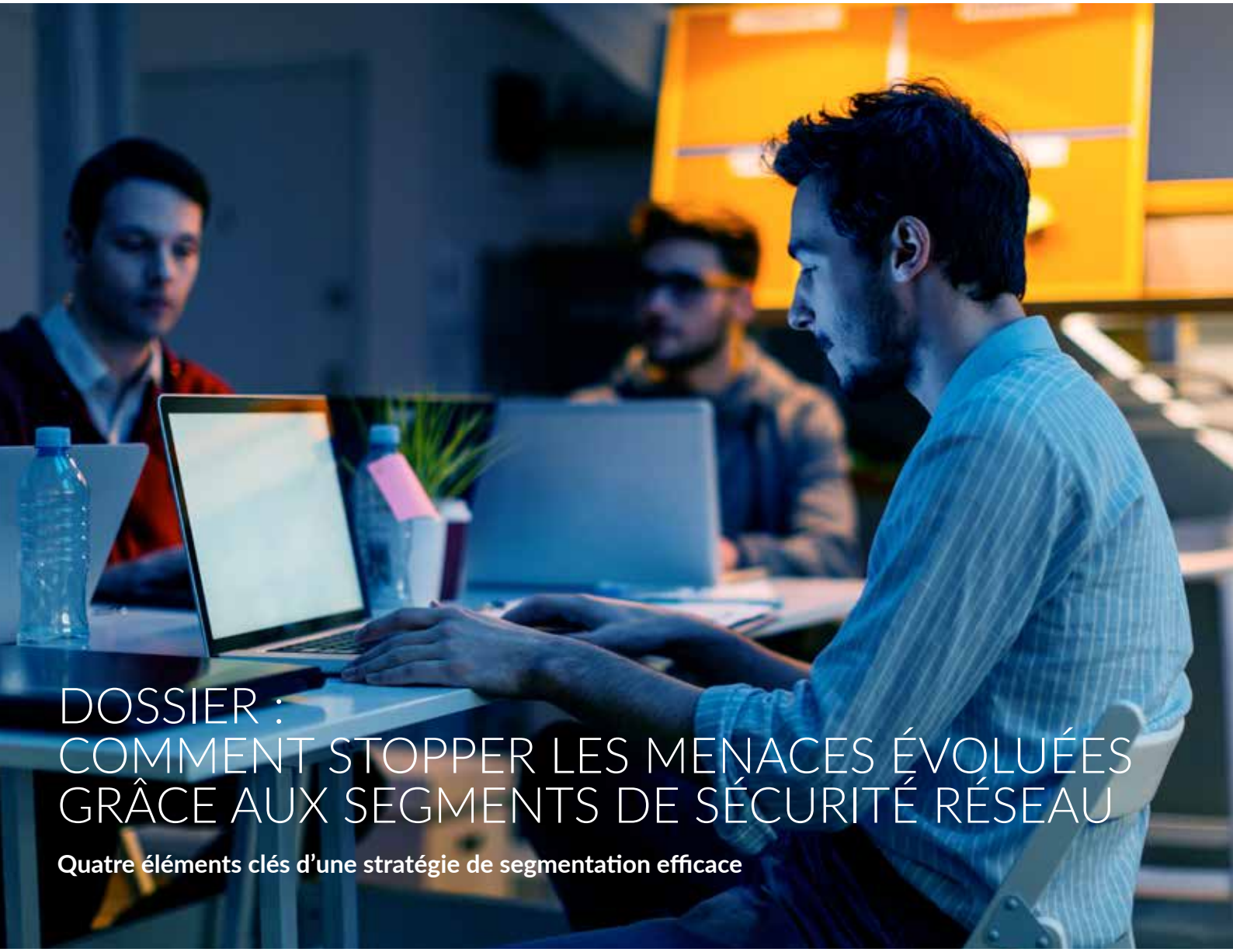
SONICWALL



DOSSIER : COMMENT STOPPER LES MENACES ÉVOLUÉES GRÂCE AUX SEGMENTS DE SÉCURITÉ RÉSEAU

Quatre éléments clés d'une stratégie de segmentation efficace

Résumé

Les segments de sécurité réseau sont primordiaux pour stopper les menaces évoluées, qui exploitent plusieurs zones du réseau pour se propager. Mais définir des segments logiques ne constitue qu'une partie de la solution. Pour être efficace, la segmentation nécessite une approche intégrée et dynamique de la sécurité réseau, qui garantisse l'intégrité de chaque segment, de manière simple et abordable. Ce document passe en revue les meilleures pratiques en termes de fonctionnalités dont doit disposer votre pare-feu de segmentation, et de mise en œuvre des segments afin de garantir une sécurité optimale.

