Démarrage avec le BPA

10.0 (EoL)

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

July 15, 2020

Table of Contents

Évaluation de l'adoption des fonctionnalités de la politique de sécurité

L'outil Best Practice Assessment (BPA) vous aide à comprendre votre niveau actuel d'adoption des fonctionnalités de la politique de sécurité et à évaluer la maturité et l'efficacité de votre posture de sécurité. L'adoption de fonctionnalités telles que WildFire, la protection contre les vulnérabilités, le décryptage SSL, etc., contribue à la détection et à la prévention des attaques. Il est essentiel de bien comprendre comment et où utiliser chaque fonctionnalité dans différents environnements afin de mieux protéger votre réseau et ses précieux atouts.

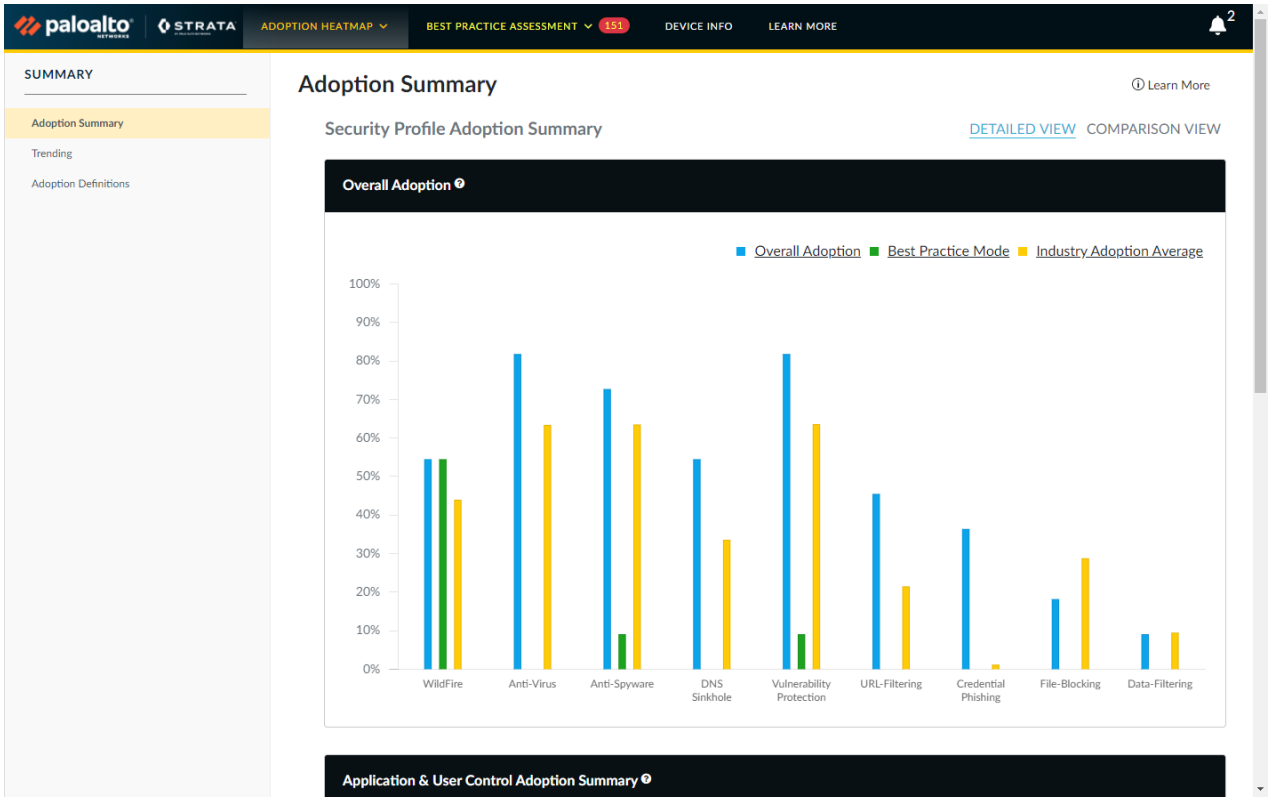
La fonctionnalité Getting Started with Best Practices (Démarrer avec les meilleures pratiques) montre comment accéder et exécuter le BPA. La section Capability Adoption Heatmaps (Cartes thermiques relatives à l'adoption des fonctionnalités) du rapport BPA vous permet de vérifier l'adoption de ces fonctionnalités dans la base de règles de la politique de sécurité. Regardez la vidéo Introduction à Heatmaps pour en savoir plus sur les cartes thermiques et profitez de la Vidéothèque BPA pour en savoir plus sur l'outil.

Examinez et analysez les informations contenues dans les onglets Heatmap (Carte thermique) pour identifier les failles dans l'adoption des fonctionnalités de sécurité et déterminer ce que vous souhaitez améliorer :

