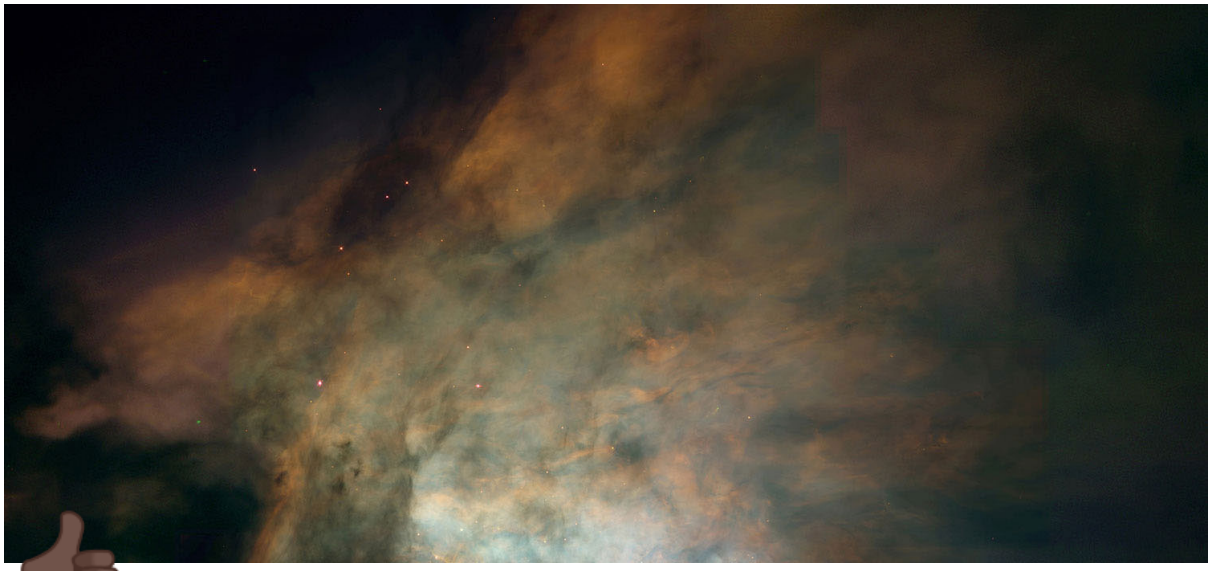

Projet

Sécurité des protocoles de routages (RIP, OSPF)

RIP

RIP peut paraître comme un protocole dépassé, mais il peut être utilisé à l'intérieure des petits réseaux LAN ou le nombre de router ne dépasse pas 50.

D'après le RFC 2453

RIP utilise le protocole UDP 520

C'est un protocole qui utilise l'adresse multicast 224.0.0.0

Mode non sécurisé :

- Pas d'authentification de la source
- Pas d'assurance de délivrance sur la confidentialité des routes

Mais RIPv2 prévoit :

- Authentification et Cisco à rajouter une authentification MD5.

Mais cette sécurité n'est pas par défaut au protocole il faut le configurer

Configuration du protocole et mise en place de la sécurité d'authentification en clair

On commence par configuré une chaine de caractère sur les routeurs concernés de manière identiques et appliquer sur les interfaces concernés avec la chaine qui vas avec.

Exemple R1 et R2

R1	R2

Router(config)#key chain amadou
Router(config-key Chain)# key (number)
Router(config-keychain-key)#key-string exemple
	Router(config)#key chain amadou
	Router(config-key Chain)# key (number)
	Router(config-keychain-key)#key-string exemple

Int <interface du router> Ip add <address> <masque>	Int <interface du router> Ip add <address> <masque>
Ip rip authentification key-chain amadou	Ip rip authentification key-chain amadou
Router rip Version 2 Network <addresse>	Router rip Version 2 Network <addresse>

Configuration par authentification md5

R1	R2

Router(config)#key chain amadou
Router(config-key Chain)# key (number)
Router(config-keychain-key)#key-string exemple
	Router(config)#key chain amadou
	Router(config-key Chain)# key (number)
	Router(config-keychain-key)#key-string exemple

Int <interface du router> Ip add <address> <masque>	Int <interface du router> Ip add <address> <masque>
Ip rip authentification mode md5 Ip rip authentification key-chain amadou	Ip rip authentification mode md5 Ip rip authentification key-chain amadou
Router rip Version 2 Network <addresse>	Router rip Version 2 Network <addresse>

Il existe d'autres types de mécanisme pour empêcher un routeur pirate d'envoyer des informations au réseau en mettant en place une ACL qui filtre le host sur le port

UDP du routeur en autorisant la réception de ses paquets multicast et en bloquant tous routeur qui pourraient envoyées des paquets rip.