Introduction

Comme nous l'expliquons dans notre présentation intitulée « Why you need network security segments to stop advanced threats » (Pourquoi segmenter la sécurité réseau pour bloquer les menaces évoluées), les menaces évoluées persistantes (APT) profitent de toutes les zones de votre réseau pour s'infiltrer par le biais de différents vecteurs. La mise en place de segments de sécurité crée des barrières propres à empêcher ces menaces de se propager librement à travers le réseau et en limite ainsi la portée et les effets. La sécurité réseau basée sur des segments est un moyen efficace et flexible de gérer des segments de réseau internes et externes, permettant à l'administrateur de séparer et de protéger les ressources internes vitales contre tout accès non autorisé ou toute attaque sophistiquée.

En soi, un segment est un regroupement logique d'une ou plusieurs interfaces conçu pour faire de la gestion – par exemple la définition et l'application de règles d'accès – un processus plus simple et plus intuitif que s'il fallait suivre un schéma d'interface physique strict. Un segment est une méthode de regroupement logique d'une ou plusieurs interfaces sous des noms simples, définis par les utilisateurs. Elle permet d'appliquer des règles de sécurité au trafic circulant d'un segment à un autre. Les segments de réseau offrent au pare-feu une couche supplémentaire de sécurité, plus flexible. L'administrateur peut ainsi regrouper des interfaces similaires et leur appliquer les mêmes règles au lieu d'avoir à écrire ces règles pour chaque interface.

Si l'efficacité de la segmentation ne dépend pas d'un type particulier de pare-feu, celui-ci devra toutefois posséder un ensemble performant de fonctionnalités de segmentation et de sécurité. Afin d'assurer une efficacité optimale face aux APT, la segmentation de la sécurité réseau doit installer toute une série de barrières intégrées, dynamiques et automatiques. Mais elle doit aussi répondre aux exigences en matière de performances, de confort de gestion et de prix. Le présent document décrit quatre éléments clés pour réussir votre segmentation de la sécurité réseau.

1. Une architecture de segmentation flexible et évolutive

En appliquant des règles de sécurité à l'intérieur du réseau, la segmentation permet d'organiser les ressources selon différents segments et d'autoriser ou de restreindre le trafic entre ces segments. C'est un moyen de contrôler rigoureusement l'accès aux ressources internes vitales, telles que les serveurs abritant les données salariales ou des codes d'ingénierie.

De manière générale, les segments se font selon les catégories suivantes :

- DMZ : pour les serveurs publiquement accessibles
- LAN : peut se composer de plusieurs interfaces, chacune présentant différents sous-réseaux, mais gérées comme une entité
- WAN : peut également se composer de plusieurs interfaces ; en cas d'utilisation de la fonctionnalité de basculement WAN de l'appliance de sécurité, une deuxième interface Internet peut être ajoutée au segment WAN.
- Gestion : pour la gestion des appliances
- Multicast : prend en charge le multicasting IP
- VPN : pour les connexions sécurisées à distance
- WLAN : pour l'accès sans fil et les services invités

L'efficacité d'un pare-feu de segmentation dépend aussi de sa capacité à appliquer automatiquement des restrictions de segmentation en fonction de critères dynamiques, comme par exemple les informations d'identité des utilisateurs, la localisation GeoIP ou encore le statut de sécurité des terminaux mobiles. Pour encore plus de sécurité, le pare-feu de segmentation doit être en mesure d'intégrer la commutation réseau multi-gigabit à ses règles de sécurité des segments.[1] Il doit pouvoir soumettre le trafic à ces règles au niveau des points de commutation du réseau et, globalement, gérer l'application de la sécurité par segment depuis un seul et même endroit.

