Supervision SNMP +

SNMP

SNMP permet aux administrateurs de gérer et de surveiller les appareils sur un réseau IP.

ÉLÉMENTS SNMP

- Gestionnaire SNMP
- Agent SNMP
- Mib

OPÉRATION SNMP

- Trap
- Get
- Set

Modèle et niveaux de sécurité SNMP

- Configuration du SNMP
- Étapes de configuration
- Configurer la chaîne communauté
- Emplacement du document de l'appareil
- Contact du système de documents
- Restreindre l'accès au SNMP
- Spécifier le destinataire des trap SNMP
- Activer les trap sur l'agent SNMP

```
(config)#snmp-server community <nom> RO
access-list 10 deny any log
snmp-server community public RO 10
```

Sécurisation SNMPv3

Niveaux de sécurité

SNMP offre 3 niveaux de sécurité différents:

- **noAuthNoPriv**
- **AuthNoPriv**
- **AuthPriv**

Auth signifie **Authentication** et Priv for **Privacy** (cryptage).

- noAuthNoPriv = *authentification du nom d'utilisateur et pas de cryptage* .
- AuthNoPriv = Authentification *MD5 ou SHA mais pas de chiffrement* .
- AuthPriv = *Authentification ET chiffrement MD5 ou SHA* .

SNMPv1 et SNMPv2 **ne prennent en charge que noAuthNoPriv** car ils ne proposent aucune authentification ni aucun cryptage. SNMPv3 prend en charge l' un des trois niveaux de sécurité. Lorsque vous décidez d'utiliser noAuthNoPriv pour SNMPv3, le nom d'utilisateur **remplacera la chaîne de communauté** .

La chaîne de communauté pour SNMPv1 et SNMPv2 est envoyée en texte clair. SNMPv3 est beaucoup plus sécurisé car il n'envoie pas les mots de passe de l'utilisateur en texte clair, mais utilise l'authentification par hachage MD5 ou SHA1. Le cryptage est effectué à l'aide de DES, 3DES ou AES.

Configurer la communauté SNMP avec la liste d'accès

Les meilleures pratiques actuelles recommandent d'appliquer des listes de contrôle d'accès (ACL) aux chaînes de communauté et de s'assurer que les chaînes de communauté de requête ne sont pas identiques aux chaînes de communauté de notification. Les listes d'accès offrent une protection supplémentaire lorsqu'elles sont utilisées en combinaison avec d'autres mesures de protection.

Cet exemple configure ACL en chaîne de communauté

```
access-list 10 deny any snmp-server host 1.1.1.1 mystring1
snmp-server community mystring1 RO 10
```

Exemple de configuration

- Attribuez un ID de moteur à l'entité SNMP (facultatif).
- Définissez un utilisateur, **userone** , appartenant au groupe **groupone** et appliquez **noAuthentication** (pas de mot de passe) et **noPrivacy** (pas de cryptage) à cet utilisateur.
- Définissez un utilisateur, **usertwo** , appartenant au groupe **grouptwo** et appliquez **noAuthentication** (pas de mot de passe) et **noPrivacy** (pas de cryptage) à cet utilisateur.
- Définissez un utilisateur, **userthree** , appartenant au groupe **groupthree** et appliquez une **authentification** (le mot de passe est user3passwd) et une **confidentialité** (sans cryptage) à cet utilisateur.
- Définissez un utilisateur, **userfour** , appartenant au groupe **groupfour** et appliquez l' **authentification** (le mot de passe est user4passwd) et la **confidentialité** (chiffrement des56) à cet utilisateur.
- Définissez un groupe, **groupone** , à l'aide de USM (User Security Model) V3 et disposant d'un accès en lecture sur la vue **v1default** (valeur par défaut).
- Définissez un groupe, **grouptwo** , à l'aide de USM V3 et disposant d'un accès en lecture sur la vue **myview** .
- Définissez un groupe, **groupthree** , à l'aide de USM V3, disposant d'un accès en lecture sur la vue **v1default** (par défaut) et à l'aide de l' **authentification** .
- Définissez un groupe, **groupfour** , à l'aide de USM V3, disposant d'un accès en lecture sur la vue **v1default** (par défaut) et à l'aide de **Authentication** and **Privacy** .
- Définissez une vue, **myview** , qui fournit un accès en lecture sur la MIB-II et refuse l'accès en lecture sur la MIB Cisco privée.

```
snmp-server engineID local 111100000000000000000000
snmp-server user userone groupone v3
snmp-server user usertwo grouptwo v3
snmp-server user userthree groupthree v3 auth md5 user3passwd snmp-
server user userfour groupfour v3 auth md5 user4passwd priv des56
```

```
user4priv
snmp-server group groupone v3 noauth
snmp-server group grouptwo v3 noauth read myview
snmp-server group groupthree v3 auth
snmp-server group groupfour v3 priv
snmp-server view myview mib-2 included
snmp-server view myview cisco excluded
snmp-server community public RO
```

Cisco Switch Port Analyzer (SPAN)

Miroir de port

La fonction de miroir de port permet un commutateur pour copier et envoyer des trames Ethernet des ports spécifiques au port de destination connecté à un analyseur de paquets. La trame d'origine est toujours transmise de la manière habituelle.

