERSPAN MTU    : 9000
    ERSPAN Header Type: 2
  
```

affichée :

Prochaines étapes

Connectez-vous au système ExtraHop via <https://<extrahop-hostname-or-IP-address>> et visualisez le trafic surveillé.