

# MAIL SECURE PINEAPP



**Solution pour la sécurité d'Email, Cryptage d'Email, filtrage Web, Archivage d'Email et la protection transparente contre spam sortant, et à la protection de l'abus IP : PineApp**

## ✓ COMPREHENSION

Le réseau de Solution de Sécurité PineApp fournit des solutions de réseau complètes pour les PME, les entreprises et les fournisseurs de services. Fondée en 2001, Le portefeuille sécurité de PineApp couvre AS / AV Sécurité d'Email, Cryptage d'Email, filtrage Web, Archivage d'Email et la protection transparente contre spam sortant, et à la protection de l'abus IP. Avec des installations dans plus de 50 pays à travers le monde, les Solutions PineApp comprennent



- **Mail SeCure** - Solution de Sécurité pour messagerie électronique :
- Anti-spam
- Anti-virus
- **Cryptage de mail PineAppOutbound**
- **Spam Guard** – outbound spam protection
- **Surf Secure** – Web Surfing Security

Des produits pour l'analyse de messagerie, transfert de courrier électronique et de filtrage entre les réseaux distincts et une inspection approfondie du contenu du trafic SMTP.

PineApp offre une expérience utilisateur intuitive et toutes les solutions PineApp de sécurité sont disponibles sur plusieurs plates-formes, ce qui suppose un appel plus large du marché, évolutivité et prestation des services plus rentable.

Toutes les solutions PineApp sont disponibles comme :

- Appliance
- **Software** – installé sur le hardware local
- **Software** – installé sur une plateforme virtuelle (VMware, Hyper-V, Citrix XEN)

#### ✓ RECOGNITION AND PARTNERSHIP



#### ✓ APERÇU DE LA SOLUTION

Le client est à la recherche d'une solution pour contrôler les problèmes de flux de messagerie qui sont le résultat du trafic de spam et de malware en essayant de pénétrer le réseau du client. L'abus flagrant de l'infrastructure de messagerie du client afin de distribuer des quantités massives de spam et virus, affecte la qualité et l'efficacité du service.

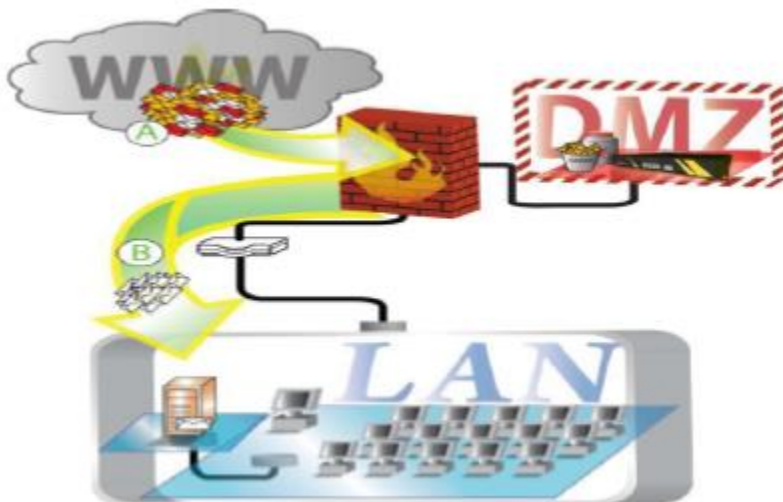
### Le défi

- Réduire le spam entrant sur le réseau du client
- Réduire la bande passante utilisée par SMTP
- Réduire les réclamations des clients pour spam.
- Renforcer la marque et la réputation du client

