Réseaux SDSN : les avantages concrets

Pour une neutralisation automatisée des menaces, sans impact sur la continuité opérationnelle

Problématique

Devant la complexité croissante des menaces qui planent sur leurs réseaux, les entreprises doivent sans cesse s'adapter et évoluer. Or, bien souvent, cette priorité sur la sécurité éclipse d'autres aspects stratégiques. Ainsi, trop d'entreprises se voient contraintes d'arbitrer entre la sécurité de leurs réseaux d'un côté, et leur continuité opérationnelle de l'autre.

Solution

Les entreprises doivent transformer leur réseau traditionnel en un réseau sécurisé. Concrètement, il s'agit de mettre en place un système centralisé de gestion, d'analytique et de règles pour faire entrer en synergie l'ensemble des composants réseau et sécurité d'un écosystème ouvert et multifournisseur.

Avantages

- Détection des menaces plus précise et plus efficace
- Système centralisé de cyberveille et de gestion des politiques de divers écosystèmes
- Multiplication des points de contrôle sur le réseau pour un niveau plus granulaire de mise en quarantaine
- Neutralisation rapide et automatisée des menaces

La révolution technologique à l'œuvre ces dix dernières années a profondément modifié la physionomie des réseaux. Cloud, Internet des objets (IoT), blockchains… ces technologies qui séduisent un nombre croissant d'entreprises font toutes un usage intensif des réseaux.

Dans le même temps, les entreprises ont revu à la hausse leurs investissements dans la protection de leurs infrastructures existantes et nouvelles. En vain, car les cas de violations se multiplient. C'est ainsi que des informations clients et autres données internes se retrouvent sur les marchés noirs, à la merci du plus offrant. Pour les entreprises victimes, l'atteinte à la réputation est souvent irréparable. D'où la question suivante : comment accompagner les entreprises sur la voie d'un réseau vraiment sécurisé ?

La problématique

Aujourd'hui, le marché regorge de solutions et technologies de sécurité hautement efficaces. Citons par exemple les pare-feu de nouvelle génération, les solutions de sandboxing ou de protection des terminaux, les brokers d'accès au cloud sécurisé (CASB) ou encore les systèmes de gestion des informations et événements de sécurité (SIEM). Toutefois, n'oublions pas que la sécurité d'un réseau se mesure d'abord à l'aune de son maillon le plus faible. Sans une parfaite osmose et synchronisation des divers composants, les entreprises entrouvrent des failles de sécurité dans lesquelles les attaquants n'hésiteront pas à s'engouffrer. Pour tous les acteurs concernés, force est de constater que les lourds investissements consentis sur le front de la sécurité n'ont pas livré les résultats escomptés.

Propagation des menaces dans une infrastructure équipée de produits de sécurité traditionnels

Faisons d'abord le point sur l'approche traditionnelle. Nous prendrons le cas d'un réseau type composé de clients, terminaux, commutateurs d'accès et points d'accès sans fil. Le plus souvent, l'entreprise utilise un dispositif anti-malware relié à un pare-feu de périmètre de nouvelle génération qui contrôle le trafic Nord-Sud. Les clients sont quant à eux protégés par un logiciel de protection des terminaux (selon le type et le modèle). Notons que dans les environnements IoT, sur les imprimantes en réseau et sur certains nouveaux types de terminaux, ce type de protection n'est pas disponible.

Déroulement de la compromission d'un réseau

La figure 1 ci-dessous illustre un cas typique de compromission du réseau. En règle générale, ces violations suivent un schéma bien défini :

1. Le client tente de télécharger un malware inconnu.
2. Le fichier est intercepté par le pare feu de périmètre.
3. Le pare-feu envoie le fichier au dispositif anti-malware qui l'analyse et confirme son caractère malveillant.
4. Le pare-feu bloque le téléchargement du fichier.
5. Le problème : si le client est compromis manuellement ou en dehors du réseau de l'entreprise (environnement « hors entreprise »), l'infection se propage à tous les hôtes accessibles sur le réseau (selon le type de menace).

