Commencer les bonnes pratiques avec le BPA et l'Assurance de sécurité

Version 9.1

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

March 5, 2020

Table of Contents

Getting Started with Best Practices

Les bonnes pratiques en matière de sécurité empêchent les menaces connues et inconnues, réduisent la surface d'attaque et offrent une visibilité sur le trafic pour que vous puissiez ainsi connaître et contrôler les applications, les utilisateurs et le contenu présents sur votre réseau. Lorsque vous mettez en œuvre les bonnes pratiques en matière de sécurité, vous :

- Minimisez les risques d'une intrusion réussie.
- Identifiez la présence de pirates.
- Protégez vos précieuses données.
- Protégez vos clients, partenaires et employés, et donc la réputation de votre entreprise.
- Aidez à réaliser un environnement de sécurité Zero Trust.

Pour passer aux bonnes pratiques en matière de sécurité, vous devez d'abord comprendre votre posture de sécurité réseau actuelle et identifier les domaines d'amélioration. Palo Alto Networks propose une voie de transition guidée : l'évaluation des bonnes pratiques (BPA) associée aux étapes de transition en toute sécurité et à une documentation technique sur les bonnes pratiques.

Lorsque vous souscrivez au contrat de support Premium (à compter du 1er novembre 2019) ou Platinum, vous avez la possibilité de préparer l'Assurance de sécurité. L'Assurance de sécurité donne accès aux experts en sécurité de Palo Alto Networks et à des outils pour aider à l'enquête initiale sur les incidents.

- Identification et hiérarchisation des bonnes pratiques
- Accès et exécution du BPA
- Assurance de sécurité

Identification et hiérarchisation des bonnes pratiques

Le Best Practice Assessment (BPA) de Palo Alto Networks utilise votre fichier de support technique pour analyser les paramètres de configuration de pare-feu nouvelle génération et de Panorama et compare cette configuration aux bonnes pratiques de Palo Alto Networks. Le BPA indique l'état actuel de l'adoption des bonnes pratiques en matière de sécurité et suggère des modifications spécifiques pour aligner la configuration sur les bonnes pratiques en matière de sécurité. L'exécution du BPA vous indique non seulement les domaines dans lesquels vous pouvez améliorer votre posture de sécurité, mais établit également une base de référence pour une comparaison ultérieure et fournit des liens vers une documentation technique vous expliquant comment traduire les recommandations du BPA en une configuration respectant les bonnes pratiques.

En utilisant une approche itérative et hiérarchisée, vous pouvez transformer votre posture de sécurité en un état respectant les bonnes pratiques, étape par étape, en mesurant les progrès à votre rythme et à votre niveau de confort :

STEP 1 | Chargez un fichier de support technique sur le portail de support client et procédez vous-même à Accès et exécution du BPA, ou contactez votre SE de Palo Alto Networks ou votre partenaire pour exécuter le BPA sur Panorama ou vos pare-feu nouvelle génération.

Si vous exécutez vous-même le BPA, nous vous recommandons de contacter votre SE de Palo Alto Networks ou votre partenaire pour interpréter les résultats et discuter des étapes suivantes.

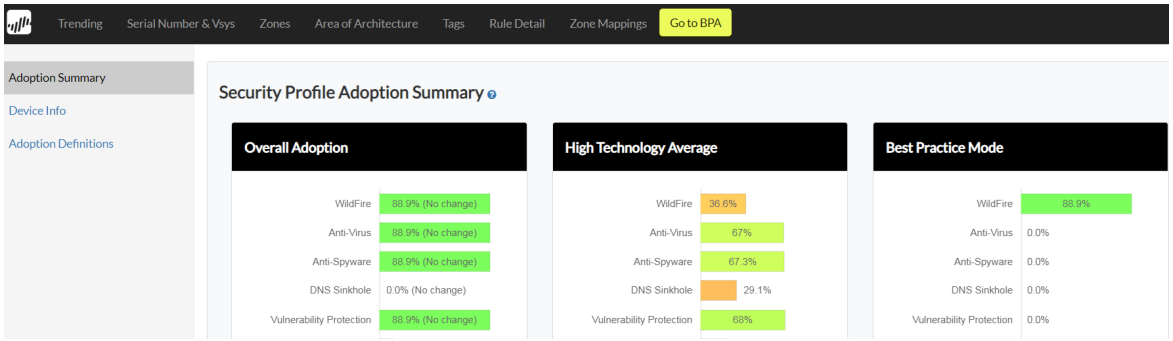
STEP 2 | Identifiez et hiérarchisez le premier domaine d'amélioration pour commencer la transition vers les bonnes pratiques.

Que ce soit votre SE de Palo Alto Networks ou votre partenaire qui exécute le BPA ou que ce soit vous, votre SE ou votre partenaire peut vous aider à élaborer un plan hiérarchisé pour appliquer en toute sécurité les bonnes pratiques. Prévoyez de commencer par les modifications les plus sûres, les plus simples et les plus efficaces, telles que l'application de profils d'analyse WildFire, antivirus, antispyware et protection contre les vulnérabilités à vos règles d'autorisation de politique de sécurité.

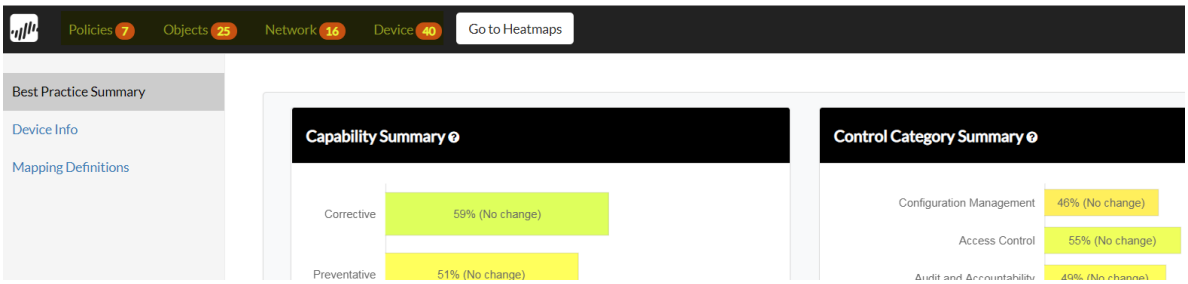
STEP 3 | Utilisez les liens du BPA vers la documentation technique pour configurer les bonnes pratiques que vous hiérarchisez.