2. Application exhaustive des règles de segments

L'efficacité des segments se mesure à la sécurité qui peut être assurée entre eux. Par exemple, le pare-feu de segmentation doit être capable d'appliquer un service de prévention des intrusions (IPS) qui analyse le trafic entrant et sortant sur le segment WLAN afin d'améliorer la sécurité du trafic réseau en interne.

Pour chaque segment, vous devez pouvoir mettre en œuvre un ensemble complet de services de sécurité sur plusieurs interfaces par le biais de règles rigoureuses. Outre l'IPS, il s'agit des services de sécurité suivants (liste non exhaustive) :

- Filtrage de contenu
- Antivirus et antivirus client (Enforced Client Anti-Virus)
- Anti-spyware
- Surveillance et contrôle des applications
- Déchiffrement et inspection TLS/SSL

Pour une protection optimale contre les APT, le pare-feu de segmentation doit pouvoir appliquer des techniques de surveillance et de correction en mode sandbox dans le cloud. Il doit également avoir la possibilité d'activer les services invités sans fil pour le trafic transitant par les segments WLAN, ou veiller à ce que la connexion se fasse par HTTPS.

Pour appliquer les règles de sécurité par segment, chaque segment correspondrait à un type ou une catégorie de sécurité spécifique. Par exemple :

- Fiable : un type de sécurité Fiable correspondrait au plus haut niveau de confiance. Autrement dit, le trafic venant de segments fiables serait soumis au plus bas niveau de contrôle. La sécurité fiable peut être envisagée du côté protégé de l'appliance de sécurité. Par exemple, le segment LAN désigné peut être considéré comme fiable.
- Non fiable : le type de sécurité Non fiable représente le niveau le plus bas de confiance. Il est utilisé pour les segments WAN et multicast. Habituellement, un segment de sécurité non fiable peut être envisagé du côté WAN (non protégé) de l'appliance de sécurité. Par défaut, le trafic provenant de segments non fiables ne serait pas autorisé à entrer dans tout autre type de segment sans des règles explicites.

Check-list d'un pare-feu de segmentation :

1. Architecture de segmentation flexible et évolutive
2. Application exhaustive des règles de segments
3. Performances à vitesse de ligne à travers les segments
4. Simplicité de déploiement et de gestion

[1] *Par exemple, les commutateurs Dell Networking série X sont pris en charge par les pare-feux SonicWALL TZ600, TZ500/W, TZ400/W et TZ300/W.*

En revanche, le trafic de tout autre type de segment peut pénétrer sur des segments non fiables.

- Public : un type de sécurité Public offre un niveau de confiance plus élevé qu'un segment non fiable, mais moins élevé qu'un segment fiable. Les segments publics peuvent correspondre à une zone sécurisée entre le côté LAN (protégé) et le côté WAN (non protégé) de l'appliance de sécurité. La DMZ, par exemple, serait un segment public dans la mesure où le trafic qui en sort circule tant vers le LAN que le WAN. Tout trafic circulant d'une DMZ vers le LAN devrait être refusé par défaut. Le trafic entre la DMZ et le LAN ne devrait provenir que de connexions initiées dans le LAN. La DMZ n'aurait qu'un accès par défaut au WAN, pas au LAN.
- Gestion : le type de sécurité Gestion serait réservé au segment et à l'interface de gestion et présenterait également le niveau le plus élevé de confiance.
- Chiffré : un type de sécurité Chiffré servirait aux segments VPN et VPN SSL. Tout le trafic de et vers un segment Chiffré devrait être chiffré.
- Sans fil : un type de sécurité Sans fil pourrait être appliqué au segment WLAN ou à tout segment où la seule interface au réseau est constituée de points d'accès sans fil de confiance. Le type de sécurité Sans fil fonctionne particulièrement bien dans les situations où le pare-feu sait détecter et configurer automatiquement le point d'accès fiable. Seul le trafic passant par un tel point d'accès sans fil serait autorisé à traverser un segment Sans fil. Tout autre trafic serait refoulé.

3. Performances à vitesse de ligne à travers les segments

Le pare-feu de segmentation doit pouvoir traiter le trafic interne et « est-ouest » sans ralentir les performances réseau.

