BLUE COAT | Réseau + Sécurité + Cloud

Guide en 5 étapes de mise en œuvre de la gestion du trafic chiffré (ETM)

Découvrez tout ce qui menace la sécurité de votre réseau.

1. Agissez maintenant. Il n'y a pas de temps à perdre.

Pour la majorité des RSSI d'entreprise, il n'est plus possible de remettre en doute la nécessité de prendre des mesures contre les menaces avancées qui se cachent dans un trafic chiffré.

Les dernières statistiques

- Le chiffrement SSL/TLS représente **35 à 50 %** de tout le trafic réseau des entreprises
- Le trafic chiffré augmente de **20 %** par an
- Plus de **50 %** des attaques se dissimuleront dans le trafic chiffré en 2017
- Les serveurs de commandes et contrôle (C&C) ont vu les instances de logiciels malveillants être multipliées par **200** l'année dernière

Le problème du trafic SSL/TLS empire

Les angles morts de la sécurité réseau ont augmenté en raison du nombre croissant d'applications de Cloud, mobiles et Web

Alors que

Le nombre de logiciels malveillants basés sur les familles SSL Blacklist2 a fortement augmenté – en particulier pendant les périodes de vacances

Le nombre de logiciels malveillants qui utilisent le protocole SSL augmente rapidement

Jan. 2014 – Oct. 2015: **+ de 500**

Oct. 2015 – Jan. 2016: **+ de 29 000**

Augmentation de 58 % du nombre de logiciels malveillants basés sur le protocole SSL !

Le nombre de logiciels malveillants basés sur les protocoles SSL/TLS dans les serveurs de C&C connus augmente rapidement

T3 2014: **+ de 1 000**

T3 2015: **+ de 200 000**

Augmentation de 200 % sur les serveurs C&C basés sur le protocole SSL !

Défendez votre entreprise et réduisez le risque avec une solution ETM qui :

A à la fois un impact élevé et un fort retour sur investissement

S'inscrit dans une stratégie plus étendue au sein des parties prenantes afin d'améliorer l'efficacité des autres systèmes de sécurité

Peut être mise en place dans un délai relativement court

2. Faire l'inventaire. Évaluer vos outils de sécurité réseau et les risques potentiels.

Vos technologies existantes de sécurité réseau, comme NGFW, IDS/IPS, DLP et l'analyse/sandboxing de logiciels malveillants, peuvent-elles reconnaître, inspecter et prévenir suffisamment les menaces, même si celles-ci sont chiffrées ?

NON

***L'inaction* peut engendrer des failles de sécurité, une non conformité avec** les accords de niveau de service (SLA) ou les règlementations sur la confidentialité et conduire à des litiges dus à la responsabilité.

Pourrait être très onéreux— le coût moyen d'une faille de sécurité est de 3,8M $

OUI

Comprendre l'impact sur les performances et la productivité quand l'inspection SSL/TLS est activée ; certains appareils peuvent provoquer des dégradations importantes des performances

Si inefficace ou limité, peut perturber les activités, les services informatiques et avoir un impact sur les employés, les clients et les partenaires

Pourrait violer les politique de confidentialité des données s'il n'y a pas de déchiffrement sélectif

3. Aller au-delà de l'informatique. Collaborer avec les services juridiques, de la conformité ou des RH pour garantir la confidentialité des données.

Collaborer avec les services juridiques, de la conformité ou des RH pour définir et communiquer des politiques sur la confidentialité des données et la conformité réglementaire, puis :

- Identifier tous les lieux où se trouvent les employés et les sous-traitants
- Conseiller sur les politiques officielles concernant le contrôle et la gestion du trafic chiffré
- Surveiller, affiner et mettre en œuvre des politiques pour les applications et le trafic chiffrés qui entrent sur le réseau et en sortent
- Garantir la conformité avec les règlementations d'entreprise et gouvernementales

Etablir des politiques d'entreprise et des ensembles de règles pratiques sur vos appareils de sécurité pour garantir l'inspection et le déchiffrement du trafic SSL/TLS de manière sélective, en particulier :