Configuration d’une ACL :

Access-list 101 permit udp host <addresse> eq 520 any eq 520
Access-list 101 deny udp any eq 520 any eq 520
Acess-list 101 permit ip any any
Ip acces-group 101 in

On peut aussi protéger la diffusion de route en contrôlant la liste des routes diffusées en entrée et en sortie.
Cette méthode n’est applicable que seulement si on connait toutes les routes , du coup sa met en question l’évolutivité du réseau.

Exemple :

Router rip
Version 2
Network <address>
Network <address>
Distribute-list sousreseau in
No auto-summary
Ip acces-list standard sousreseau permit 1.1.1.0 0.0.0.255

La passive interface

C’est d’activé une interface qui ne fait qu’écouter sans envoyer des paquets multicast du protocole rip sur le réseau.
Configuration :
Router rip
Version 2
Network 10.1.1.0
Passive-interface <type-interface> <numéro-interface>

Ospf

OSPF est un protocole à état de lien . le protocole utilise le concept de zones (AREA) . Tous les routeurs dans la même zone ont la même table de topologie réseau.

La zone zéro (0) ou area 0 doit être la première zone crée. Cisco conseille de ne pas dépasser 50 routeurs par zone.

L’ensemble de ces liens forme ce qu’on appelle Link-state database ou topologie table

Les routeurs ospf doivent établir une des relations de voisinage(Neighbors relanship) avant d’échanger les infos de leur table de routage

Le protocole stocke ses informations dans trois(3) tables .

- Table de routage (routing table)
- Table de voisin (neighbor table)
- Table de topologie (topology table)

Les routeurs utilisent les adresses multicast pour les messages ospf. les routeurs envoient de paquets hello toutes les 10 secondes.

Un routeur qui a des interfaces dans plus d’une zone s’appelle **Area Border Router** (ABR).

Un routeur qui connecte un réseau OSPF à d’autres domaines de routage (Internet, par exemple) s’appelle **Autonomous System Border Router** (ASBR).

Le rôle d’un ABR consiste à résumer et annoncer les routes

Configuration et vérification

- **Router(config)#router ospf process ID**

- **Router(config-router)# network <subnet> <wildcard mask> area <area nr>**
-

Sécurité

Comme le protocole ripv2 , ospfv2 a aussi un mécanisme d’Authentication similaire, il existe deux types (clair, md5) et cela ce fait par le biais : du lien et la zone(area).

Comme pour la sécurité de rip, il est possible de filtrer les routes pour s’assurer qu’elles sont valides.

interface	**zone**
Interface <type><number> Ip add <address> <masque>	Network <réseau> <wildcard mask>
Ip ospf message-digest-key <1-255> md5 <mot de passe>	Area <number> authentification message-digest

Aujourd’hui une nouvelle version d’algorithme est développé qui s’appelle le HMAC-SHA (Hash Message Authentification Code Secure Hash Algorithm). Chez Cisco cette version n’est disponible qu’à partir de la version 15.4T de l’Ios Cisco.

# ☻ **mise en place** Conf t Key chain <name> Key <number> Cryptographic-algorithm hmac-sha-512 Key-string <mot_de_passe>	**Interface** Int <type> <number> Ip add <address> <masque> Ip ospf authentification Ip ospf authentication key-chain <name>

Journalisation

Présentation

Les appareils réseaux Cisco (Routeurs, Commutateurs, Pare-feu etc..) génèrent des messages et alertes à travers leur système d’exploitation.

Par exemple, un routeur Cisco peut générer un message Syslog lorsqu'une interface tombe en panne ou que la configuration est modifiée.

Ces messages sont généralement stockés dans le Memory buffer ou log buffer.

Le protocole nous permet de transporter ces messages vers un Syslog Serveur.

Les périphériques Cisco peuvent être configurés pour envoyer les messages Syslog à un Syslog Serveur

Fonctionnement

Le protocole Syslog utilise le port UDP 514.

De ce fait il n y a pas d’accusé de réception pour les messages Syslog envoyés au serveur

Le paquet de Syslog est comporte les informations suivantes :

- **Facility** : source (système d’exploitation, processus ou application)qui a généré le message
- **Severity** : correspond au degré d'urgence du message.
- **Hostname**: le nom d'hôte (tel que configuré sur l'hôte lui-même) ou l'adresse IP.

Timestamp: est l'heure locale de l'appareil lorsque le message a été généré

Message: Il s'agit du texte du message syslog, ainsi que des informations supplémentaires sur le processus qui a généré le message. Les messages syslog générés par les périphériques Cisco IOS commencent par un signe de pourcentage (%) et utilisent le format suivant:

%FACILITY-SEVERITY-MNEMONIC: Message-text

MNEMONIC : C'est un code spécifique à l'appareil qui identifie le message de manière unique.

Message-text : Il s'agit d'une chaîne de texte décrivant le message

Configuration

- Définir un Syslog Serveur
- Router(config)#logging A.B.C.D