- Examen du résumé de l'adoption
- #unique_3
- #unique_4

Examen du résumé de l’adoption

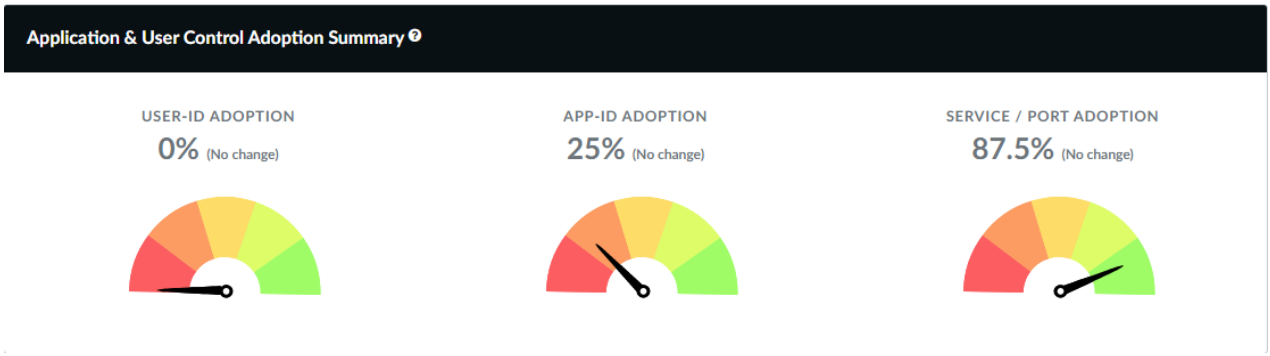
Après que vous ou votre représentant de Palo Alto Networks avez procédé à l’exécution du BPA, le rapport HTML qui en résulte s’ouvre sur la page Adoption Heatmap (Carte thermique relative à l’adoption), dans le Adoption Summary (Résumé de l’adoption). La vue Adoption Summary (Résumé de l’adoption) fournit une vue d’ensemble de l’adoption globale des fonctionnalités de sécurité par votre équipement. Le rapport indique le pourcentage d’adoption actuel pour chaque indicateur (à l’exception d’Industry Average [Moyenne de l’industrie] qui fournit les moyennes d’adoption de votre secteur), et entre parenthèses, le pourcentage de changement dans l’adoption depuis la dernière exécution du BPA sur le fichier de configuration de l’équipement (ou **No change** [Aucun changement] si la valeur est la même qu’à la dernière exécution du BPA).



Overall Adoption (Adoption globale) : adoption des profils de sécurité dans les règles d’autorisation de la politique de sécurité. Les pourcentages sont basés sur le nombre de règles d’autorisation pour lesquelles un ou plusieurs profils sont activés dans le cadre de la règle. Le BPA ne compte pas les règles désactivées ni les règles de blocage.

Industry Average (Moyenne du secteur) : adoption moyenne des profils de sécurité dans les règles d’autorisation pour le secteur de votre entreprise.

Best Practice Mode (Mode respectant les meilleures pratiques) : adoption des profils de sécurité configurés de la manière respectant les meilleures pratiques recommandée dans les règles d’autorisation. Le BPA ne compte que les règles dont les profils passent avec succès toutes les vérifications de meilleures pratiques.

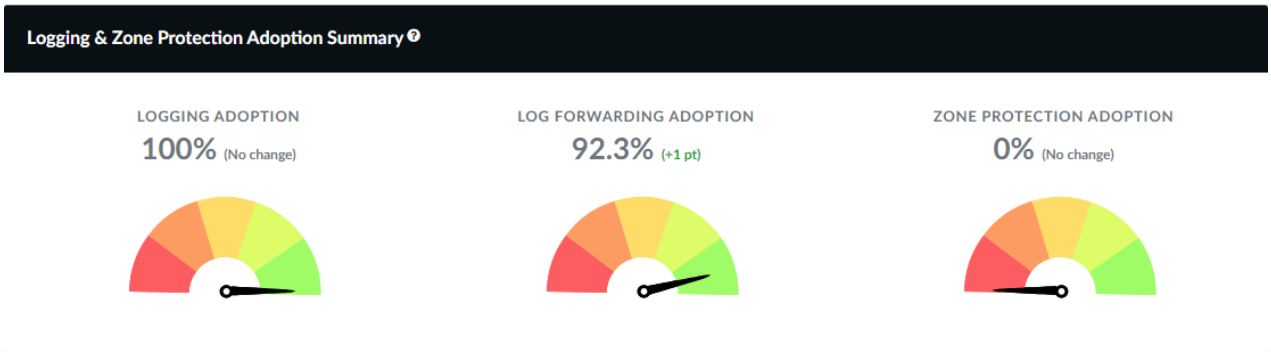


App-ID Adoption (Adoption d'App-ID) : adoption d'App-ID dans les règles de politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles d'autorisation avec une ou plusieurs applications définies (l'application n'est pas **any** (tout)). Le BPA ne compte pas les règles désactivées.

User-ID Adoption (Adoption de User-ID) : adoption de User-ID dans les règles de politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles d'autorisation avec les utilisateurs (y compris les valeurs **known-user** (utilisateur connu) et **unknown** (inconnu)) ou des groupes d'utilisateurs. Le BPA ne compte pas les règles désactivées.

Service/Port Adoption (Adoption de service/port) : adoption du service/port dans les règles de politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles d'autorisation avec un service ou un port défini (le Service n'est pas **any** (tout)). Le BPA ne compte pas les règles désactivées.

Le BPA ne compte pas l'adoption d'App-ID, de User-ID ou de service/port pour les règles de blocage, car la logique de blocage varie d'une entreprise à l'autre. Le BPA ne peut donc pas faire de recommandations basées sur des règles de blocage.