Les réseaux d'entreprises distribuées et les environnements de centres de données peuvent être particulièrement sensibles aux fonctionnalités de sécurité qui restreignent le trafic, ce qui à son tour se répercute sur la productivité et les niveaux de service. Dans de tels environnements, il est primordial que le pare-feu de segmentation soit conçu pour opérer le filtrage applicatif (DPI) du trafic inter-segment à des débits multi-gigabits.

Il existe des évaluations des performances de pare-feux effectuées par des analystes indépendants tels que NSS Labs.

4. Simplicité de déploiement et de gestion

Les exigences commerciales et opérationnelles requièrent une solution

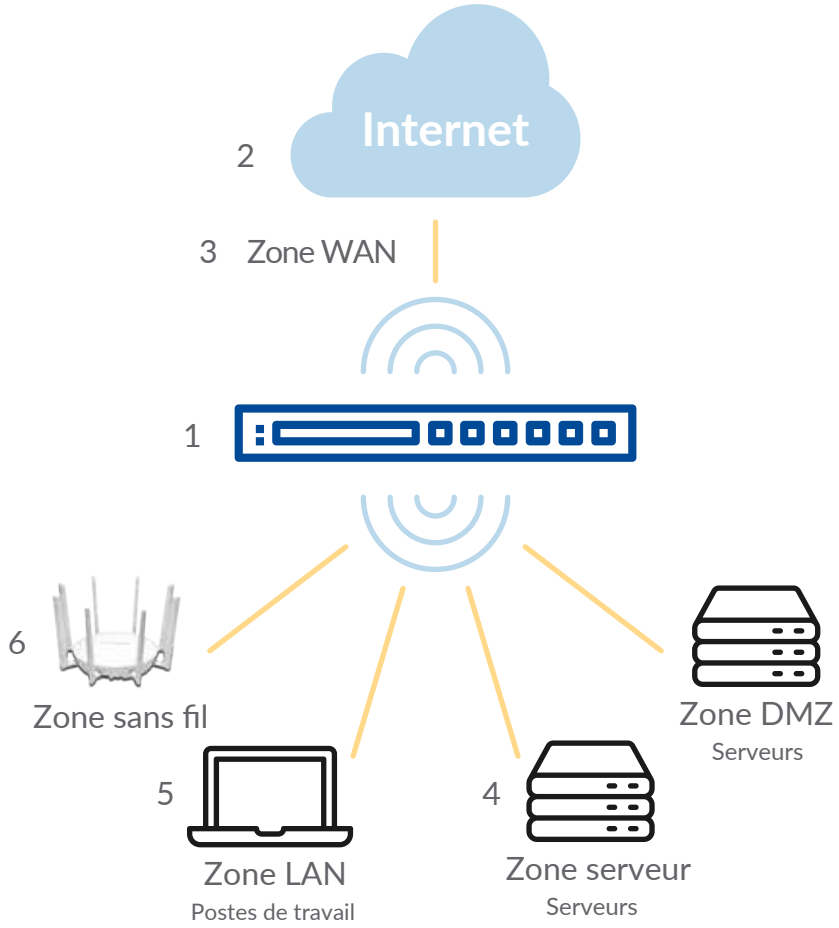


Figure 1 : modèle de sécurité réseau basée sur la segmentation

1. En raison de la grande densité d'interfaces réseau et de la topologie segmentée, le pare-feu devrait pouvoir créer plusieurs zones de réseau au sein d'une seule appliance de sécurité.
2. Une grande partie des sites Internet et services les plus courants étant désormais chiffrés (HTTPS), le pare-feu de segmentation devrait pouvoir soumettre le trafic SSL au filtrage applicatif (DPI SSL).
3. Chaque segment devrait pouvoir être isolé physiquement et/ou logiquement des autres segments par le pare-feu afin d'être protégé à la fois contre les attaques basées sur le LAN et les attaques sans fil provenant d'appareils mobiles.
4. Chaque segment devrait pouvoir appliquer des règles uniques de configuration de la sécurité, notamment un antivirus au niveau de la passerelle, la détection et la prévention des intrusions, un anti-spyware, un anti-botnet, le filtrage de contenu ainsi que des règles applicatives.
5. Le pare-feu devrait être en mesure d'analyser chaque paquet et d'empêcher tout programme malveillant provenant d'appareils qui utilisent des réseaux non sécurisés de pénétrer dans des segments protégés.
6. La sécurité sans fil peut être encore améliorée par le déploiement de points d'accès sans fil intégrant des règles de segmentation réseau et de sécurité.

