Atténuer les attaques d'ARP

1. Inspection ARP dynamique (DAI : Dynamic ARP Inspection)

Dans une attaque ARP typique, un acteur de menace peut envoyer des réponses ARP non sollicitées à d'autres hôtes du sous-réseau avec l'adresse MAC de l'acteur de menace et l'adresse IP de la passerelle par défaut. Pour empêcher l'usurpation ARP et l'empoisonnement ARP qui en résulte, un commutateur doit garantir que seules les requêtes et les réponses ARP valides sont relayées.

L'inspection ARP Dynamique (DAI) nécessite l'espionnage DHCP (snooping) et aide à prévenir les attaques ARP en :

- Ne pas relayer les réponses ARP non valides ou gratuites vers d'autres ports du même VLAN.
- Interception de toutes les requêtes et les réponses ARP sur les ports non approuvés.
- Vérification de chaque paquet intercepté pour une liaison IP-MAC valide.
- Abandon et journalisation des réponses ARP provenant de non valides pour empêcher l'empoisonnement ARP.
- Error-disabling l'interface si le nombre DAI des paquets ARP configurés sont dépassées.

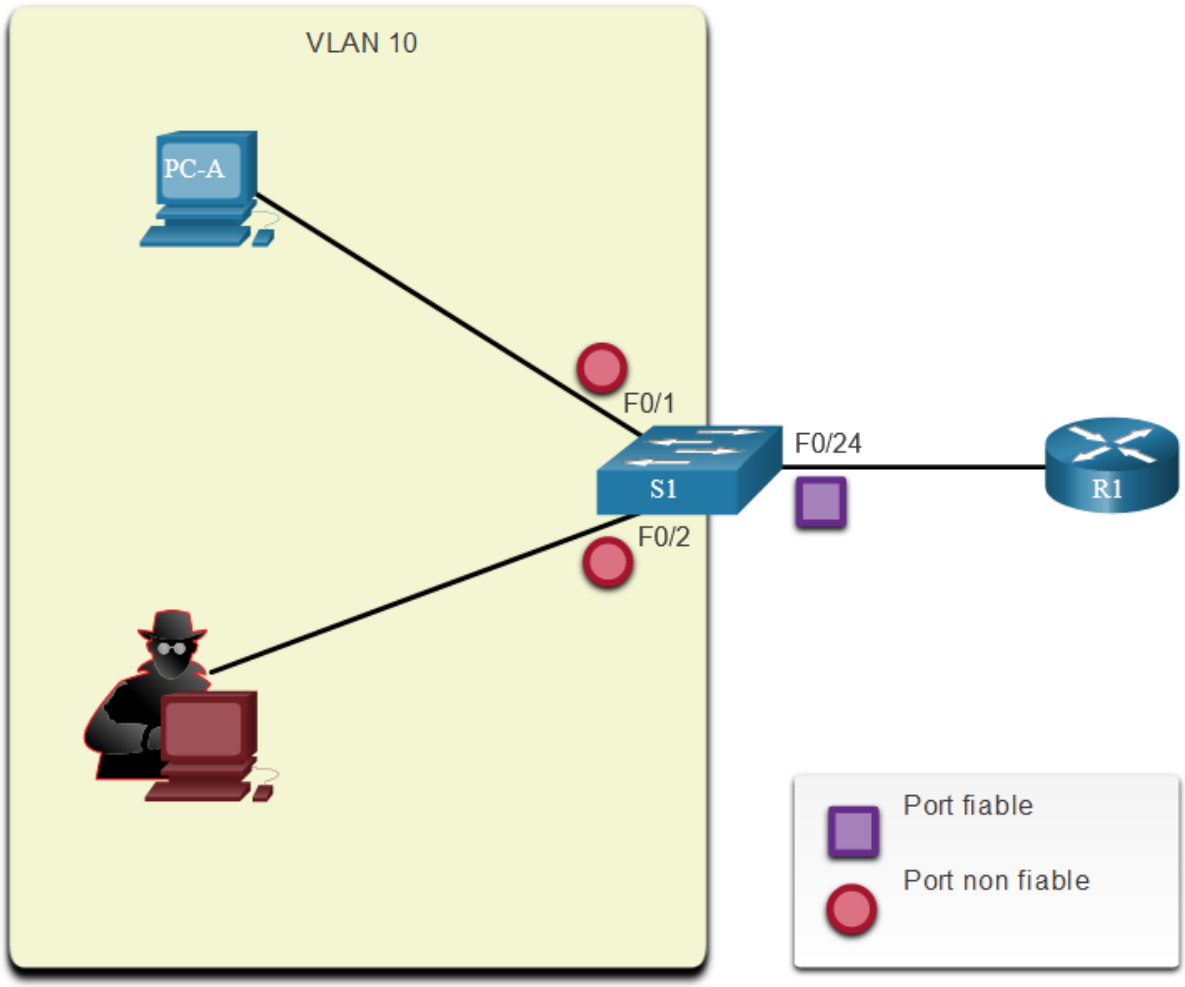
2. Directives de mettre en œuvre DAI

Pour atténuer les risques d'usurpation ARP et d'empoisonnement ARP, suivez ces directives d'implémentation DAI:

- Activez globalement L'espionnage DHCP (snooping).
- Activer l'espionnage DHCP sur les VLAN sélectionnés.
- Activer l'inspection ARP dynamique (DAI) sur les VLAN sélectionnés.
- Configurer les interfaces approuvées avec l'espionnage DHCP et l'inspection ARP.

Il est généralement conseillé de configurer tous les ports de commutateur d'accès comme non approuvés et de configurer tous les ports de liaison montante qui sont connectés à d'autres commutateurs comme approuvés.

L'exemple de topologie de la figure identifie les ports approuvés et non approuvés.



3. Exemple de configuration DAI