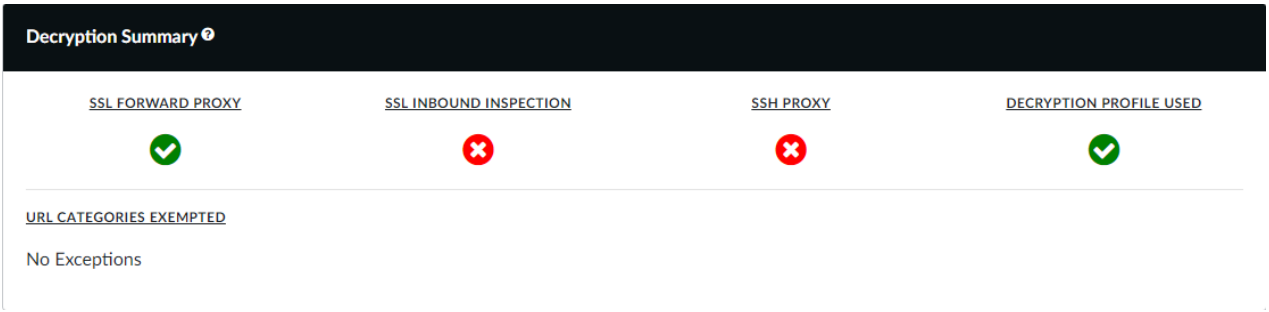
Logging Adoption (Adoption de la journalisation) : adoption de **Log at Session End** (Journaliser à la fin de la session) dans les règles de la politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles avec **Log at Session End** (Journaliser à la fin de la session) activée. Le BPA ne compte pas les règles désactivées.

Log Forwarding Adoption (Adoption du transfert de journaux) : adoption de profils de transfert de journaux dans les règles de la politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles avec un profil de transfert de journaux configuré. Le BPA ne compte pas les règles désactivées.

Zone Protection Adoption (Adoption de la protection de zone) : adoption de la protection de zone dans les règles d'autorisation de la politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles d'autorisation dans lesquelles un profil de protection de zone est configuré dans la zone source. Le BPA ne compte pas les règles désactivées.

Pour chacun de ces indicateurs, la valeur entre parenthèses à côté de chaque pourcentage est le pourcentage de changement dans l'adoption depuis la dernière exécution du BPA sur le fichier de

configuration de l'équipement (ou **No change** (Aucun changement) si la valeur est la même qu'à la dernière exécution du BPA).



Decryption Summary (Résumé du décryptage) : indique si la configuration inclut des règles de politique de décryptage pour le proxy de transfert SSL, l'inspection SSL entrante et le proxy SSH. Le résumé indique également si la configuration inclut des profils de décryptage et identifie les catégories d'URL que l'équipement exclut du décryptage.

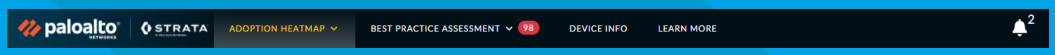
Si vous ne déchiffrez pas une catégorie d'URL (ou des applications individuelles), vous ne pouvez pas inspecter son trafic, car le pare-feu ne peut pas voir le contenu du trafic crypté. Le pare-feu peut uniquement inspecter le trafic que vous déchiffrez.

Étape suivante :#unique_3 pour comprendre les domaines dans lesquels vous pouvez améliorer la sécurité.

Évaluation de la configuration des meilleures pratiques

L'outil Best Practice Assessment (BPA) vous aide à comprendre le niveau actuel de configuration de votre politique de sécurité vis-à-vis des meilleures pratiques afin que vous puissiez évaluer la maturité de votre posture de sécurité. Regardez la vidéo Introduction au BPA pour en savoir plus sur le BPA et profitez de la Vidéothèque BPA pour en savoir encore plus sur l'outil.

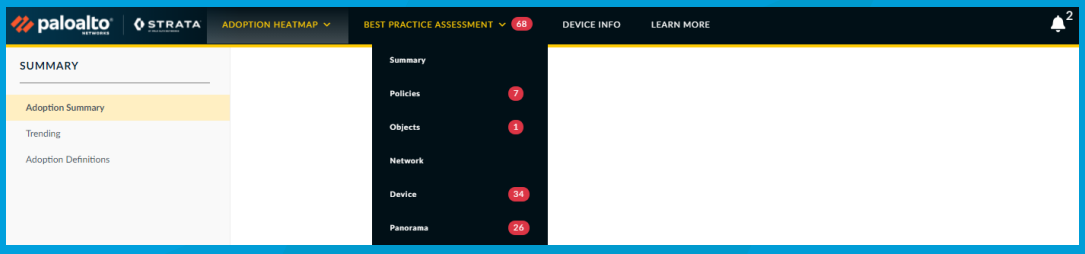
Le rapport BPA s'ouvre d'abord sur la page Adoption Heatmap (Carte thermique relative à l'adoption). Cliquez sur l'outil **Best Practice Assessment** pour voir la section BPA du rapport qui se concentre sur l'adoption des meilleures pratiques en matière de configuration pour les pare-feu nouvelle génération et Panorama.



Outre cette documentation, vous pouvez visionner la Démonstration BPA et une courte vidéo sur Comment exécuter un BPA pour en savoir plus sur l'utilisation du BPA.