Le téléchargement du rapport BPA vous fournit un fichier .zip contenant le rapport HMTL détaillé, le récapitulatif et une feuille de calcul Excel répertoriant les échecs de vérifications des bonnes pratiques. Vous pouvez accéder à la documentation technique de deux manières :

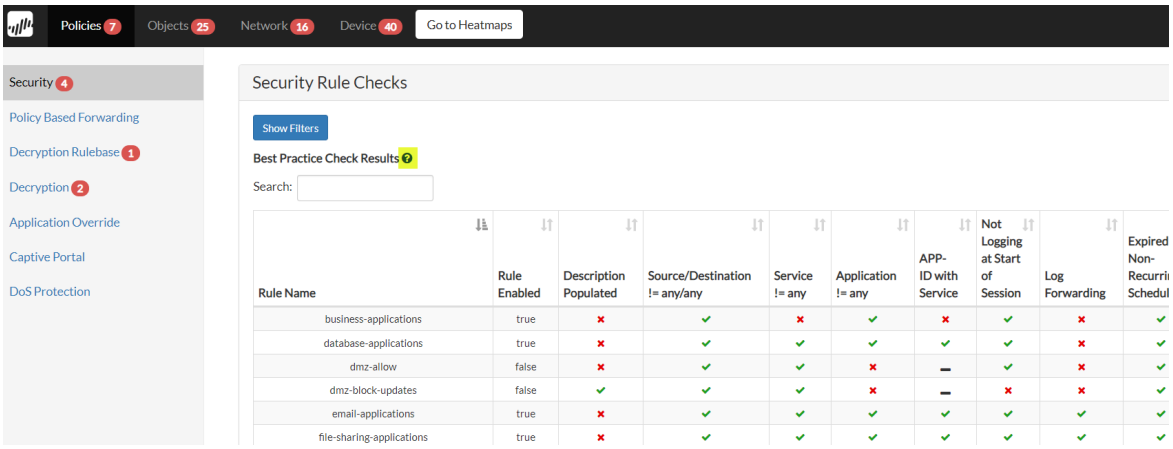
- Depuis la feuille de calcul : l'onglet Documentation fournit des liens pour chaque vérification ayant échoué. De plus, le numéro d'identification dans la colonne Check ID (ID de vérification) des onglets Policies (Polices), Objects (Objets), Network (Réseau) et Device (Équipement) est directement lié à la ligne correspondante de l'onglet Documentation.
- À partir du rapport HTML : lorsque vous ouvrez le rapport HTML, vous voyez une carte thermique résumant l'adoption des bonnes pratiques. Cliquez sur **Go to BPA** (Accéder au BPA) pour accéder au rapport.



Sur la page de résumé du BPA, affichez les rapports détaillés des onglets **Policies** (Politiques), **Objects** (Objets), **Network** (Réseau) ou **Device** (Équipement) pour l'évaluation de la configuration sélectionnée.



À partir d'un rapport détaillé, cliquez sur le **?** bleu entouré pour obtenir des descriptions et des justifications de la vérification de la configuration et des liens vers la documentation technique pour une configuration respectant les bonnes pratiques.



Pour les profils de sécurité (Protection contre les vulnérabilités, Antivirus, Antispyware, Filtrage des URL, Blocage des fichiers), utilisez les conseils de transition en toute sécurité pour garantir la disponibilité des applications essentielles à vos activités lorsque vous passez aux profils de sécurité respectant les bonnes pratiques.

STEP 4 | Une fois que vous avez mis en œuvre le premier ensemble de modifications des bonnes pratiques, exécutez à nouveau BPA pour mesurer les progrès et vérifier que les modifications fonctionnent comme prévu.

Comparez les résultats du premier BPA et du BPA suivant pour voir les améliorations apportées à votre posture de sécurité. Identifiez et hiérarchisez le prochain domaine d'amélioration à traiter.

STEP 5 | Utilisez les liens du BPA vers la documentation technique pour configurer le prochain ensemble de bonnes pratiques que vous avez hiérarchisées.

STEP 6 | À votre rythme, répétez le processus d'exécution du BPA pour mesurer les progrès ainsi qu'identifier et hiérarchiser les prochaines étapes, puis configurez les bonnes pratiques à l'aide de la documentation technique.

STEP 7 | Commencez maintenant ! Procédez à l'Accès et exécution du BPA ou contactez votre SE de Palo Alto Networks ou votre partenaire et commencez dès aujourd'hui la transition vers un réseau plus sécurisé !

Accès et exécution du BPA

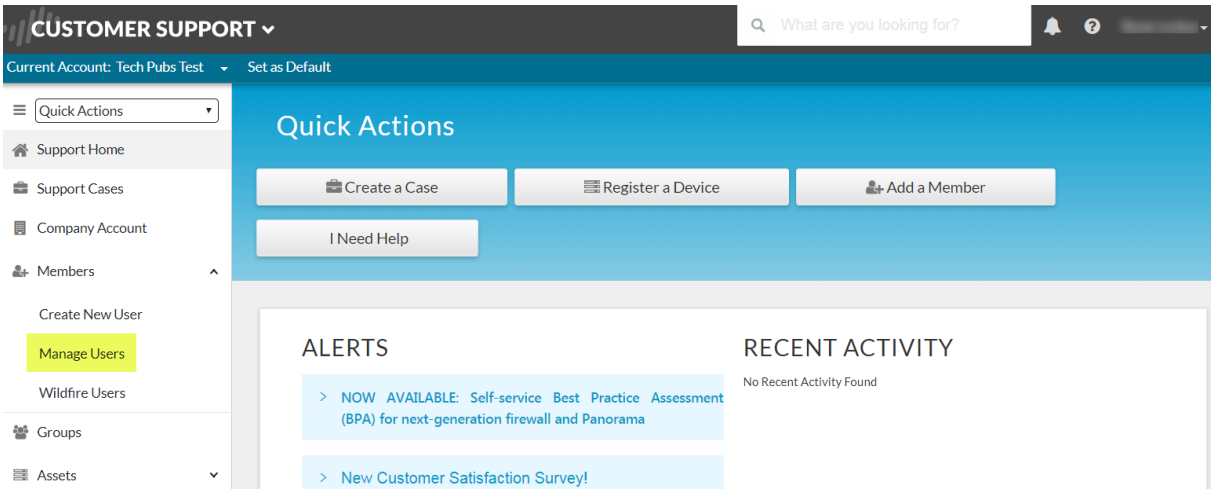
Accédez au Best Practice Assessment (BPA) à partir du Portail Support Client. Les comptes de Super Users (Super-utilisateurs) ont automatiquement accès au BPA et peuvent attribuer le rôle *BPA User* (Utilisateur BPA) à un profil de Standard User (Utilisateur standard) afin que ce dernier puisse exécuter le BPA. Cette procédure montre aux Super Users (Super-utilisateurs) comment donner accès aux Standard Users (Utilisateurs standard) et comment exécuter le BPA. Vous pouvez également visionner de courtes vidéos sur Comment exécuter un BPA et Comment comprendre les résultats.

En outre, si vous souscrivez au contrat de support Premium (à compter du 1er novembre 2019) ou Platinum, vous avez la possibilité de préparer et d'activer Assurance de sécurité. L'Assurance de sécurité donne accès aux experts en sécurité de Palo Alto Networks et à des outils pour aider à l'enquête initiale sur les incidents. Nous vous recommandons vivement d'exécuter le BPA pour mesurer votre adoption des sept fonctionnalités de sécurité clés et vous assurer que votre taux d'adoption est au moins égal au taux d'adoption moyen dans votre secteur d'activité afin que votre réseau soit mieux protégé. L'activation de l'Assurance de sécurité se fait automatiquement grâce à la combinaison du contrat de support Premium ou Platinum et à une mesure récente du BPA qui montre que votre taux d'adoption des sept fonctionnalités de sécurité clés correspond à la moyenne dans votre secteur d'activité.