Le SPAN permet à un switch de rediriger le trafic d'un port source vers un port de destination ceci afin d'analyser ce flux.

Le SPAN se configure à l'aide de la commande monitor session et une suite de paramètres définissant la source et la destination. Le nombre de session simultanée peut différer selon la plateforme du switch. Les switchs C3550 et C2950 ne supporte que 2 sessions simultanées, alors que les switchs plus puissant peuvent supporter jusqu'à 64 sessions.

Remarques sur la Source

- Un port source peut être utilisé dans plusieurs sessions SPAN simultanément.
- Un port source peut faire partie d'un Etherchannel.
- Un port source ne peut pas être défini comme port de destination.
- Un port source peut être de n'importe quel type – Ethernet, FastEthernet, etc.

Remarque sur la Destination

- Un port de destination peut être de n'importe quel type.
- Un port de destination ne peut être utilisé que dans une seule session SPAN.
- Un port de destination ne peut être un port source.
- Un port de destination ne peut faire partie d'un Etherchannel.
- Un port de destination ne participe pas dans STP, CDP, VTP, PaGP, LACP, ou DTP.

Configuration

Spécifier le port source

```
SW(config)# monitor session 1 source interface fa 0/1
```

Il est possible de spécifier une plage de ports en source

```
SW(config)# monitor session 1 source interface fa 0/1 – 5
```

Spécifier le port de destination

```
SW(config)# monitor session 1 destination interface fa 0/10
```

RSPAN – Remote SPAN

Dans ce cas le port source et le port destination ne sont pas sur le même switch. Il faut alors créer un nouveau VLAN pour transporter ce trafic “mirroir”.

Voici quelques points à avoir en tête avant de configurer un RSPAN:

- S’il y a des switches intermédiaires entre les 2 switches source et destination, ils doivent être RSPAN-capable.
- VTP traite le VLAN configuré pour le RSPAN comme tout autre VLAN. Ce VLAN sera propagé dans le domain VTP s’il est créé sur le serveur VTP. Sinon, il faut créer ce VLAN sur tous les switches utilisés pour transporter ce flux.
- Les adresses MAC ne sont pas enregistrées sur un VLAN RSPAN.
- La source et la destination doivent être définis sur le switch disposant du port source mais aussi sur le port disposant du port de destination, cependant ces commandes ne seront pas identiques.

Configuration

Créer un VLAN pour le RSPAN

```
SW1(config)# vlan 99

SW1(config-vlan)# remote-splan
```

Configuration du switch source
Définir le port source
SW1(config)# monitor session 2 source interface fast 0/4

Définir la destination
SW1(config)# monitor session 2 destination remote vlan 99

Configuration du switch destination
Définir la source
SW2(config)# monitor session 2 source remote vlan 99
Définir le port destination
SW2(config)# monitor session 2 source interface fast 0/10

Vérification
SW2# show monitor

Résumé

À la couche 2, il existe un certain nombre de vulnérabilités qui nécessitent des techniques d'atténuation spécialisées :

- Les attaques d'inondation de la table d'adresse DU MAC sont traitées avec la sécurité du port.
- Les attaques VLAN sont contrôlées par la désactivation du DTP et le respect des directives de base pour la configuration des ports de tronc.
- Les attaques DHCP sont traitées par l'espionnage DHCP.

Le protocole SNMP comporte trois éléments : le gestionnaire, l'agent et le MIB. Le gestionnaire SNMP réside sur le Network Managment Server, tandis que l'agent et la MIB sont sur les appareils du client.

Le gestionnaire SNMP peut sonder les périphériques du client pour obtenir des informations, ou il peut utiliser un message TRAP qui indique à un client de signaler

immédiatement si le client atteint un seuil particulier. SNMP peut également être utilisé pour modifier la configuration d'un appareil.

SNMPv3 est la version recommandée car elle assure la sécurité.

L'analyseur de port (SPAN) est employé pour refléter le trafic allant et/ou venant de l'hôte. Il est généralement mis en œuvre pour prendre en charge les analyseurs de trafic ou les périphériques IPS.