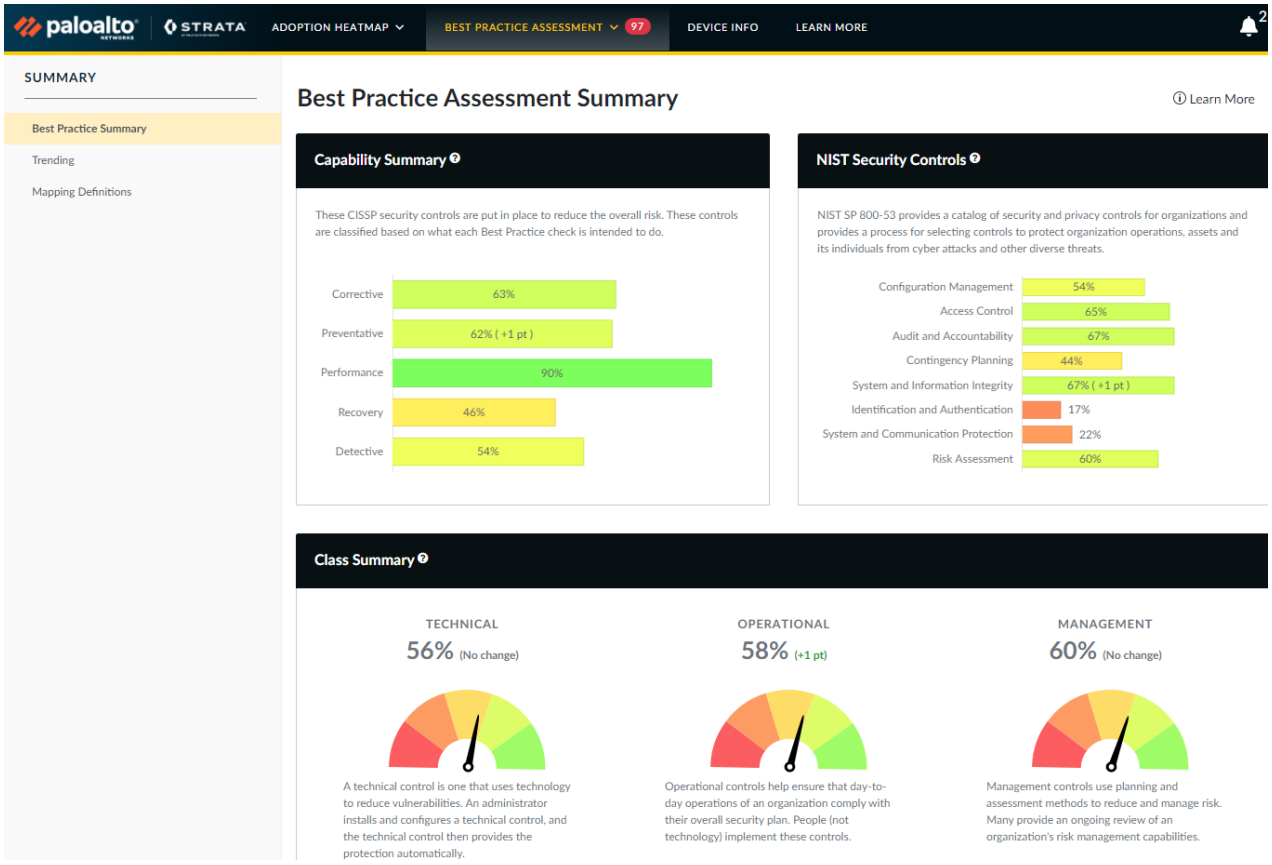
Un rapport BPA évalue un fichier de configuration du pare-feu nouvelle génération ou de Panorama avec plus de 200 vérifications des meilleures pratiques. Le BPA regroupe les résultats de l'évaluation en fonction des informations sur les politiques, objets, réseau et équipement/Panorama de la même manière que sur l'interface utilisateur PAN-OS. Examinez et analysez les informations pour trouver les domaines à améliorer sur lesquels vous concentrer :

> Examen du résumé des meilleures pratiques
> Examen de la configuration de la politique en matière de meilleures pratiques
> #unique_8
> #unique_9
> #unique_10



Examen du résumé des meilleures pratiques

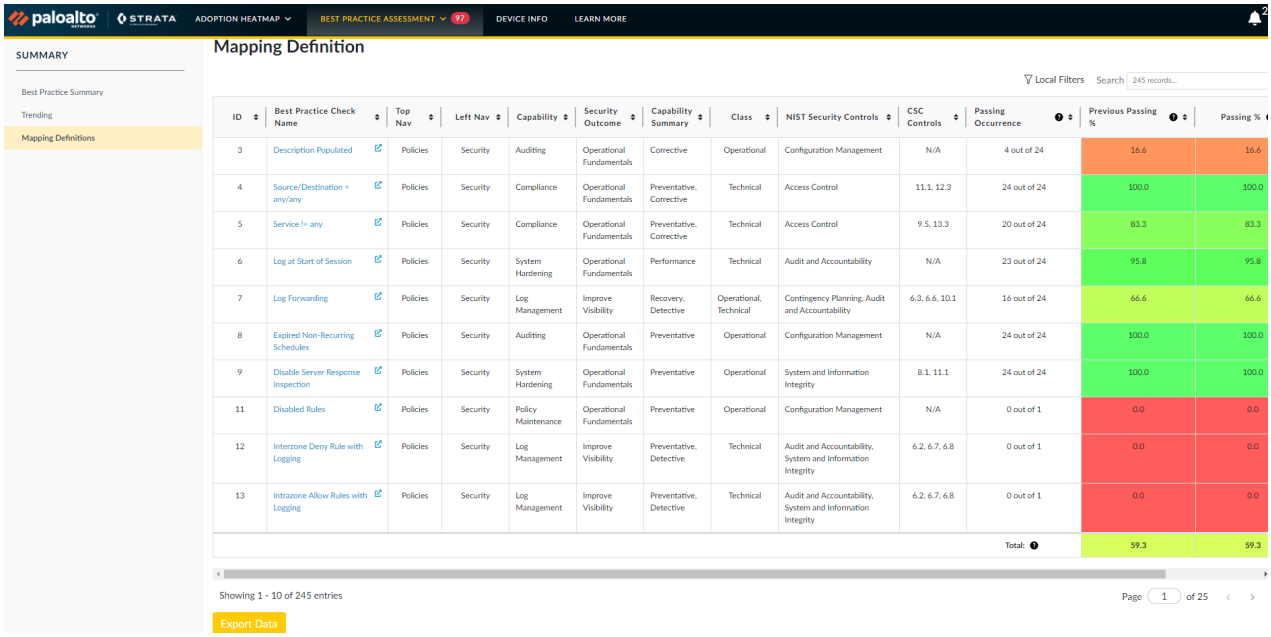
Sélectionnez **Summary** (Résumé) dans le menu **Best Practice Assessment** pour voir le résumé des meilleures pratiques.