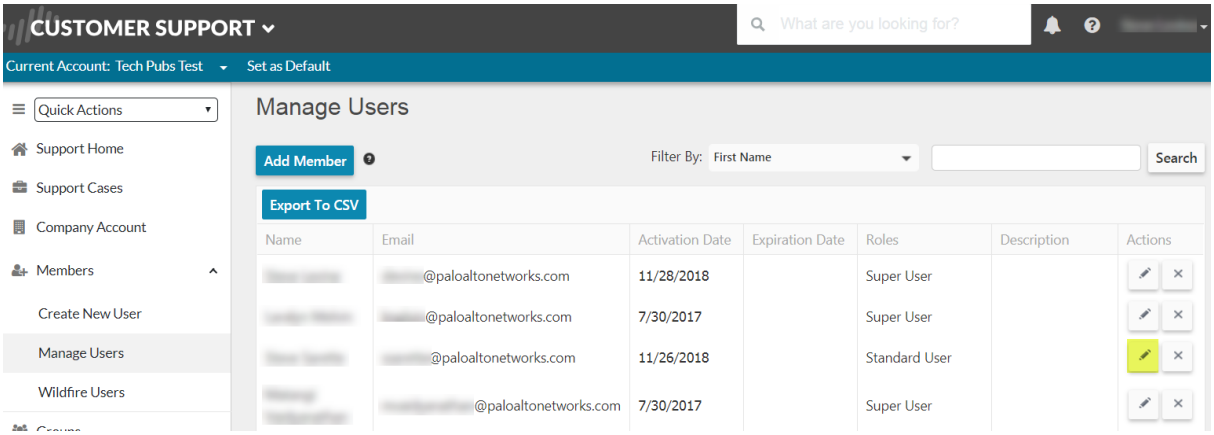
- Accès au BPA à partir du portail de support client
- Génération et téléchargement d'un rapport BPA

Accès au BPA à partir du portail de support client

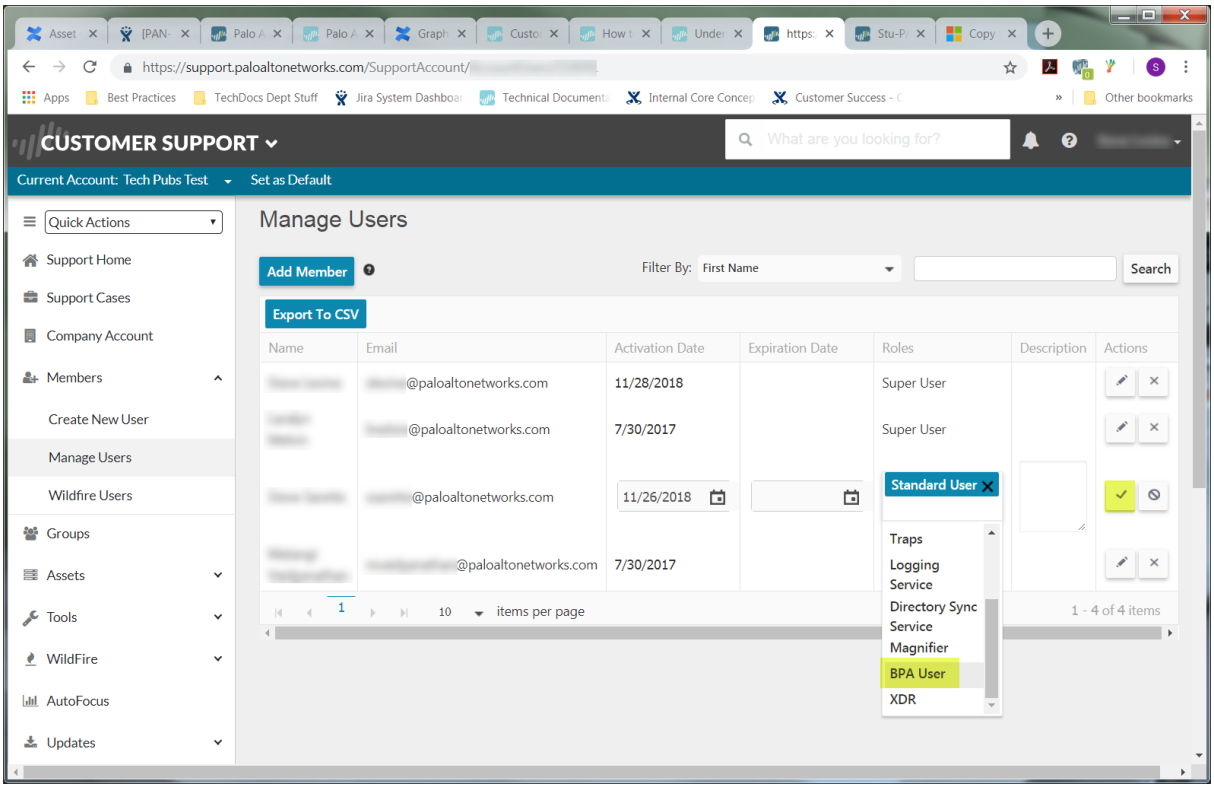
STEP 1 | Dans l'écran d'accueil de l'authentification du portail de support client, sélectionnez **Members (Membres)** > **Manage Users (Gérer les utilisateurs)**.



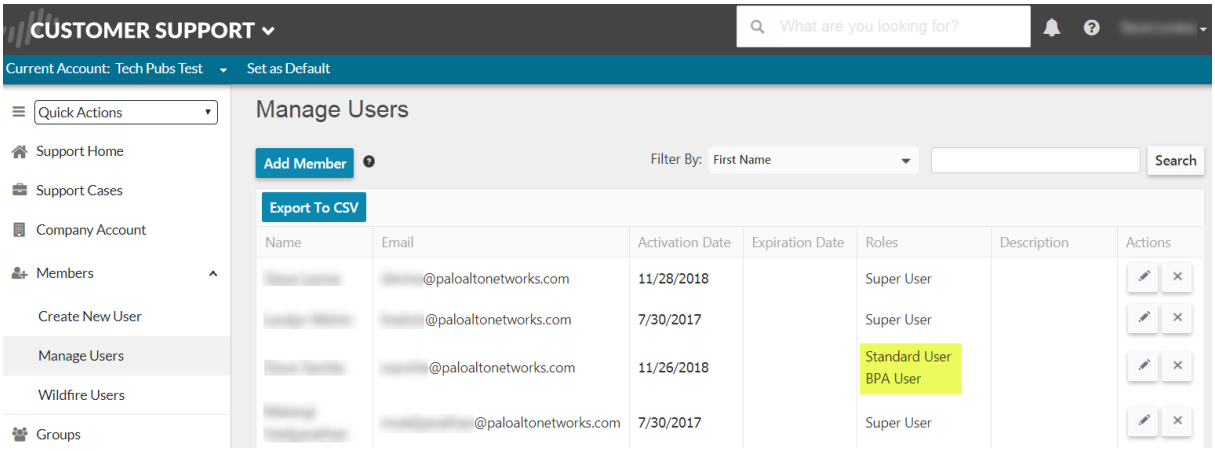
STEP 2 | Cliquez sur l'icône en forme de crayon pour modifier le Standard User (Utilisateur standard) auquel vous souhaitez attribuer des autorisations BPA.