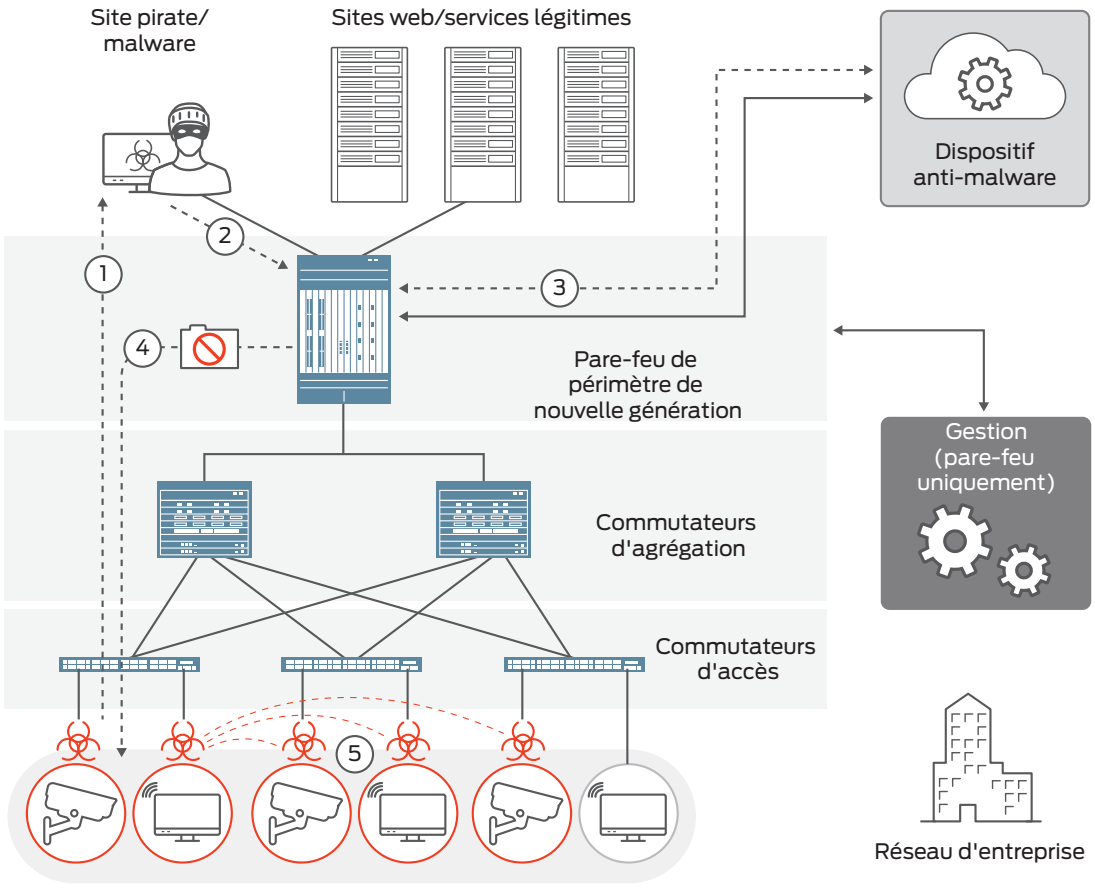

Figure 1 – Réseau compromis dans une infrastructure équipée de produits de sécurité traditionnels

Les failles de l'approche traditionnelle :

a. Le seul blocage des interactions du client avec l'extérieur est une méthode inefficace qui n'empêche pas la propagation latérale des menaces.

b. L'absence de communication et d'interopérabilité entre les solutions de sécurité et les composants réseau se solde par un manque de visibilité et une réduction des points de contrôle.

c. L'incapacité à agréger les rapports d'anomalie de différentes sources de données (journalisation des serveurs, terminaux et autres composants réseau…) donne lieu à des failles de sécurité majeures.

d. Les pare-feu forment la pierre angulaire de l'approche traditionnelle. Or, la complexité des règles qui les régissent peut rapidement déstabiliser les équipes de sécurité – *a fortiori* dans les entreprises établies à l'international.

La solution SDSN de Juniper Networks

Avec le réseau SDN sécurisé (SDSN) de Juniper Networks®, les entreprises atteignent des niveaux de protection sans précédent. Elles bénéficient notamment d'une visibilité de bout en bout sur leur réseau, condition indispensable à la détection et au blocage des menaces dans tous leurs environnements, physiques comme virtuels. À travers une suite complète de produits, notre plateforme SDSN unifiée centralise et automatise votre sécurité en agissant sur les trois leviers que sont les règles de sécurité, la détection et le contrôle.