Le résumé présente les résultats de la vérification de la configuration des meilleures pratiques correspondant aux catégories de contrôles des normes du secteur, telles que les contrôles de sécurité critiques du Centre pour la sécurité Internet (CIS) et la publication du National Institute of Standards and Technology (NIST) sur les contrôles de sécurité et les procédures d'évaluation. L'objectif de ces informations est de fournir un bon moyen d'apprendre comment les vérifications BPA sont liées aux normes du secteur, et non de servir d'audit.

Comme le Résumé de l'adoption, le Best Practice Summary (Résumé des meilleures pratiques) inclut des mesures indiquant votre taux d'adoption actuel et la progression de l'adoption (entre parenthèses) depuis la dernière génération du BPA sur la configuration de l'équipement.

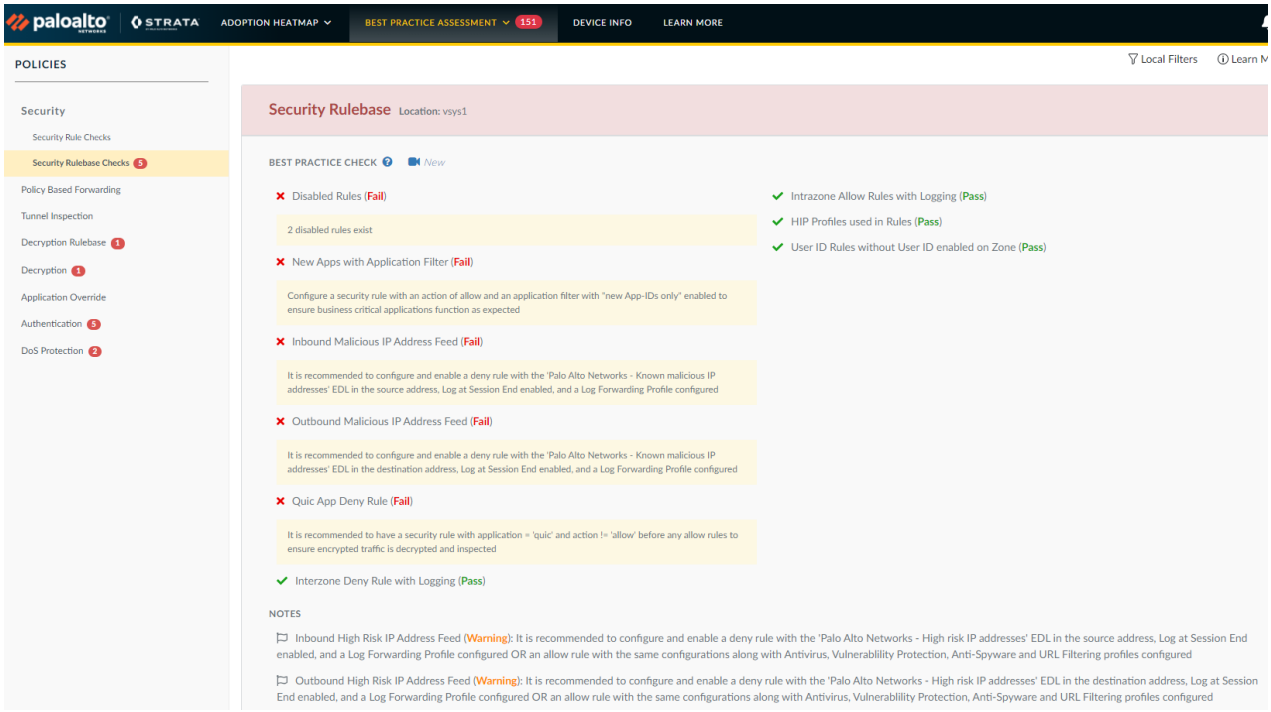
Cliquez sur **Mapping Definitions** (Définitions de mappage) (barre latérale gauche) pour voir une liste complète de toutes les vérifications mappées et de leurs scores individuels. Cliquez sur **Show Filters** (Afficher les filtres) pour définir des filtres, **Apply Filters** (Appliquer les filtres) pour appliquer des filtres au fichier généré et **Export mappings** (Exporter des mappages) pour exporter les mappages dans un fichier .csv.