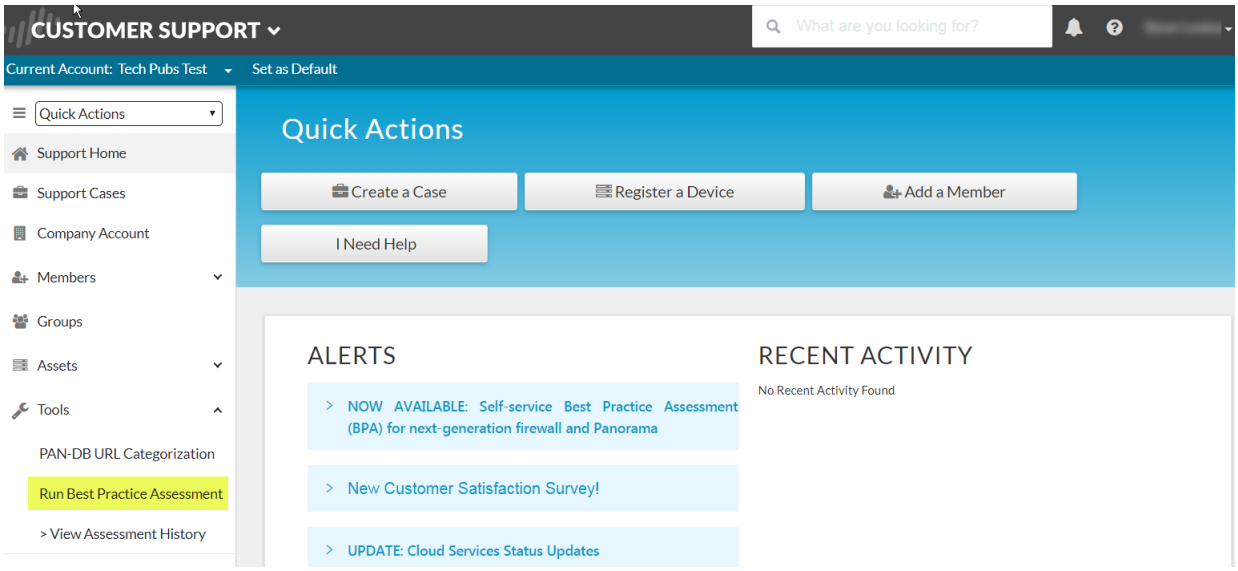
STEP 3 | Sélectionnez un rôle **BPA User** (Utilisateur BPA), puis cliquez sur la coche de mise à jour pour ajouter le nouveau rôle.



STEP 4 | L'utilisateur standard dispose maintenant des privilèges du rôle d'utilisateur BPA.



STEP 5 | Les Super Users (Super-utilisateurs) et les Standard Users (Utilisateurs standard) dotés du rôle de BPA User (Utilisateur BPA) peuvent se connecter au Portail Support Client pour accéder au BPA et l'exécuter (**Tools (Outils)** > **Run Best Practice Assessment (Exécution du Best Practice Assessment)**).



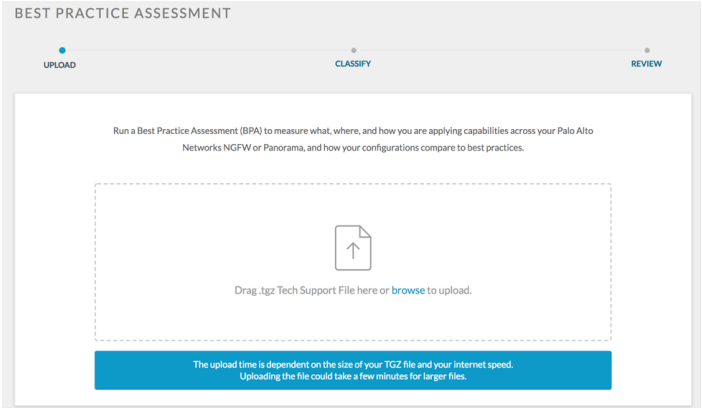
Génération et téléchargement d'un rapport BPA

Après avoir obtenu l'accès au BPA, vous pouvez générer un rapport BPA pour un appareil Panorama ou pour un pare-feu nouvelle génération.

Si possible, générez des rapports BPA pour les appareils Panorama au lieu de pare-feu nouvelle génération individuels afin d'obtenir une visibilité complète de tous les pare-feu de votre environnement en un seul rapport. Générez régulièrement des rapports afin de mesurer les progrès réalisés dans l'adoption de fonctionnalités de sécurité et de bonnes pratiques de sécurité.

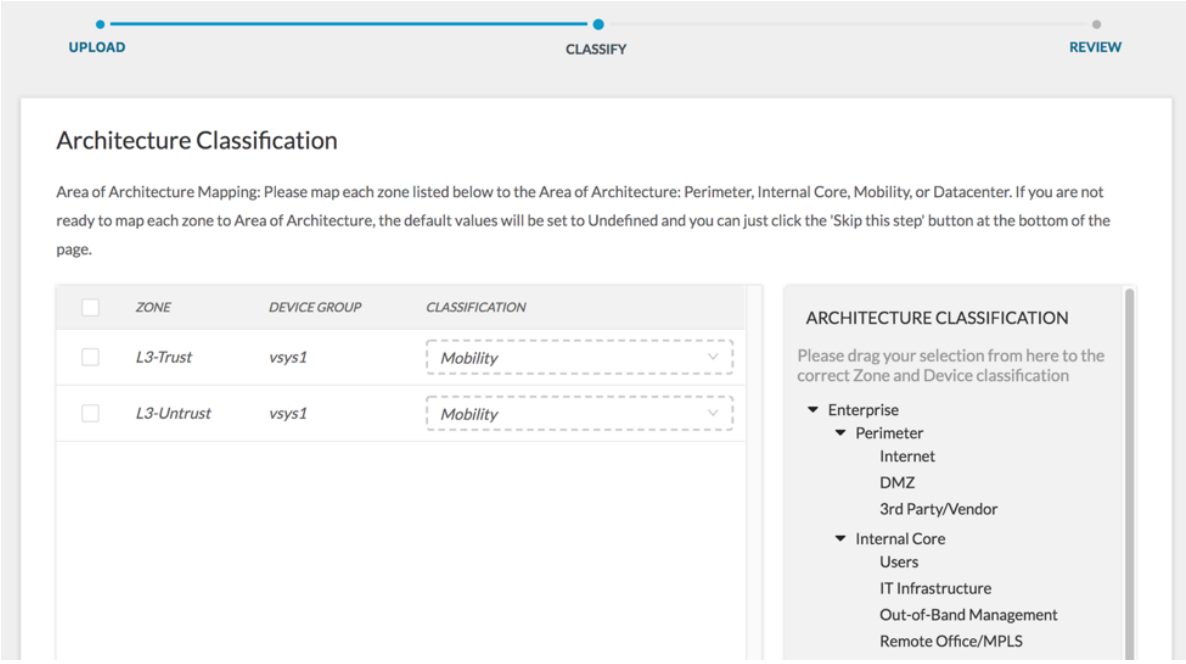
STEP 1 | Faites glisser ou déposez un Fichier de support technique (fichier .tgz) dans la fenêtre du portail de support client ou recherchez un fichier de support technique.

