paloalto
TECHDOCS

Démarrage avec le BPA

10.2

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to 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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Last Revised

May 13, 2022

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 (Cartes thermiques) pour en savoir plus sur les cartes thermiques et profitez de la vidéothèque BPA et de la vidéothèque BPA+ pour en savoir plus sur l'outil.

Dans les environnements gérés par Panorama, Panorama peut gérer un grand nombre de pare-feu nouvelle génération. Devez-vous exécuter le BPA sur Panorama ou sur chaque pare-feu individuel ? Le compromis est la rapidité et la commodité par comparaison à l'exhaustivité.

L'exécution du BPA sur Panorama est rapide et pratique ; cela permet d'évaluer la plupart des capacités des pare-feu gérés, mais cela n'examine pas les remplacements de pare-feu locaux.

L'exécution du BPA sur chaque pare-feu géré permet d'évaluer la configuration complète (y compris les remplacements locaux), mais est plus chronophage.

La méthode la plus pratique consiste à exécuter d'abord le BPA sur Panorama. Examinez les résultats afin d'identifier des appareils gérés particuliers, puis exécutez le BPA sur ces appareils. Cette méthode vous permet de gagner du temps et de vous concentrer sur les informations pertinentes qui vous permettent d'améliorer votre posture de sécurité.

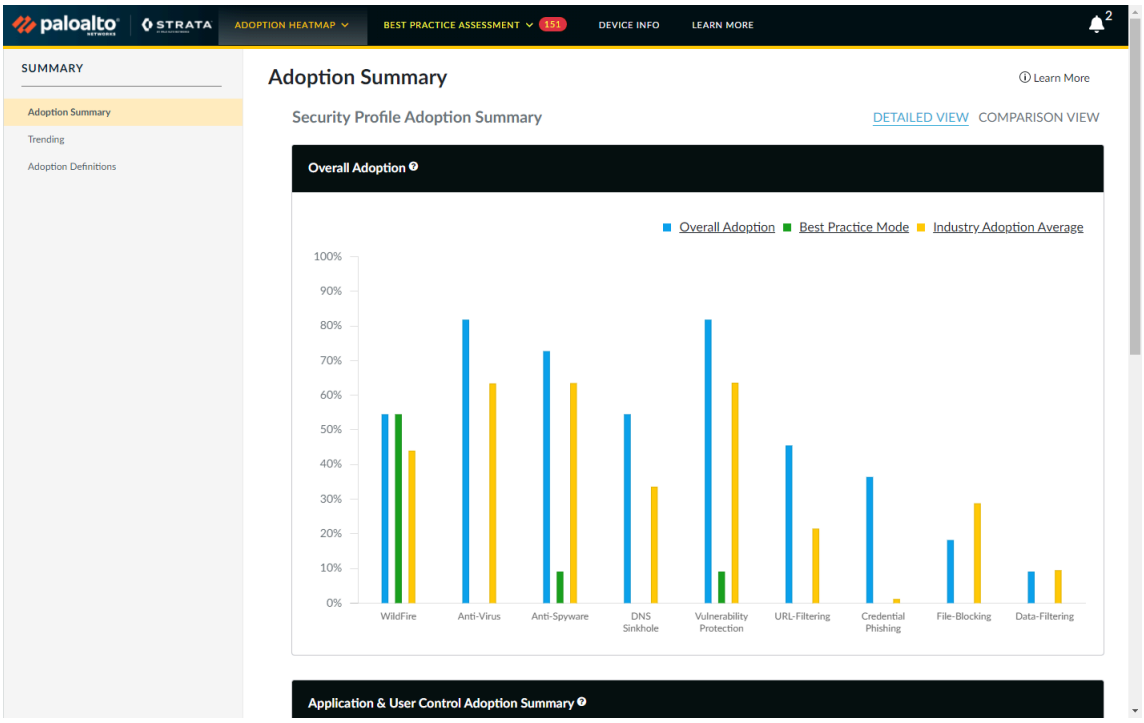
Examinez et analysez les informations contenues dans les onglets Heatmap (Carte thermique) pour identifier les failles dans l'adoption des fonctionnalités de sécurité et déterminer ce que vous souhaitez améliorer :

- Examen du résumé de l'adoption
- Identification des failles en matière d'adoption

- Identification des règles à améliorer

Examen du résumé de l'adoption

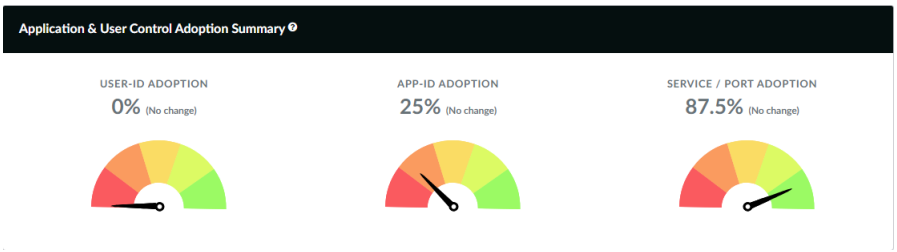
Après que vous ou votre représentant de Palo Alto Networks avez procédé à l'exécution du BPA, le rapport HTML qui en résulte s'ouvre sur la page Adoption Heatmap (Carte thermique relative à l'adoption), dans le Adoption Summary (Résumé de l'adoption). La vue Adoption Summary (Résumé de l'adoption) fournit 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.