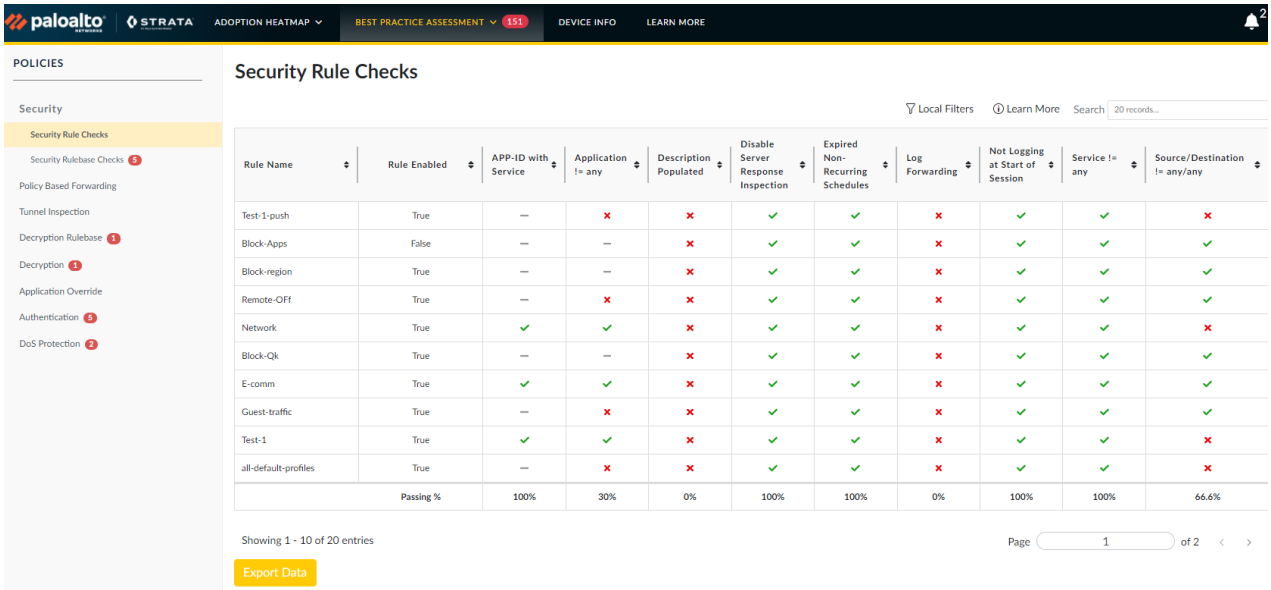
Étape suivante : Examen de la configuration de la politique en matière de meilleures pratiques.

Examen de la configuration de la politique en matière de meilleures pratiques

Best Practice Assessment > **Policies** montre toutes les vérifications relatives aux différents types de politiques de pare-feu et commence sur la page **Security Rulebase checks** (Vérifications de la base de règles de sécurité). **Security Rulebase Checks** (Vérifications de la base de règles de sécurité) résume les résultats de la vérification des meilleures pratiques par groupe d'appareils, avec un statut Pass (Réussite)/Fail (Échec) et des recommandations sur les mesures à prendre pour les échecs de vérification. Cliquez sur l'aide ( ) pour afficher la description et la justification de chaque résultat, ainsi qu'un lien vers la documentation technique comme référence.



Sélectionnez le type de politique que vous voulez examiner dans le menu à gauche pour identifier les améliorations potentielles des règles. Par exemple, **Security Rule Checks** (Vérifications de la règle de sécurité) montre les résultats des vérifications relatives à la règle. Cliquez sur **Local Filters** (Filtres locaux) pour configurer des filtres qui limitent les résultats aux règles pour lesquelles une ou plusieurs vérifications particulières ont échoué. Vous pouvez cliquez sur **Export data** (Exporter les données) pour exporter la liste dans un fichier .csv pour une analyse de la correction.



Lorsque vous examinez les informations sur la **Policy** (Politique), examinez au minimum les éléments suivants pour vous aider à comprendre la portée de la correction de la politique (alternez entre les vues) :

- **Security** (Sécurité) : identifiez les règles qui échouent à la vérification **Source/Destination !=any/any** (Source/Destination != tout/tout).
- **Security** (Sécurité) : identifiez les règles qui échouent à la vérification **App-ID with Service** (App-ID avec service).
- **Security** (Sécurité) : identifiez les règles User-ID qui échouent à la vérification **User-ID Rules without User ID enabled on Zone** (Règles de User-ID sans User-ID activé sur zone).
- **Decryption Rulebase** (Base de règles de décryptage) : vérifications du décryptage du proxy SSH.
- **Decryption** (Décryptage) : chaque règle de politique de décryptage doit avoir un profil de décryptage associé.

> *L'exception est le trafic TLSv1.3 que vous choisissez de ne pas déchiffrer en appliquant une politique de non-décryptage au trafic. Lorsque vous joignez un profil de non-décryptage à la politique, le profil vérifie les informations de certification et bloque les sessions de décryptage qui utilisent de mauvais certificats. Cependant, comme TLSv1.3 crypte les informations de certificat, le pare-feu ne peut pas bloquer le trafic non-décrypté sur la base des informations du certificat, il n'y a donc pas besoin de joindre le profil à une politique.*

- **Application Override** (Contrôle prioritaire sur l'application) : les règles de contrôle prioritaire sur l'application qui utilisent une application personnalisée simple contournent l'inspection de couche 7 du trafic correspondant. Réduisez ou éliminez les règles de contrôle prioritaire sur l'application qui utilisent une application personnalisée simple pour pouvoir procéder à l'Amélioration de la visibilité sur le trafic et inspecter les applications et le contenu que ces règles contrôlent.

Étape suivante : #unique_8.