Les Super Users (Super-utilisateurs) peuvent créer des fichiers de support technique (**Device (Périphérique)** > **Support** > **Tech Support File (Fichier de support technique)** ou **Panorama** > **Support** > **Tech Support File (Fichier de support technique)**).



STEP 2 | Vous pouvez éventuellement mapper chaque zone sur la zone d'architecture ou cliquer sur **Skip this step** (Ignorer cette étape) pour exécuter le BPA sans mapper les zones.

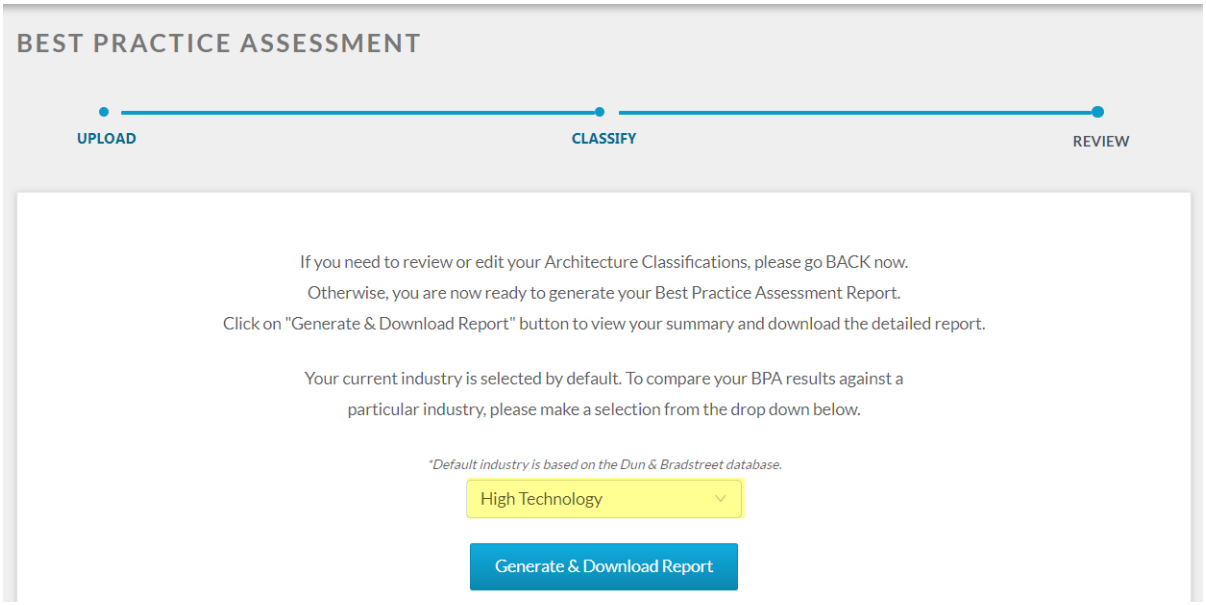
Faites glisser et déposez la valeur architecturale depuis la classification de l'architecture, utilisez la liste déroulante **Classification** pour sélectionner une valeur, ou utilisez plusieurs cases à cocher pour sélectionner plusieurs zones, puis appliquez une valeur à toutes les zones sélectionnées simultanément.



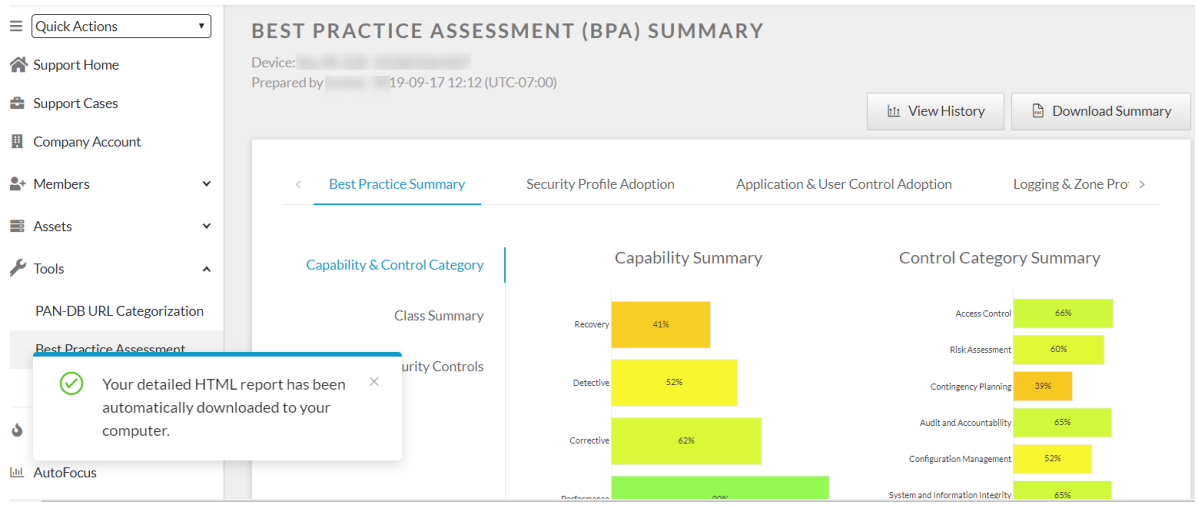
STEP 3 | Identifiez le secteur d'activité correspondant à votre compte, puis générez et téléchargez le rapport BPA (**Generate & Download Report (Générer et télécharger un rapport)**).

Vous pouvez modifier le secteur d'activité auquel le BPA compare vos résultats à l'aide de la liste déroulante. Si vous souhaitez modifier quelque chose avant de générer le rapport, vous pouvez également revenir en arrière et effectuer ces modifications.

La fonction **Generate & Download Report (Générer et télécharger un rapport)** télécharge le rapport BPA détaillé, le récapitulatif et une feuille de calcul qui montre les échecs de vérifications des bonnes pratiques dans le système à partir duquel vous avez accédé au BPA et l'avez exécuté.



STEP 4 | Le BPA généré affiche le résumé et vous informe que le rapport HTML détaillé a été téléchargé sur votre ordinateur.



STEP 5 | Maintenant que vous savez comment exécuter le BPA, accédez au Portail Support Client et essayez-le dès aujourd'hui (ou contactez votre SE de Palo Alto Networks ou votre partenaire pour exécuter le BPA) afin de commencer la transition vers un réseau plus sécurisé.

Si vous souscrivez au contrat de support Premium (à compter du 1er novembre 2019) ou Platinum, utilisez le BPA pour préparer votre posture de sécurité afin de tirer profit de Assurance de sécurité, ce qui vous aidera dans l'enquête initiale sur les incidents.

Assurance de sécurité

Si vous détectez une activité suspecte sur votre réseau, l'Assurance de sécurité vous fournit une aide supplémentaire de Palo Alto Networks lorsque vous en avez le plus besoin. L'Assurance de sécurité fournit :

- L'accès aux experts en sécurité de Palo Alto Networks et à leurs outils spécialisés de renseignement sur les menaces et leurs pratiques de recherche de menaces.
- Une analyse avancée des journaux et des indicateurs de compromis (IOC).
- Une évaluation de la configuration qui comprend des recommandations personnalisées sur la sécurité des produits.
- Des recommandations pour l'étape suivante afin d'accélérer la transition vers votre fournisseur de réponse aux incidents (RI) pour vous aider à gérer et à résoudre l'incident.