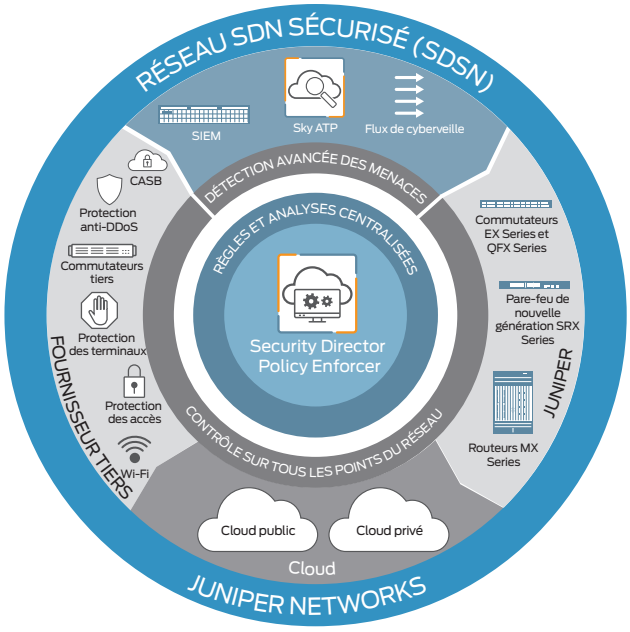

Figure 2 – Éléments clés du SDSN de Juniper Networks

Éléments clés du SDSN

Le SDSN repose sur les composants suivants :

1. Moteur de détection avancée des menaces
   a. Juniper Networks Sky Advanced Threat Prevention (Sky ATP) est une solution cloud de détection des malwares, capable de repérer avec précision les menaces connues et inconnues.
   b. La détection des menaces connues passe par l'agrégation des données de cyberveille de différentes sources (serveurs C&C, géolocalisation des adresses IP (GeoIP), équipements de fournisseurs tiers via des API REST) et des journaux de serveurs internes.
   c. Pour identifier les menaces inconnues, Sky ATP utilise des technologies comme le sandboxing, l'apprentissage automatique et d'autres techniques de leurre.
2. Gestion centralisée des composants, des règles de sécurité et des données d'analyse :
   a. Avec Junos® Space Security Director, Juniper Networks offre aux entreprises une solution de gestion de la sécurité évolutive et hautement réactive pour centraliser et améliorer l'administration des politiques de sécurité.
   b. Le module Policy Enforcer de Security Director centralise les données de cyberveille. Ses missions :
      - Communiquer avec les composants réseau et produits de sécurité des fournisseurs tiers, comme les pare-feu de nouvelle génération, pour fournir des analyses et assurer l'application globale des règles de sécurité
      - Consolider les données de cyberveille issues des systèmes internes sur site
3. Contrôle et application des règles de sécurité sur tous les points du réseau :
   a. Le SDSN fait de chaque composant réseau un point de contrôle de sécurité.
   b. Le SDSN mise sur un écosystème ouvert et multifournisseur pour opérer des contrôles de sécurité sur les solutions Juniper, les écosystèmes non-Juniper et dans le cloud.
   c. Le SDSN permet le blocage et la mise en quarantaine rapides des menaces pour empêcher toute propagation Nord-Sud ou Est-Ouest.