de segmentation qui limite la complexité et les charges d'administration, afin de favoriser la croissance et de réduire le coût total de possession (TCO). Pour être efficace en la matière, un pare-feu de segmentation doit être en mesure d'offrir une visibilité approfondie et un contrôle de l'ensemble du trafic, à travers tous les segments, depuis une seule et même console de gestion. Le pare-feu de segmentation doit permettre une application dynamique des règles, simplifier la configuration de terminaux sans fil et mobiles, et se charger automatiquement des mises à jour de la sécurité.

Afin de simplifier le déploiement, limiter les perturbations et améliorer l'évolutivité, le pare-feu de segmentation devrait pouvoir être déployé dans un réseau existant avec une transparence absolue, en mode pont couche 2 (L2) ou en mode transparent. Les segments devraient également être configurés de manière à permettre une divulgation totale de la table de NAT (traduction d'adresses réseau) pour le contrôle du trafic passant par les interfaces, les adresses source et de destination étant contrôlées au passage du trafic d'un segment à un autre. Cela veut dire que le NAT serait appliqué en interne, ou à travers des tunnels VPN. L'efficacité des pare-feux de segmentation dépend aussi de leur capacité à soumettre le trafic VPN aux règles NAT et de segment, les VPN étant logiquement regroupés dans leur propre segment VPN.

Scénario de segmentation de la sécurité réseau

Suivant la flexibilité et l'évolutivité de la solution, le déploiement de segments de réseau pourrait se faire avec un seul pare-feu hautes performances appliquant la sécurité sur tous les segments définis, ou avec plusieurs pare-feux selon les besoins.

> Aucun pare-feu n'est exclusivement un « pare-feu de segmentation ». Mais pour assurer une segmentation efficace de la sécurité réseau, il faut en tout cas se tourner vers une plate-forme de pare-feu robuste et complète.

La figure 1 de la page 3 illustre un modèle de déploiement au sein d'un VLAN. Selon cette approche, le pare-feu inspecte les données transitant entre tous les segments du réseau, y compris le trafic entre ressources internes. Tout le trafic réseau pourrait être dirigé vers le segment approprié à l'aide du marquage VLAN sur les commutateurs et des passerelles de couche 3 sur le pare-feu. Dans ce scénario, un programme malveillant de type APT pourrait certes pénétrer dans un segment, mais il serait analysé, bloqué et des alertes seraient déclenchées dès qu'il tenterait de se propager à d'autres segments.

Conclusion

Aucun pare-feu n'est exclusivement un « pare-feu de segmentation ». Mais pour assurer une segmentation efficace de la sécurité réseau, il faut en tout cas se tourner vers une plate-forme de pare-feu robuste et complète.

Pour combattre les menaces évoluées persistantes, un pare-feu de segmentation doit être en mesure d'attribuer et d'appliquer une vaste gamme de contrôles de sécurité sur la base des profils de sécurité définis au niveau des segments ainsi que d'autres critères dynamiques. Le tout dans le respect des exigences commerciales et opérationnelles. Toutes les solutions de pare-feu ne sont pas en mesure de fournir tous les éléments requis pour stopper les menaces évoluées de nouvelle génération à l'aide de segments de sécurité réseau.

SonicWall peut vous aider à répondre à toutes les exigences de segmentation de la sécurité réseau, avec des solutions complètes et flexibles, conçues pour s'adapter à tous les types de segmentation. Pour en savoir plus sur les solutions de sécurité réseau SonicWall, rendez-vous sur www.sonicwall.com/solutions/security-solutions.

À propos de nous

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

Pour toute question concernant l'usage potentiel de ce document, contactez :

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Pour plus d'informations, consultez notre site Internet.
www.sonicwall.com

SolutionBrief-HowToStopAdvThreats-US-KJ-MKTG2860