Pour bénéficier de l'Assurance de sécurité, vous devez souscrire au contrat de support Premium (à compter du 1er novembre 2019) ou au contrat de support Platinum.

La première étape vers l'Assurance de sécurité consiste à effectuer une évaluation des bonnes pratiques (BPA) pour mesurer votre adoption des sept fonctionnalités de sécurité clés : WildFire, antivirus, antispyware, DNS Sinkhole, filtrage des URL, protection contre les vulnérabilités et journalisation. Nous vous recommandons de vous assurer que votre taux d'adoption de ces fonctionnalités de sécurité est au moins égal au taux d'adoption moyen dans votre secteur d'activité.

L'exécution du BPA et l'adoption de niveaux plus élevés des fonctionnalités de sécurité clés assurent une meilleure protection de votre réseau et contribuent à éviter les incidents. Le BPA mesure également le niveau d'adoption de nombreuses autres fonctionnalités de sécurité telles que l'App-ID et l'User-ID, la configuration des zones et d'autres profils de sécurité tels que les profils de blocage de fichiers et de protection DoS. Le BPA fait également des recommandations sur la manière d'améliorer votre posture de sécurité.

Exécutez le BPA à intervalles réguliers (par exemple, tous les mois ou tous les trimestres) pour mesurer l'adoption des fonctionnalités de sécurité clés, comprendre l'état de la sécurité de votre réseau et hiérarchiser les améliorations de sécurité.

Lorsque vous souscrivez au contrat de support Premium (à compter du 1er novembre 2019) ou au contrat de support Platinum et que vous exécutez le BPA, s'il s'avère que vous avez adopté les sept fonctionnalités de sécurité clés à un taux conforme à la moyenne dans votre secteur d'activité, alors l'Assurance de sécurité est automatiquement activée. Si vous avez besoin d'aide pour adopter ces fonctionnalités clés à un taux conforme à la moyenne dans votre secteur d'activité, contactez votre représentant commercial Palo Alto Networks pour vous aider à définir les exigences, à fournir des critères de justification, etc. Si des raisons commerciales vous empêchent d'adopter les fonctionnalités de sécurité clés à ce niveau, veuillez travailler avec votre représentant commercial Palo Alto Network sur la manière d'accéder aux avantages de l'Assurance de sécurité.

Les sept fonctionnalités de sécurité clés à adopter

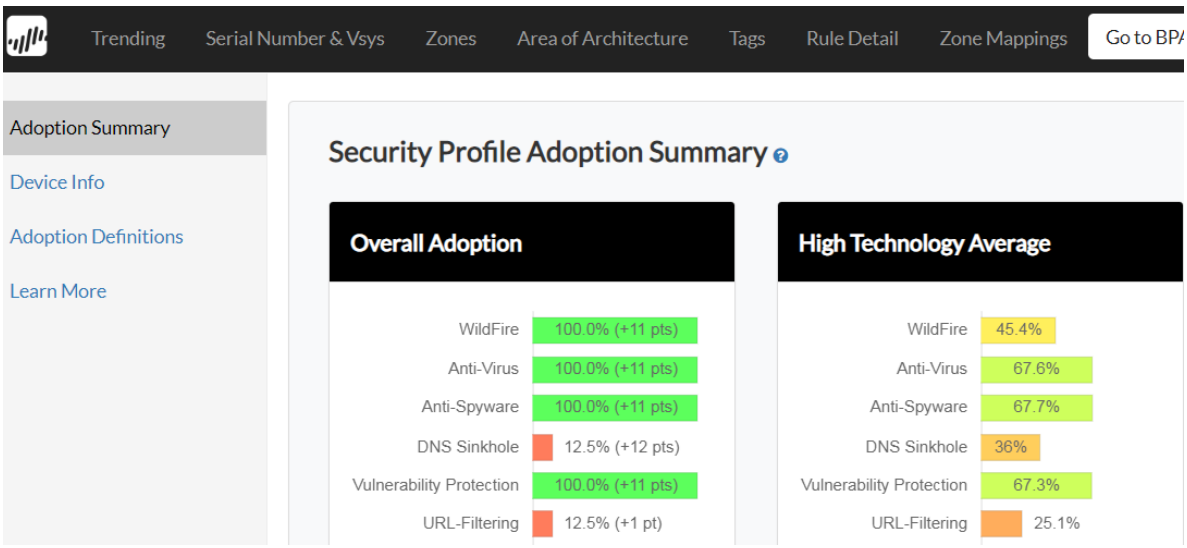
Nous recommandons vivement l'adoption de ces sept fonctionnalités de sécurité clés pour les raisons suivantes :

- **WildFire** : associez un profil de sécurité WildFire aux règles de politique de sécurité qui permettent au trafic de protéger votre réseau contre de nouvelles menaces inconnues. WildFire est une défense solide contre les menaces persistantes avancées (ATP).
- **Antivirus** : associez un profil de sécurité antivirus aux règles de sécurité qui permettent au trafic de bloquer les fichiers malveillants connus tels que les logiciels malveillants, les ransomwares, les bots et les virus.
- **Antispyware** : associez un profil de sécurité antispyware aux règles de sécurité qui permettent au trafic de détecter le trafic de commande et de contrôle (C2) initié par un code malveillant s'exécutant sur un serveur ou un terminal et d'empêcher les systèmes infectés d'établir une connexion sortante à partir de votre réseau.
- **DNS Sinkhole** : configurez la partie DNS Sinkhole d'un profil de sécurité antispyware qui est associé aux règles de politique de sécurité qui autorisent le trafic. La fonctionnalité DNS Sinkhole permet d'identifier les hôtes potentiellement compromis qui tentent d'accéder à des domaines douteux en localisant les hôtes et en les empêchant d'accéder à ces domaines.
- **Filtrage des URL** : associez un profil de filtrage des URL à des règles de politique de sécurité qui autorisent le trafic pour empêcher l'accès à des contenus Web à risque (sites pouvant contenir des contenus malveillants). Les profils de filtrage des URL et les catégories d'URL vous donnent un contrôle granulaire sur les types de sites Web auxquels vous autorisez l'accès.
- **Protection contre les vulnérabilités** : associez un profil de sécurité de protection contre les vulnérabilités à des règles de politique de sécurité qui permettent au trafic d'empêcher les pirates d'exploiter les vulnérabilités côté client et côté serveur et de transmettre des charges utiles malveillantes à votre réseau et à vos utilisateurs, et d'empêcher les pirates d'utiliser les vulnérabilités pour se déplacer latéralement au sein de votre réseau.
- **Journalisation** : activez la journalisation de tout le trafic (autorisé et refusé) pour fournir une piste d'audit horodatée des événements du système et du trafic réseau. Les journaux fournissent des informations essentielles pour les enquêtes sur les incidents. Le transfert des journaux vous permet d'envoyer les journaux de tous vos pare-feu à Panorama ou à l'extérieur afin d'agréger les journaux pour analyse.