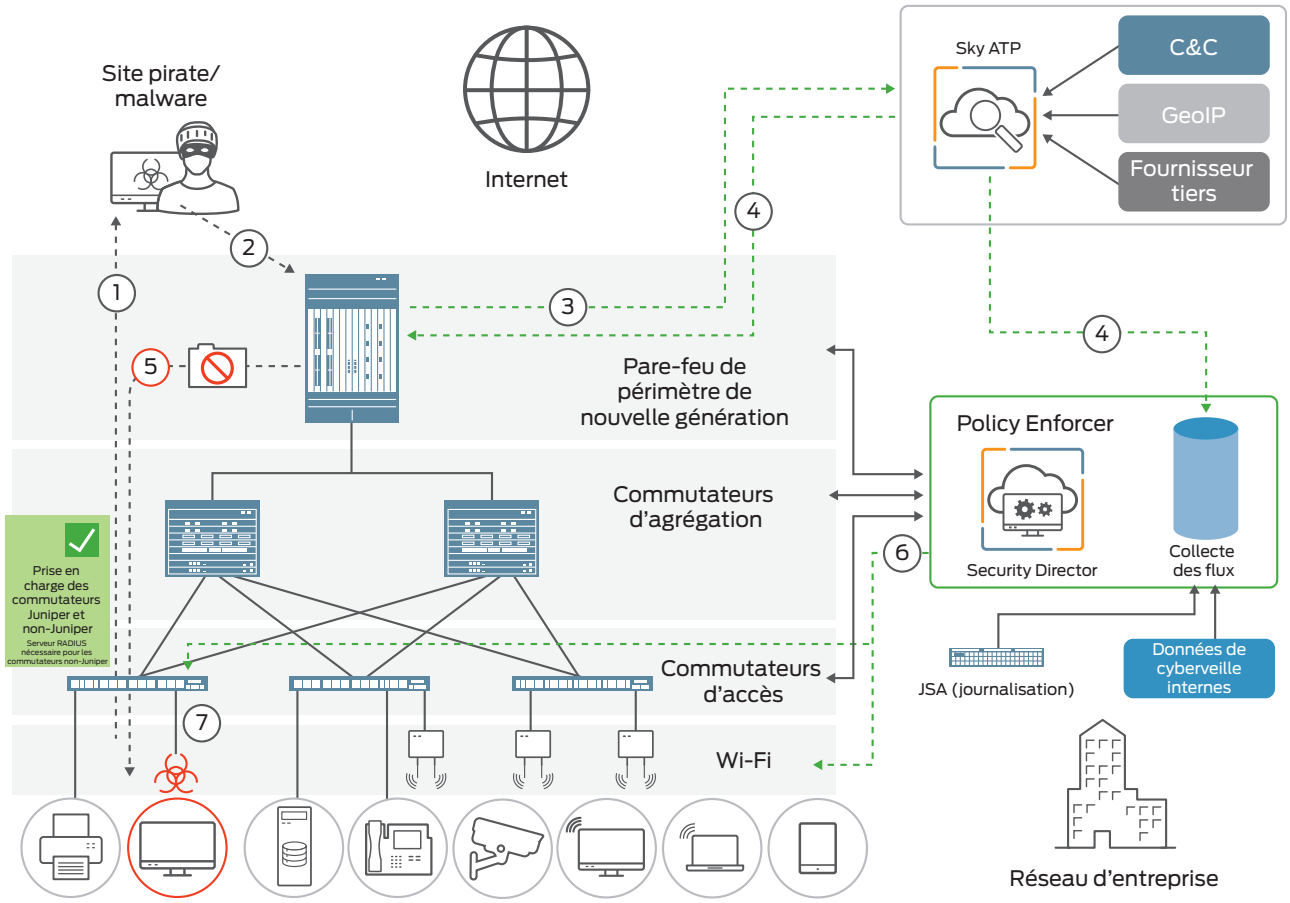

Figure 3 : Déploiement d'un réseau SDSN

Déploiement d'un réseau SDSN

Prenons l'exemple d'un réseau SDSN utilisant les passerelles de services SRX Series de Juniper Networks. Les passerelles sont déployées sous la forme de pare-feu de périmètre et communiquent avec le dispositif anti-malware de Sky ATP. Au cœur de cette configuration, on retrouve le module Security Director Policy Enforcer, qui communique avec l'ensemble des composants réseau (y compris les pare-feu de nouvelle génération) pour orchestrer le contrôle et l'application des règles de sécurité à tous les niveaux.

Policy Enforcer se base pour cela sur le module d'agrégation Feed Collector, dont la mission consiste à collecter les données issues des divers équipements (sur site et dans le cloud), ainsi que les flux de cyberveille internes et des journaux. Les clients/terminaux sont équipés d'un logiciel de protection des terminaux pour une connexion sécurisée aux commutateurs et points d'accès sans fil. Si, par nature, les appareils IoT, imprimantes réseau et nouveaux types de terminaux sortent de ce périmètre de protection, Policy Enforcer communique néanmoins avec les équipements d'accès pour partager de l'information et faire appliquer les règles de sécurité.

Les réseaux SDSN ouvrent une nouvelle ère de la cybersécurité. Voyons maintenant la réaction d'un réseau sécurisé par Juniper face à deux scénarios d'attaque.

Scénario nº 1 – Téléchargement d'un malware

1. Un client tente de télécharger un malware inconnu.
2. Le fichier est intercepté par le pare-feu de périmètre SRX Series.
3. Le pare-feu SRX Series envoie le fichier pour analyse à Sky ATP.
4. Après identification du malware, Sky ATP notifie le pare-feu SRX Series et le module Policy Enforcer.
5. Le pare-feu SRX Series bloque le téléchargement du fichier.
6. Policy Enforcer procède à la mise en quarantaine de l'hôte dans un VLAN dédié (au niveau du commutateur) pour une investigation plus approfondie. Policy Enforcer peut également désactiver le port du commutateur ou le point d'accès Wi-Fi auquel le client est connecté.
7. Les autres hôtes du réseau sont à présent à l'abri de toute infection par le client ciblé. La propagation Est-Ouest et Nord-Sud du malware a été bloquée. Policy Enforcer mémorise l'identité du client. Même si ce dernier passe à un autre commutateur ou point d'accès Wi-Fi, Policy Enforcer reconnaît et bloque la menace.