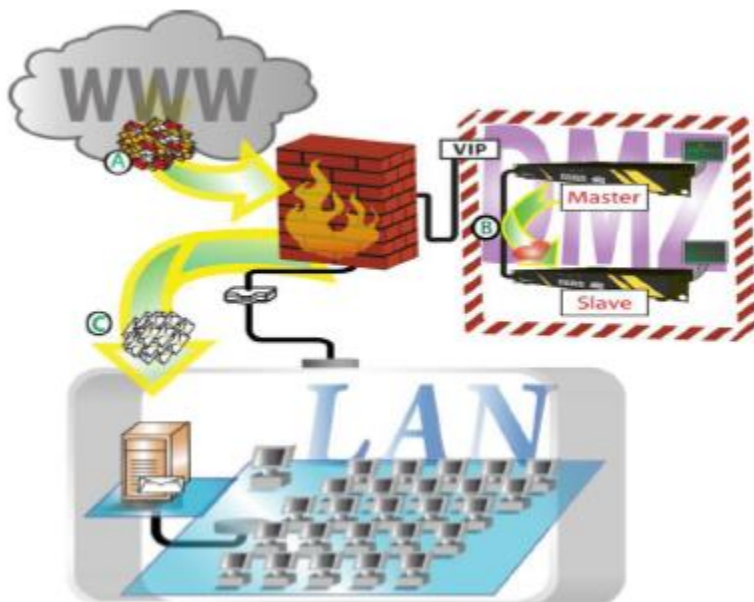
### La solution Pineapp

- Mail Secure une solution reconnue.
- Empêche le spam de pénétrer dans le réseau – limite les plaintes des clients pour spam
- Solution déclinable pour fournisseur de service « Carrier Grade »
- Solution Logiciel déclinable sur multiples plateformes
- Options de déploiement multiple (simple, équilibrage de charge, cluster)

#### ✓ MAIL-SECURE PINEAPP- OPTIONS DE DEPLOIEMENT



1. Toutes les connexions SMTP arrivent de l'Internet vers l'organisation, et sont acheminés par son firewall vers l'appareil Mail SeCure, situé dans la DMZ du réseau \*.
2. Les e-mails sont analysés par l'appareil Mail-SeCure, en vérifiant tout contenu malveillant. Tous les messages propres sont transmis via firewall vers le serveur mail de l'organisation, où les utilisateurs peuvent accéder et récupérer leur courrier personnel.



1. Les connexions SMTP arrivent de l'Internet vers l'organisation, et sont acheminés par son firewall au VIP du réseau Mail-SeCure.
2. L'unité principale, qui détient le VIP et gère toutes les connexions, envoie un paquet multicast ("heart beat") à l'unité secondaire (qui reste en mode d'écoute perpétuel), notifie qu'il est l'unité maître, et qu'il gère actuellement tout le volume du courrier.
3. L'unité principale traite tous les e-mails, et les transmet au serveur de messagerie.

### ✓ DIMENSIONNEMENT DU MAIL-SECURE

Afin de fournir aux fournisseurs de services avec une estimation de dimensionnement de niveau de production approprié, il sera important pour PineApp de recevoir les paramètres de flux de messagerie supplémentaires :

- Nombre d'utilisateurs de messagerie électronique dans l'organisation
- Estimation du nombre de messages électroniques par jour (pour toute l'organisation)
- La taille moyenne des messages estimée (optionnel, KB)
- Nombre de domaines primaires \*
- Combien des primaires \* domaines ont un suffixe international (.net, .com, .org, etc.)
- Nombre de domaines \*\* secondaires
- Combien de \* domaines secondaires ont un suffixe international (.net, .com, .org, etc)

### Les fonctions activées :

- Anti-Spam
- Anti-Virus
- Rétrodiffusion
- Politique
- Contrôle de contenu
- Contrôle de contenu inappropriée de (Porno / détection d'image Nue)
- Synchronisation LDAP

- Rapports du trafic périodiques
- Accès personnels à l'interface graphique de quarantaine
- Cryptage d'email
- Archivage d'email
- Emplacement de l'unité
- Réponse directe aux connexions SMTP
- Derrière un proxy SMTP ou une passerelle supplémentaire
- Type de communication
- Accès direct HTTP (pas de proxy)
- Derrière proxy http
- Méthode de livraison du mail
- Transfert Régulier de SMTP
- Besoins spéciaux de plateformes redondantes
- Haute disponibilité
- Evolution à envisager
- Quarantaine sanitaire centralisée & gestion des logs