L'adoption de ces fonctionnalités clés améliore considérablement votre posture de sécurité, réduit la surface d'attaque, augmente votre visibilité sur le trafic réseau, prévient les attaques connues et nouvelles, et protège vos données, ressources, applications et services les plus précieux pour votre réseau.

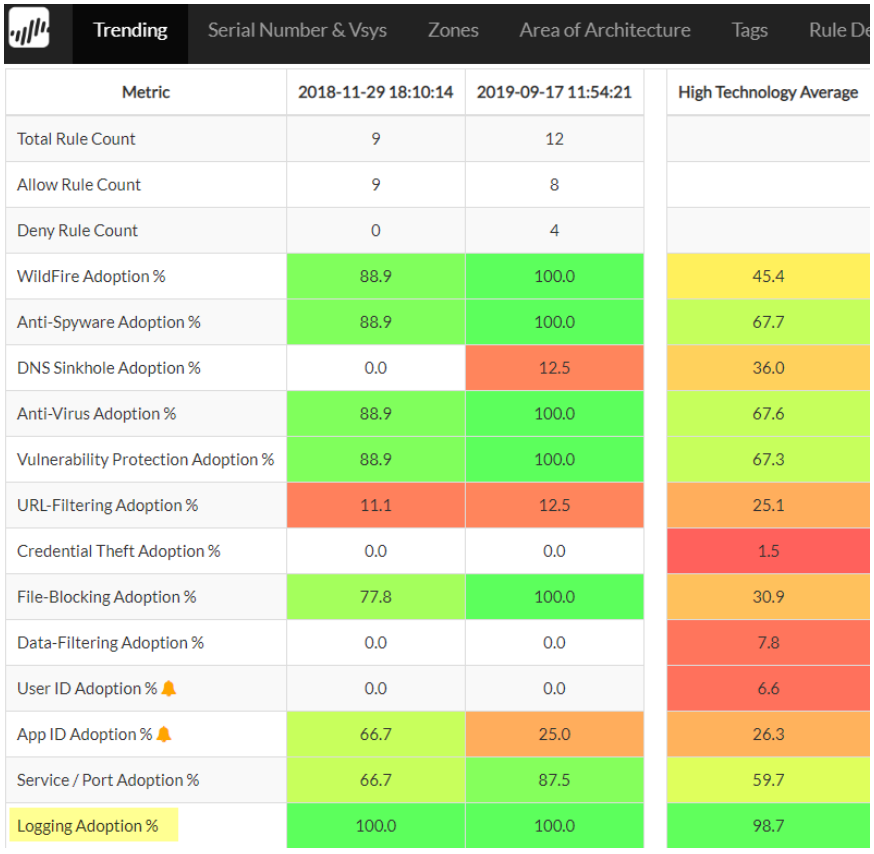
Vérification de l'adoption des sept fonctionnalités clés de sécurité

Dans le rapport BPA détaillé (format HTML) que vous recevez lorsque vous générez et téléchargez vos résultats BPA, accédez à la page Adoption Summary (Résumé de l'adoption) pour vérifier votre adoption globale des six fonctionnalités du profil de sécurité (WildFire, antivirus, antispyware, DNS Sinkhole, filtrage des URL, protection contre les vulnérabilités et journalisation) et l'adoption moyenne de ces fonctionnalités dans votre secteur d'activité (la journalisation est une vérification distincte). La page Adoption Summary (Résumé de l'adoption) montre l'adoption de vos fonctionnalités de sécurité par rapport à votre secteur d'activité et vous aide à identifier les lacunes dans l'adoption. Par exemple, si votre secteur d'activité est la haute technologie :



Les résultats montrent que la configuration correspond à l'adoption moyenne dans le secteur d'activité pour quatre fonctionnalités : profils WildFire, Antivirus, Antispyware et Protection contre les vulnérabilités. Les résultats montrent également que la configuration ne correspond pas à la d'adoption moyenne dans le secteur d'activité pour deux fonctionnalités : DNS Sinkhole et Filtrage des URL. Cela indique la prochaine action à entreprendre : configurer DNS Sinkhole dans le profil Antispyware et appliquer le filtrage des URL au trafic Internet.

Dans le rapport BPA détaillé au format HTML, accédez à la page **Trending (Tendance)** pour vérifier votre adoption globale des fonctionnalités de journalisation et l'adoption moyenne de la journalisation dans votre secteur d'activité.



Metric	2018-11-29 18:10:14	2019-09-17 11:54:21	High Technology Average
Total Rule Count	9	12	
Allow Rule Count	9	8	
Deny Rule Count	0	4	
WildFire Adoption %	88.9	100.0	45.4
Anti-Spyware Adoption %	88.9	100.0	67.7
DNS Sinkhole Adoption %	0.0	12.5	36.0
Anti-Virus Adoption %	88.9	100.0	67.6
Vulnerability Protection Adoption %	88.9	100.0	67.3
URL-Filtering Adoption %	11.1	12.5	25.1
Credential Theft Adoption %	0.0	0.0	1.5
File-Blocking Adoption %	77.8	100.0	30.9
Data-Filtering Adoption %	0.0	0.0	7.8
User ID Adoption %	0.0	0.0	6.6
App ID Adoption %	66.7	25.0	26.3
Service / Port Adoption %	66.7	87.5	59.7
Logging Adoption %	100.0	100.0	98.7

Cette page montre non seulement votre niveau d'adoption par rapport à votre secteur d'activité, mais aussi par rapport à la dernière fois que vous avez exécuté le BPA. Il s'agit d'une mesure de l'amélioration de la sécurité au fil du temps ainsi que d'un appel à l'action si vos résultats indiquent que votre sécurité n'est pas aussi stricte que vous le souhaitez.

Si le profil et les résultats de journalisation montrent que votre adoption des sept fonctionnalités correspond à la moyenne dans votre secteur d'activité, l'Assurance de sécurité est automatiquement activée. Si vous avez besoin d'aide pour adopter ces fonctionnalités clés à un taux conforme à la moyenne dans votre secteur d'activité, contactez votre représentant commercial Palo Alto Networks pour vous aider à définir les exigences, à fournir des critères de justification, etc. Si des raisons commerciales vous empêchent d'adopter les fonctionnalités de sécurité clés à ce niveau, veuillez travailler avec votre représentant commercial Palo Alto Network sur la manière d'accéder aux avantages de l'Assurance de sécurité.

Amélioration de l'adoption des sept fonctionnalités clés de sécurité

Utilisez le BPA en association avec la documentation technique de Palo Alto Networks pour identifier les fonctionnalités de sécurité qui doivent être améliorées et pour apporter les améliorations nécessaires, en particulier dans les sept fonctionnalités de sécurité clés. L'amélioration de votre posture de sécurité contribue à protéger vos utilisateurs et vos périphériques, ressources, applications et services précieux.

