

## Quarantaine TippingPoint

### FICHE TECHNIQUE

Indépendant des postes clients

- Protection de tous les systèmes d'exploitation (Windows, Linux, Mac)
- Protection contre les équipements dotés de systèmes d'exploitation embarqués (imprimantes, fax/photocopieurs, équipements sans fil, téléphones IP)

Automatisé

- Evite le tri en urgence des correctifs de failles
- Diffuse automatiquement les mises à jours du service Digital Vaccine® de TippingPoint dès l'annonce de nouvelles failles
- Bloque automatiquement les attaques en plaçant en quarantaine l'hôte infecté

Complet

- S'intègre au système d'administration SMS de TippingPoint, pour l'application des règles de sécurité jusqu'aux postes clients
- Contrôle le comportement des terminaux pour les protéger des « Exploits » non publiés et des attaques inconnues
- Bloque les attaques et empêche les paquets nuisibles de pénétrer sur le réseau
- Protège le système d'information plus complètement que via une simple validation du pare-feu personnel, des patches OS et des configurations Anti-Virus
- Empêche les spyware, adware, virus et vers de s'installer ou de communiquer
- Bloque les activités des utilisateurs malintentionnés et limite automatiquement leurs accès

Indépendant de l'infrastructure

- Préviend l'infection d'autres segments du LAN, ou d'autres portions du segment
- Fonctionne avec toutes les marques d'équipements réseaux
- N'exige pas de modification de l'infrastructure

Flexible

- Nombreuses options de correction possibles après détection du poste infecté : envoi de pages d'information avec procédure à suivre, redirection vers une page web, affectation à un VLAN de quarantaine ou déconnexion automatique du réseau selon le degré de gravité ou le type d'utilisateur
- Peut être configuré pour permettre les exceptions et autoriser les accès d'urgence
- N'exige pas des utilisateurs invités qu'ils se conforment à un profil type de sécurité
- N'interfère pas avec les moteurs anti-virus ni avec les logiciels clients Microsoft

Exploiter les solutions de protection des intrusions (IPS) pour isoler les postes utilisateurs infectés.

Les risques les plus sérieux pour la sécurité proviennent souvent de l'intérieur du LAN de l'entreprise. Bien souvent, la seule défense efficace consiste alors à appliquer rigoureusement les règles de sécurité sur l'ensemble du réseau. Ces risques internes ne sont pas nécessairement le fait d'employés mécontents. Les vers, qui infectent les portables des itinérants, les PC des invités et des visiteurs, mais aussi les applications non approuvées telles que le partage de fichiers en P2P, souvent accompagné par des spyware, ne sont que quelques exemples des méthodes employées par les codes nuisibles pour contourner le périmètre protégé du réseau.

Les systèmes de prévention des intrusions (IPS) TippingPoint intègrent des fonctions originales pour éviter la propagation des attaques à partir de l'intérieur du réseau et mettre en quarantaine les équipements infectés. La mise en quarantaine empêchera l'équipement infecté de nuire aux systèmes voisins et assurera la réorientation instantanée vers des pages web ou adresses URL proposant des correctifs.

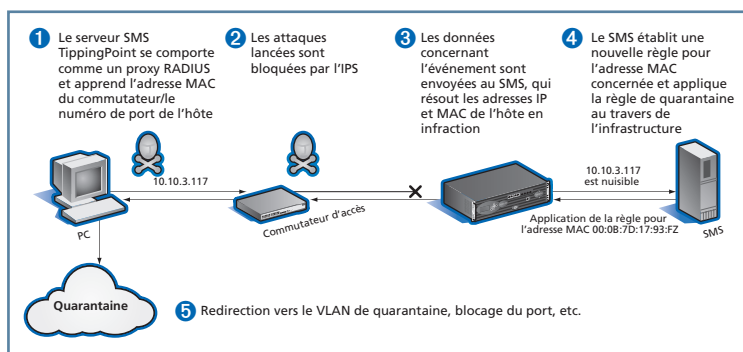
Au départ, la sécurité des postes clients se doit, bien entendu, d'inclure un logiciel anti-virus et des mises à jour du système d'exploitation. La protection TippingPoint par quarantaine complète et dépasse la simple vérification des mises à jour du système d'exploitation et des signatures de l'anti-virus, en contrôlant le comportement des terminaux connectés au LAN. Par la mise en quarantaine, l'administrateur étend virtuellement les filtres sophistiqués de l'IPS TippingPoint aux postes de travail, tout en conservant un contrôle total, à partir d'un point central situé à l'intérieur du périmètre du réseau.

La quarantaine dans les environnements réseaux complexes

Avec la mise en quarantaine, TippingPoint étend les fonctionnalités de ses systèmes de prévention des intrusions, créant ainsi un réseau convergent sécurisé capable d'appliquer les règles de sécurité automatiquement et sans intervention de l'utilisateur, et ce, quelle que soit l'infrastructure réseau existante. L'administrateur pourra ainsi bloquer automatiquement les trafics nuisibles, prévenir l'utilisateur qu'un équipement est infecté et mettre cet équipement en quarantaine pour correction.

La solution TippingPoint permet aussi à l'administrateur de sélectionner ses filtres et de définir les seuils à partir desquels la quarantaine sera déclenchée. Lorsqu'un système IPS repèrera un problème, il empêchera le trafic nuisible de se propager sur le réseau et communiquera avec l'infrastructure du LAN pour identifier l'équipement fautif.

De plus, la solution de quarantaine TippingPoint est basée sur le réseau : elle ne requiert aucune installation d'agent ou de logiciel sur les PC clients. Cette approche simplifie notablement l'administration des postes de travail et les coûts qu'elle engendre ; elle assure une protection totale contre les attaques pouvant provenir d'autres équipements rattachés au réseau, imprimantes, téléphones IP, assistants numériques personnels, qui accroissent considérablement le risque d'exposition. De plus, la solution de quarantaine TippingPoint facilite l'application de règles flexibles pour les systèmes critiques, les invités et les personnels clés.



La sécurisation approfondie permise par les systèmes TippingPoint couvre à la fois l'intérieur et l'extérieur du réseau. TippingPoint permet ainsi à l'entreprise une grande souplesse d'accès au réseau pour ses employés itinérants, ses partenaires ou d'autres utilisateurs autorisés, sans exposer le système d'information.