Hiérarchisation des modifications des meilleures pratiques

La quantité d'informations dans un rapport BPA peut être considérable. Ce chapitre fournit des recommandations pour vous aider à hiérarchiser les améliorations à apporter à votre configuration afin que vous puissiez remédier aux failles de sécurité, commencer par mettre en œuvre les améliorations les plus importantes et progresser vers une meilleure pratique en matière de posture de sécurité.

Les rubriques suivantes traitent de la manière d'améliorer votre posture de sécurité dans l'ordre dans lequel les nouveaux déploiements sont généralement mis en œuvre, en commençant par la gestion, puis la visibilité, le contrôle et l'application. Les déploiements existants ont peut-être déjà atteint une certaine maturité dans chaque domaine.

- Renforcement de la posture de gestion des appareils
- Amélioration de la visibilité sur le trafic
- Mise en œuvre des contrôles initiaux des meilleures pratiques
- Ajustement et amélioration des contrôles des meilleures pratiques

Renforcement de la posture de gestion des appareils

Le renforcement de votre posture de gestion des équipements sécurise le pare-feu en empêchant tout accès non autorisé qui pourrait le compromettre, en réduisant l'impact opérationnel de événements imprévus et en offrant une meilleure visibilité sur le fonctionnement du pare-feu.

- Suivez les meilleures pratiques pour sécuriser l'accès administratif pour empêcher tout accès non autorisé et non sécurisé à l'interface de gestion de l'équipement.
- Procédez au Transfert de tous les journaux du système et de la configuration vers Panorama et aux Solutions de surveillance tierces pour suivre les événements liés au système et les modifications de configuration.
- Procédez à la Création d'un planning de sauvegarde de configuration pour pouvoir ainsi résoudre plus rapidement les problèmes liés à la configuration et les pannes du système.

Après avoir configuré les modifications, procédez à l'Exécution du BPA pour valider les modifications, mesurer les progrès et hiérarchiser les modifications suivantes.

Étape suivante : Amélioration de la visibilité sur le trafic.

Amélioration de la visibilité sur le trafic

Vous ne pouvez pas vous protéger contre les menaces que vous ne voyez pas. Vous devez donc vous assurer de toujours avoir une visibilité complète sur le trafic, sur tous les utilisateurs et toutes les applications. La première étape vers un contrôle informé des politiques est atteinte par l'obtention d'une visibilité complète sur les applications, les contenus et les utilisateurs de votre réseau :

- Maximisez l'adoption du profil de sécurité. Après avoir procédé à l'Examen du résumé de l'adoption et à l'Identification des failles en matière d'adoption, corrigez les failles à l'aide des étapes de transition en toute sécurité pour passer à la mise en œuvre d'un profil de sécurité complet respectant les meilleures pratiques.
- Maximisez l'adoption de la journalisation (notamment le Transfert des journaux) à travers la base de règles de la politique de sécurité pour inspecter *tout* le trafic.
- Procédez à la Configuration des meilleures pratiques pour les mises à jour de contenu dynamiques pour vous assurer que le pare-feu dispose des dernières signatures d'applications et de menaces pour protéger votre réseau et que vous déployez des mises à jour en fonction des exigences de sécurité et de disponibilité de votre réseau.
- Procédez à la Planification du déploiement de votre décryptage SSL en fonction des meilleures pratiques.
- Procédez à l'Activation de User-ID dans les zones utilisateur (zones de confiance internes à partir desquelles les utilisateurs génèrent du trafic) pour mapper le trafic des applications et les menaces associées pour les utilisateurs et les périphériques.

  N'activez pas User-ID dans les zones externes non approuvées. Si vous activez User-ID (ou un sondage du client tel que WMI) sur une zone externe non approuvée, des sondages pourraient être envoyés en dehors de votre réseau protégé, ce qui entraînerait une divulgation des informations sur User-ID telles que le nom de compte du service de l'agent User-ID, du nom de domaine et du hachage du mot de passe crypté, ce qui pourrait permettre à un pirate de compromettre votre réseau.
- Réduisez ou éliminez les règles de contrôle prioritaire sur l'application afin de pouvoir inspecter les applications et le contenu contrôlé par ces règles (une règle de contrôle prioritaire sur l'application est une règle de couche 4 qui ne permet pas au pare-feu d'inspecter le trafic). Pour éliminer le besoin ou réduire la portée des règles de contrôle prioritaire sur l'application de base, procédez comme suit :
  - Confirmez que le cas d'utilisation de la règle existe toujours. Une règle de contrôle prioritaire sur l'application a souvent été créée pour résoudre un problème spécifique lié aux performances, aux décodeurs de protocole ou aux applications inconnues. Au fil du temps, les mises à jour PAN-OS, les mises à jour du contenu ou les mises à niveau matérielles peuvent supprimer le besoin d'avoir certaines règles de contrôle prioritaire sur l'application. Si vous exécutez PAN-OS 9.0 ou version ultérieure sur des pare-feu ou PAN-OS 9.0 ou version ultérieure sur un Panorama gérant des pare-feu exécutant PAN-OS 8.1 (ou version ultérieure), vous pouvez utiliser Policy Optimizer pour transformer la règle en règle de couche 7.
  - Réduisez la portée de la règle de contrôle prioritaire sur l'application afin qu'elle n'affecte que la quantité de trafic la plus faible possible. Les règles définies de manière trop large peuvent avoir un contrôle prioritaire sur plus de trafic que nécessaire ou prévu. Définissez les zones, adresses et/ou ports source et de destination dans chaque règle de contrôle prioritaire sur l'application afin de limiter le plus possible la portée de la règle.
  - Créez des applications personnalisées de couche 7 pour les applications internes.
  - Créez des objets de Service avec valeurs de délai d'expiration personnalisées.
- Procédez à la Planification du déploiement de la protection DoS et de zone et à la Prise de mesures de référence des CPS pour pouvoir définir des seuils raisonnables de protection contre la saturation.