Scénario nº 2 – Infection d'un appareil IoT

1. Un appareil IoT connecté au réseau est infecté. Il tente alors de télécharger un fichier malveillant ou lance une attaque contre une infrastructure critique.
2. Juniper Security Analytics (JSA) enregistre la tentative de téléchargement et notifie Security Director Policy Enforcer.
3. Policy Enforcer applique une liste/règle de contrôle des accès au port du commutateur/point d'accès Wi-Fi infecté pour mettre l'hôte en quarantaine et neutraliser rapidement la menace.

Sur un réseau non-SDSN, le pare-feu de nouvelle génération ne bloque que les communications entre l'appareil IoT et l'extérieur. Autrement dit, l'appareil infecté conserve l'accès à diverses informations sur le réseau. Les dégâts sont d'autant plus graves lorsque l'attaquant possède un accès physique à l'appareil et lance l'attaque de l'intérieur.

Fonctionnalités et avantages

La plateforme SDSN de Juniper offre les avantages suivants :

- **Sécurité pervasive –** Notre plateforme SDSN étend la sécurité à toutes les couches du réseau, y compris aux commutateurs, routeurs, points d'accès Wi-Fi et pare-feu. Côté déploiement, elle se décline sur de nombreux modèles : sur site, dans des clouds privés (comme VMware NSX et Juniper Contrail) ou dans des clouds publics (comme Amazon AWS et Microsoft Azure). Nos clients ont ainsi toutes les cartes en main pour implémenter une sécurité sans compromis.
- **Écosystème ouvert et multifournisseur –** La majorité des entreprises opèrent dans des environnements composés des solutions de multiples fournisseurs. Dès lors, on peut s'interroger sur la pertinence des solutions qui exigent le remplacement des infrastructures existantes ou enchaînent le client à un fournisseur unique. Bien souvent, une telle approche bride l'adoption des nouvelles tendances en général, et des nouvelles technologies et fonctionnalités en particulier. À l'inverse, la plateforme SDSN de Juniper Networks se veut résolument ouverte. Les entreprises peuvent ainsi migrer vers un réseau sécurisé tout en conservant la majorité de leurs équipements existants. Grâce à des partenariats avec d'autres fournisseurs reconnus, Juniper Networks adopte une approche à la fois complète et hautement collaborative de la sécurité des réseaux.
- **Gestion globale des règles de sécurité –** À travers son module Policy Enforcer, Junos Space Security Director permet d'appliquer des règles de sécurité cohérentes à l'ensemble du réseau, local ou international. Forts d'une visibilité granulaire sur les systèmes, les administrateurs sécurité peuvent intervenir sur la couche réseau comme dans les environnements virtuels, avec à la clé une sécurité optimisée et renforcée.
- **Neutralisation dynamique et automatisée des menaces –** En matière de sécurité des réseaux, la réactivité est le nerf de la guerre. Pour assurer une détection précise et continue des menaces, notre plateforme SDSN libère toutes les synergies de Sky ATP, des capteurs tiers et des flux de cyberveille internes. Au cœur du dispositif, Policy Enforcer bloque et isole les menaces au niveau du réseau, de manière automatisée et quasi immédiate. Au-delà d'une réduction des coûts d'administration, cette approche accélère et simplifie la sécurité du réseau à mesure que ce dernier se développe.

Conclusion

Afin de garantir une sécurité pervasive et une neutralisation réellement automatisée des menaces, le SDSN de Juniper Networks fédère tous les composants réseau et sécurité au sein d'un système de gestion et d'analytique centralisé. Notre plateforme ouverte favorise la création d'un écosystème SDSN multifournisseur dans lequel les entreprises peuvent conserver leurs infrastructures existantes pour pérenniser leurs investissements tout en préservant leur continuité opérationnelle.

Prochaines étapes

Pour en savoir plus sur les solutions de sécurité de Juniper Networks, rendez-vous sur www.juniper.net/us/en/products-services/security. Nos conseillers auront également plaisir à répondre à toutes vos questions.

À propos de Juniper Networks

Juniper Networks défie le statu quo avec des produits, solutions et services qui redéfinissent le modèle économique de votre réseau. En collaboration avec nos clients et partenaires, nous innovons pour déployer des réseaux automatisés, évolutifs et sécurisés, vecteurs d'agilité, de performances et de valeur ajoutée. Pour en savoir plus, rendez vous sur Juniper Networks ou suivez-nous sur Twitter et Facebook.

Siège social et commercial
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089, États-Unis
Téléphone : 888.JUNIPER (888.586.4737)
ou +1 408 7452000
Fax : +1 408 7452100
www.juniper.net

Siège EMEA et APAC
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Pays-Bas
Téléphone : +31 0 207 125 700
Fax : +31 0 207 125 701

3510608-002-FR Juin 2017