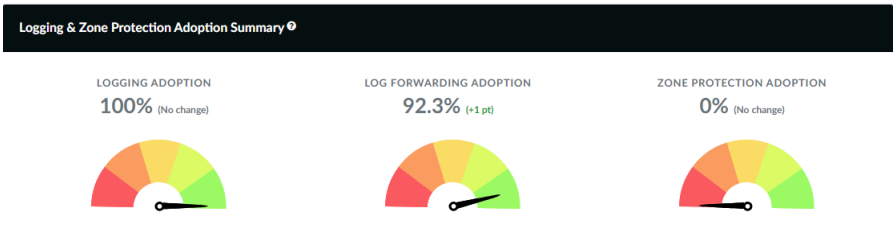


App-ID Adoption (Adoption d'App-ID) : adoption d'App-ID dans les règles de politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles d'autorisation avec une ou plusieurs applications définies (l'application n'est pas **any** (tout)). Le BPA ne compte pas les règles désactivées.

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.



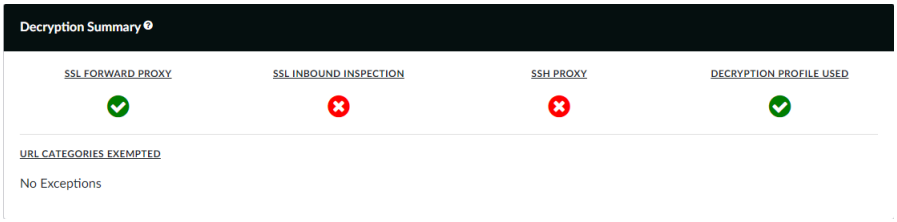
Logging Adoption (Adoption de la journalisation) : adoption de **Log at Session End** (Journaliser à la fin de la session) dans les règles de la politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles avec **Log at Session End** (Journaliser à la fin de la session) activée.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

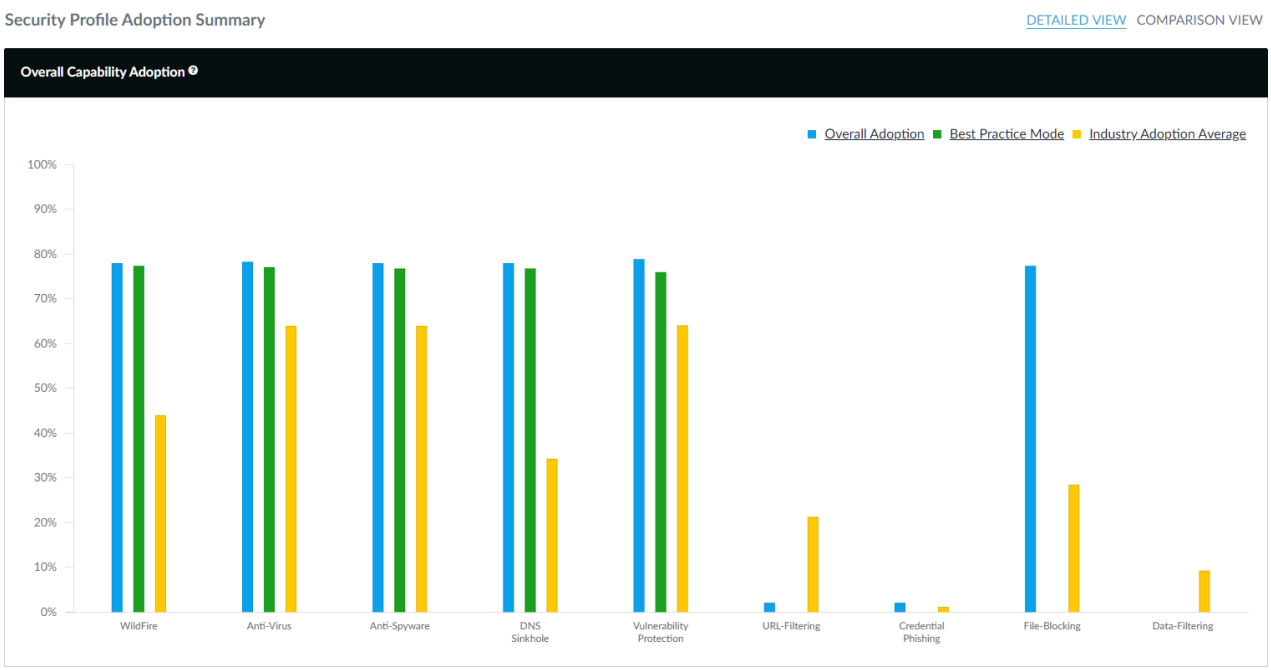
Ensuite : Identification des failles en matière d'adoption pour comprendre les domaines dans lesquels vous pouvez améliorer la sécurité.