- **WildFire** : transition des profils WildFire en toute sécurité vers les bonnes pratiques puis mise en œuvre des bonnes pratiques WildFire. Le profil WildFire des bonnes pratiques est le profil par défaut.
- **Antivirus** : transition des profils antivirus en toute sécurité vers les bonnes pratiques puis mise en œuvre des bonnes pratiques antivirus (ou bonnes pratiques antivirus pour le centre de données légèrement plus strictes).
- **Antispyware et DNS Sinkhole** : la configuration de DNS Sinkhole se trouve dans l'onglet **DNS Signatures (Signatures DNS)** du profil de sécurité antispyware. Transition des profils antispyware en toute sécurité vers les bonnes pratiques puis mise en œuvre des bonnes pratiques antispyware (ou bonnes pratiques antispyware pour le centre de données légèrement plus strictes).
- **Filtrage des URL** : transition des profils de filtrage des URL en toute sécurité vers les bonnes pratiques puis mise en œuvre des bonnes pratiques de filtrage des URL.
- **Protection contre les vulnérabilités** : transition des profils de protection contre les vulnérabilités en toute sécurité vers les bonnes pratiques puis mise en œuvre des bonnes pratiques de protection contre les vulnérabilités (ou bonnes pratiques de protection contre les vulnérabilités pour le centre de données légèrement plus strictes).
- **Journalisation** : journalisation des règles de politique de sécurité à la fin de la session par défaut.

En outre, le BPA et la documentation technique vous montrent comment améliorer de nombreuses autres fonctionnalités de sécurité telles que l'App-ID, l'User-ID, les profils de blocage de fichiers, la protection de zone et DoS, et la protection contre le vol d'informations d'identification. Voici quelques ressources clés :

- Premiers pas avec le BPA : vous montre comment utiliser le BPA pour examiner l'adoption des fonctionnalités de sécurité et identifier les lacunes dans l'adoption, évaluer votre configuration, y compris les politiques, les objets, le réseau et la configuration des périphériques et de Panorama, et hiérarchiser les changements, y compris le renforcement de votre posture de gestion des périphériques, l'amélioration de la visibilité dans le trafic et la mise en œuvre des contrôles initiaux des bonnes pratiques.
- Bonnes pratiques de déchiffrement : vous montre comment augmenter votre visibilité en déchiffrant tout le trafic que votre métier, les considérations de confidentialité et les réglementations autorisent, afin que vous puissiez inspecter le maximum de trafic et protéger votre réseau des menaces chiffrées.
- Bonnes pratiques de protection de zone et DoS : vous montre comment adopter une approche par couches pour vous protéger contre les attaques par déni de service (DoS) qui tentent de neutraliser votre réseau et pour défendre le périmètre, les zones et les périphériques individuels de votre réseau.

- Meilleures pratiques pour les mises à jour du contenu de menace et des applications : déploie des mises à jour de contenu et d'applications de la meilleure manière possible pour vos exigences d'affaires et garantit que votre réseau est protégé contre les dernières menaces et identifie les applications les plus récentes.

Vous trouverez tous ces documents et bien d'autres encore sur le portail Best Practices (Bonnes pratiques) et sur la page Transition to Best Practices (Transition vers les bonnes pratiques).

Comment faire appel à l'Assurance de sécurité

Si vous êtes confronté à une activité suspecte, vous devez, lorsque vous faites appel à l'Assurance de sécurité, fournir un ensemble de données spécifiques sur l'incident suspect afin que les experts de Palo Alto Networks puissent enquêter sur l'activité en question.

- Données à collecter avant de faire appel à l'Assurance de sécurité
- Faire appel à l'Assurance de sécurité

Données à collecter avant de faire appel à l'Assurance de sécurité

Les experts de Palo Alto Networks ont besoin au minimum des informations suivantes sur l'activité suspecte pour commencer à diagnostiquer le problème potentiel. Veuillez collecter ces données avant de faire appel à l'Assurance de sécurité.

Détails de base concernant l'activité suspecte :

- **Vecteur et type de l'attaque suspecte** : quelle preuve de l'activité suspecte a alerté votre équipe administrative ou d'intervention ?
- **Chronologie** :
  - Date et heure de l'attaque initiale suspecte, si elles sont connues.
  - Heure à laquelle vous avez identifié le problème potentiel.
- **Détails de l'incident** :
  - Adresses IP connues des systèmes touchés.
    - Adresses IP des hôtes touchés qui sont accessibles au public par NAT.
    - Services critiques pouvant faire du ou des systèmes une cible, par exemple les bases de données, les services Web et les serveurs d'accès à distance (RDP, Citrix, etc.).
  - Adresses IP connues ou suspectes qui peuvent être liées à l'attaque.
  - User-ID des comptes utilisateur compromis (le cas échéant).
- **Aperçu ou diagramme de la topologie** : l'emplacement du pare-feu par rapport aux hôtes touchés. (Un diagramme complet de la topologie du réseau n'est pas nécessaire.)
- **Indicateurs de compromis et logiciels malveillants** :
  - Échantillons.
  - Hachages.

Données du pare-feu :

- **Fichiers de support technique** :
  - Générez et chargez des fichiers de support technique à partir des pare-feu dans le chemin d'accès aux périphériques potentiellement touchés au moment de l'activité suspecte.
  - Si vous utilisez Panorama pour gérer les pare-feu, générez et chargez le fichier de support technique Panorama.
- **Journaux du pare-feu** : exportez les journaux du pare-feu et des appareils Panorama datant de deux heures avant l'activité suspecte. Avant d'exporter les journaux, vérifiez que le paramètre de ligne CSV est à la valeur maximale de 65 535 lignes (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports)**).

Si la valeur est inférieure, augmentez-la jusqu'à la valeur maximale de 65 535 lignes. Exportez les journaux pour chacune des catégories de base suivantes (si les journaux sont activés) en fonction des informations relatives à l'adresse IP et des détails de l'horodatage (vous pouvez filtrer les journaux pour afficher les entrées de journaux selon l'adresse IP et l'heure) :

- Journaux de filtrage des données
- Journaux du trafic
- Journaux des menaces
- Journaux de filtrage des URL
- Journaux User-ID (si vous soupçonnez un mouvement latéral)
- Journaux des envois WildFire

Il est important de comprendre la politique et la capacité de conservation des journaux de votre déploiement afin de s'assurer que toutes les données pertinentes soient bien examinées. Les administrateurs peuvent devoir prendre des mesures supplémentaires, comme l'exportation de données à partir de pare-feu ou d'autres serveurs de journalisation, afin de garantir la continuité et l'exhaustivité des données pendant la durée de l'enquête.

Davantage de moyens pour identifier les données significatives concernant les activités suspectes :

- **Utilisez le centre de commande des applications (ACC)**. L'ACC peut vous montrer les pics de trafic, les anomalies et les changements avant, pendant et après l'activité suspecte.
- **Utilisez le rapport de surveillance des menaces** pour visualiser les principales menaces avant, pendant et après l'activité suspecte.

Faire appel à l'Assurance de sécurité

Une fois que vous avez collecté les données sur l'activité suspecte afin de garantir l'analyse opportune des informations pertinentes, vous êtes prêt à faire appel à l'Assistance de sécurité. Vous pouvez faire appel à l'Assistance de sécurité de deux manières :

- Ouvrez une session dans le portail de support client. Cliquez sur **Create a Case (Créer un dossier)** pour ouvrir un dossier de support. Lorsque vous remplissez le formulaire, sélectionnez **Threat (Menace)**.
- Votre ingénieur commercial (SE) peut ouvrir un dossier de support en votre nom.