Dans la topologie précédente, S1 connecte deux utilisateurs sur le VLAN 10. DAI sera configuré pour atténuer les attaques d'usurpation ARP et d'empoisonnement ARP.

Comme indiqué dans l'exemple, l'espionnage DHCP est activée car DAI nécessite la table de liaison d'espionnage DHCP pour fonctionner. Ensuite, la surveillance DHCP et l'inspection ARP sont activés pour les PC sur VLAN10. Le port de liaison montante vers le routeur est approuvé et est donc configuré comme approuvé pour l'espionnage DHCP et l'inspection ARP.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection trust
```

L'inspection ARP dynamique (DAI) peut être configuré pour examiner la destination ou la source des adresses MAC et IP :

- **MAC de destination** -vérifie l'adresse MAC de destination dans l'en-tête Ethernet par rapport à l'adresse MAC cible dans le corps ARP.

- **Source MAC** - Vérifie la source Adresse MAC dans l'en-tête Ethernet contre l'expéditeur Adresse MAC dans le corps ARP.
- **Adresse IP** - Vérifie le corps ARP pour incorrecte et inattendues adresse IP y compris l'adresses 0.0.0.0, 255.255.255.255 et tous les adresses multidiffusion IP.

La commande de configuration globale **ip arp inspection validate {[src-mac][dst-mac] [ip]}** est utilisée pour configurer DAI pour supprimer les paquets ARP lorsque les adresses IP ne sont pas valides. Il peut être utilisé lorsque les adresses MAC dans le corps des paquets ARP ne correspondent pas aux adresses spécifiées dans l'en-tête Ethernet. Remarquez dans l'exemple suivant comment une seule commande peut être configurée. Par conséquent, la saisie de plusieurs commandes **ip arp inspection validate** écrase la commande précédente. Pour inclure plusieurs méthodes de validation, saisissez-les sur la même ligne de commande comme indiqué et vérifié le résultat suivante.

```
S1(config)# ip arp inspection validate ?
dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```