- Déchiffrement ou blocage du trafic malveillant et des réseaux malveillants suspects, inconnus et connus
- Ne pas déchiffrer ou inspecter le trafic sélectionné pour soutenir la conformité de la confidentialité des données (par exemple, ne pas déchiffrer le trafic relatif aux sites bancaires personnels)
- Identifier ou bloquer les suites de chiffrement cryptographiques obsolètes ou faibles (par exemple, SSL v3.0, RC4 et SHA1)

4. Comprendre l'impact. Affiner et faire évoluer votre équipe de sécurité informatique.

La mise en œuvre d'une solution ETM efficace requiert de :

1. Suivre une approche holistique architecturale et PAS une conception produit par produit complexe
2. Envisager des solutions basées sur des produits vectoriels pour l'infrastructure de sécurité réseau
3. Comprendre les nouvelles technologies comme la gestion des certificats et des clés
   - Des solutions partenaires existent pour vous simplifier la vie (comme par exemple, Gemalto SafeNet Hardware Security Module (HSM) et Venafi Trust Protection Platform™)
4. Proposer une nouvelle formation aux employés du service informatique
5. Créer des rôles et responsabilités nouvelles ou les développer pour les administrateurs de la sécurité informatique
6. S'assurer que les parties prenantes du service informatique ou hors service sont en accord sur des politiques d'utilisation acceptables et sur les modifications organisationnelles ou opérationnelles qui doivent être effectuées

5. Planifier et se développer. Se concentrer sur l'avenir.

Lorsque vous définissez votre stratégie ETM et mettez en œuvre une solution efficace, tenez compte de plusieurs facteurs.

Pour garantir la continuité du service :

Une mise en œuvre graduelle est recommandée pour maintenir la productivité

Déployez la SSL Visibility Appliance dans un sous-ensemble de votre réseau, puis planifiez un déploiement graduel

---

Réfléchir à la mise en œuvre de quelques politiques clés, et ensuite développer.

- Établir des politiques d'utilisation acceptables basées sur une priorité principale ou deux
  - (par exemple, Identifier et arrêter tout le trafic SSL v3.0 ; Inspecter et décrypter le trafic sans certificats signés/adaptés)
- Exploiter ces politiques basées sur l'expérience de l'utilisateur et le feedback
  - (par exemple, Autoriser le trafic chiffré basé sur les sites bancaires personnels et les sites de santé)

L'évolutivité et l'interopérabilité sont des facteurs essentiels. Prévoyez :

- La possibilité d'une importante croissance du trafic SSL/TSL
  - (c'est-à-dire : Prévoyez-vous d'ajouter d'autres applications Cloud cette année ?)
- La façon dont vous pourrez vous segmenter et évoluer pour améliorer l'infrastructure de sécurité existante
  - (c'est-à-dire : Prévoyez-vous de fournir à vos solutions NGFW, IPS et anti-malware/ sanboxing du trafic déchiffré ? Et qu'en est-il des solutions DLP et d'analyse de sécurité ?)

Blue Coat fournit les meilleures solutions de gestion du trafic chiffré qui :

- Éliminent l' « angle mort » de sécurité généré par le trafic SSL/TSL
- Garantissent le meilleur niveau de chiffrement en conformité avec les dernières normes de l'industrie
- Améliorent le retour sur investissement (ROI) de votre infrastructure de sécurité réseau
- Garantissent la confidentialité et la conformité de vos données tout en fournissant une sécurité élevée

BLUE COAT | Réseau + Sécurité + Cloud

Pour en savoir plus sur les fonctionnalités de base et les bénéfices des solutions ETM Blue Coat : www.bluecoat.com/uncoverssl

1. Gartner, Security Leaders Must Address Threats from Rising SSL Traffic, Jeremy D'Hoinne et Adam Hills, 9 décembre 2013.
2. La liste noire SSL est disponible à l'adresse : https://sslbl.abuse.ch
3. 2005 Cost of Data Breach Study réalisée par Ponemon Institute