Lorsque vous mettez en œuvre ces fonctionnalités natives App-ID, Content-ID, User-ID et décryptage SSL, le pare-feu obtient une visibilité et peut inspecter tout votre trafic (applications, menaces et contenu) et lie

les événements à l'utilisateur, quels que soient l'emplacement, le type de périphérique, le port, le cryptage ou les techniques d'évasion d'un pirate.

L'amélioration de l'adoption de fonctionnalités telles que le décryptage SSL, la journalisation, la protection contre la saturation, les profils de sécurité, etc., peut entraîner une consommation supplémentaire des ressources de pare-feu. Comprenez la fonctionnalité de vos pare-feu et assurez-vous qu'ils sont correctement dimensionnés pour supporter toute charge supplémentaire. Votre SE ou CE de Palo Alto Networks peut vous aider à dimensionner le déploiement. Vous aurez peut-être également besoin d'espace de stockage supplémentaire dans les journaux.

Après avoir configuré les modifications, procédez à l'Exécution du BPA pour valider les modifications, mesurer les progrès et hiérarchiser les modifications suivantes.

Étape suivante : Mise en œuvre des contrôles initiaux des meilleures pratiques.

Mise en œuvre des contrôles initiaux des meilleures pratiques

Après avoir obtenu une visibilité et une meilleure perspective du trafic sur votre réseau (applications, contenu, menaces et utilisateurs), mettez en œuvre des contrôles stricts pour réduire la surface d'attaque et empêcher les menaces connues et inconnues afin de mener à bien la transition vers une configuration relative aux meilleures pratiques.

- Après avoir procédé à l'Examen du résumé de l'adoption et à l'Identification des failles en matière d'adoption, suivez les étapes de transition en toute sécurité pour passer aux profils de sécurité respectant les meilleures pratiques pour bloquer les menaces et réduire la surface d'attaque, notamment par la mise en place de contrôles stricts dans le centre de données afin de protéger les actifs les plus précieux de votre entreprise.
- Créez des règles de politique de sécurité basées sur une application pour le centre de données et les pare-feu de périmètre ; utilisez les recommandations relatives aux meilleures pratiques en matière de pare-feu de périmètre pour les autres pare-feu ne figurant pas dans le centre de données. Si vous exécutez PAN-OS 9.0 ou version ultérieure sur des pare-feu ou PAN-OS 9.0 ou version ultérieure sur un Panorama gérant des pare-feu exécutant PAN-OS 8.1 (ou version ultérieure), vous pouvez utiliser Policy Optimizer pour convertir les règles basées sur un port en règles basées sur une application.
- Procédez à la Création de politiques d'accès basées sur un utilisateur.
- Procédez au Déploiement des profils de protection de zone respectant les meilleures pratiques à toutes les zones.
- Procédez au Déploiement du décryptage SSL pour que le pare-feu puisse obtenir une visibilité (déchiffrer) et inspecter le trafic chiffré.

Une fois que vous avez mis en œuvre les fonctionnalités de contrôle, le pare-feu peut analyser tout le trafic autorisé et détecter et bloquer les exploitations de vulnérabilité des couches d'application et réseau, les dépassements de capacité de la mémoire tampon, les attaques DoS, les analyses de ports et les variantes de logiciels malveillants connues et inconnues. Le pare-feu contrôle l'accès aux applications et aux utilisateurs, ainsi que le blocage des applications malveillantes et indésirables.

Après avoir configuré les modifications, procédez à l'Exécution du BPA pour valider les modifications, mesurer les progrès et hiérarchiser les modifications suivantes.

Étape suivante : Ajustement et amélioration des contrôles des meilleures pratiques.

Ajustement et amélioration des contrôles des meilleures pratiques

Après avoir procédé à la mise en place du contrôle sur le trafic de votre réseau (applications, contenu, menaces et utilisateurs), commencez à ajuster les contrôles et à mettre en œuvre des fonctionnalités supplémentaires pour améliorer votre posture de sécurité.

- Si vous n'avez pas converti les applications internes en applications personnalisées pour obtenir une visibilité et un contrôle du trafic, convertissez les applications internes en applications personnalisées.
- Adaptez les profils de sécurité aux meilleures pratiques après avoir utilisé les étapes de transition sécurisées pour commencer la transition vers les profils de meilleures pratiques.
- Procédez au blocage d'adresses IP malveillantes connues en fonction des informations sur les menaces de Palo Alto Networks et des flux tiers réputés.
- Déployez GlobalProtect ou GlobalProtect Cloud Service pour étendre la plateforme de sécurité nouvelle génération aux utilisateurs et aux périphériques, quel que soit l'endroit où ils se trouvent.
- Activez la prévention contre le vol d'identifiants.
- Configurez l'authentification à plusieurs facteurs basée sur le réseau.

Ensuite : Procédez à l'exécution du BPA pour valider les modifications, mesurer les progrès et hiérarchiser les modifications suivantes, apprenez-en plus sur les meilleures pratiques et sur les nombreuses fonctionnalités de sécurité de Panorama et des pare-feu nouvelle génération de PAN-OS.