Configuration d'un Routeur - Tiers Partie v1.6

La ***qualité de service*** **(QDS)** ou ***quality of service*** (**QoS**) est un concept de gestion qui a pour but d'optimiser les ressources pour véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, gigue, taux de perte de paquets La qualité de service est un concept de gestion qui a pour but d'optimiser les ressources

Ce document fournit des informations utiles et nécessaires à la configuration de règles de QOS d'un routeur non vendu ou fournit par OMNIVIGIL.

SIP

- Le pare-feu ne doit pas bloquer le trafic UDP sur le port 5060 en provenance du réseau de nos serveurs (50.100.21.192/27 et 68.67.53.64/26)

Référence: (RFC3261 +) / https://tools.ietf.org/html/rfc3261

RTP

- Le pare-feu ne doit pas bloquer le trafic UDP sur les ports 10000 à 20000 en provenance du réseau de nos serveurs (50.100.21.192/27 ou 68.67.53.64/26)

Référence: (G711u, G722u, G729) / RFC2833 https://tools.ietf.org/html/rfc2833

T.38

- Le pare-feu ne doit pas bloquer le trafic UDP sur les ports 4000 à 5000 en provenance du réseau de nos serveurs (50.100.21.192/27 ou 68.67.53.64/26)

NTP

- Le pare-feu ne doit pas bloquer le trafic UDP au port 123 en provenance du réseau de nos serveurs (50.100.21.192/27 ou 68.67.53.64/26)

Règles de QDS

Identification de trafic voix Omnivigil

- Tous les paquets UDP avec source ou destination : 50.100.21.192/27 ou 68.67.53.64/26

Identification de trafic administrative Omnivigil

- TCP, Port 80 et 443 (HTTP et HTTPS) dont la source ou la destination est 50.100.21.192/27 ou 68.67.53.64/26
- UDP, Port 123 (NTP) dont la source ou la destination est n'importe quoi
- UDP et TCP, Port 53 (DNS) dont la source ou destination est votre serveur de DNS (assigné par DHCP) et la requête est pour un des domaines suivants :
- *.omnity.biz
- *.omnivigil.com
- *.omnity.net

Aucune reproduction sans l'autorisation d'OMNIVIGIL, une compagnie Cloudli.

Priorisation

Trafic de Voix

Il faut que le réseau du client garantisse 100kbps, avec peu de latence, dans chaque direction par canal de voix.

Exemple, si le client paie pour 5 canaux, il faut réserver 500kbps dans les deux sens.

Trafic administratif

Il n'est pas nécessaire de prioriser le trafic administratif

Autorisation

Il faut laisser passer tout le trafic voix et administrative sur le réseau client.

Serveur DHCP « Dynamic Host Configuration Protocol » (Optionnel)

Définition : Le DHCP « Protocole de configuration dynamique des hôtes) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau.

Sa configuration permet aux appareils téléphoniques de se provisionner automatiquement si non pré-paramétrés par OMNIVIGIL mais aussi après réinitialisation matérielle/aux valeurs d'usine (Factory reset). Sa configuration est optionnelle et peut différer selon certains paramètres.

- Par défaut :
    - Option 66
    - Pour toutes les marques de téléphones supportées par nous
    - À l'adresse http://voip.omnity.biz/public/provision.omni
- Exceptions
    - Yealink
        - Cette option n'est pas nécessaire. Gérer directement par Yealink /OMNIVIGIL
    - Cisco - Routeur Cisco RV042 avec téléphone Cisco uniquement
        - Par TFTP à l'adresse 50.100.21.208
        - **Définition** : TFTP « Trivial File Transfer Protocol » est un protocole simplifié de transfert de fichiers. Il fonctionne en UDP sur le port 69, au contraire du FTPqui utilise lui TCP.

Load balancing / Failover

Il est permis au client de mettre en place de l'équilibrage de charge (load balancing) dont les deux connexions font du NAT avec des adresses IP différentes avec les conditions suivantes

1. Il faut que toutes les données pour le même connexion TCP s'envoient sur le mêmeIP.
2. Il faut que toutes les données pour le même session UDP s'envoient sur le mêmeIP.
1. Le seul temps que ce soit acceptable de rediriger sur le deuxième lien les paquets UDP est dans le cas d'une panne au niveau du premier lien.

Aucune reproduction sans l'autorisation d'OMNIVIGIL, une compagnie Cloudli.

Autres notes

- Les équipements doivent avoir accès à un DNS pour trouver nos serveurs
- Le HTTP/HTTPS doit être permis pour la mise à jour de micrologiciel et de configuration
- Mettre en place des commutateurs (switch) qui supportent le PoE pour alimenter les téléphones (facultatif)
- Le SIP ALG doit être désactivé sur votre routeur dans tous les cas sans exception.
- Autoriser les requêtes ICMP pour la plage réseau 50.100.21.192/27
- Concernant NAT : Il faut que le routeur attribue toujours le même port aux paquets UDP tant que le routeur ne redémarre pas ou qu'il ait une période d'au moins 60 secondes où aucun paquet ne soit envoyé.

Aucune reproduction sans l'autorisation d'OMNIVIGIL, une compagnie Cloudli.