Identification des failles en matière d'adoption

Les options Adoption Heatmap (Carte thermique relative à l'adoption des fonctionnalités) vous indiquent les domaines dans lesquels votre politique de sécurité est forte et les domaines dans lesquels il existe des failles dans l'adoption des fonctionnalités de la politique de sécurité que vous pouvez chercher à améliorer. Pour obtenir une visibilité maximale sur le trafic et une protection maximale contre les attaques, définissez des objectifs pour l'adoption des fonctionnalités de sécurité et utilisez les recommandations suivantes comme base de référence respectant les meilleures pratiques. Évaluez votre posture actuelle par rapport à la situation de base afin d'identifier les failles dans l'adoption des fonctionnalités de la politique de sécurité.

Les Adoption Heatmaps (Cartes thermiques) relatives à l'adoption des fonctionnalités aident à identifier les dispositifs, les zones et les domaines dans lesquels vous pouvez améliorer l'adoption des fonctionnalités de la politique de sécurité. Vous pouvez examiner les informations sur l'adoption par Device Group (Groupe d'appareils), Serial Number & Vsys (Numéro de série et vsys), Zones, Areas of Architecture (Zones d'architecture), Tags (Étiquettes), Rule Details (Détails de la règle) et Zone Mappings (Mappages de la zone). Les **filtres locaux** filtrent par Device Groupe (Groupe d'appareils), Source Area of Architecture (Zone source d'architecture), Destination Area of Architecture (Zone de destination de l'architecture), Target (Cible), Source Zone (Zone source), Destination Zone (Zone de destination) et Tags (Étiquettes) pour réduire la portée de la recherche et identifier les failles. L'exemple suivant montre la Adoption Heatmap (Carte thermique relative à l'adoption) par zone d'architecture (**Adoption Heatmap** > **Areas of Architecture** :

Dans **Adoption Heatmap** > **Summary**, cliquez sur Adoption Summary (Résumé de l'adoption) pour contrôler les taux d'adoption des fonctionnalités suivantes. Utilisez les recommandations comme critères d'identification des failles. Si le taux d'adoption réel ne correspond pas aux recommandations, envisagez de remédier à la faille en procédant comme suit :



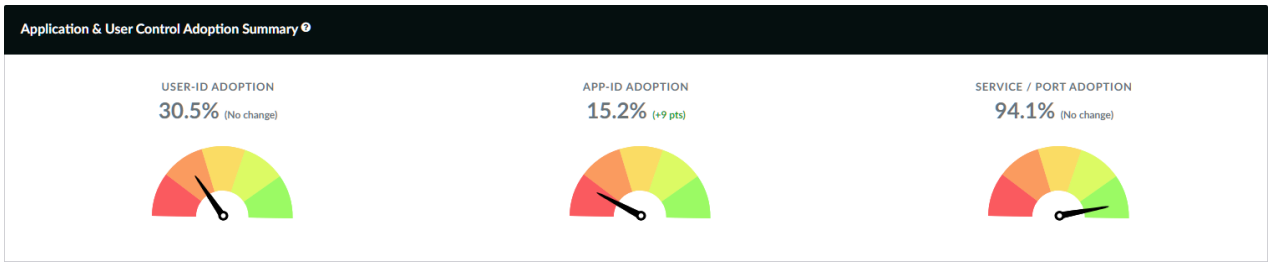
- Appliquez les profils de sécurité WildFire, Antivirus, Antispyware, Vulnerability Protection (Protection contre les vulnérabilités) et File Blocking (Blocage des fichiers) à toutes les règles autorisant le trafic avec un objectif d'adoption de 100 % ou presque. Si vous n'appliquez aucun profil à une règle d'autorisation, vérifiez qu'il existe une bonne raison professionnelle de ne pas appliquer le profil.

  La configuration de profils de sécurité sur toutes les règles d'autorisation permet au pare-feu d'inspecter le trafic décrypté à la recherche de menaces, quels que soient l'application ou le service/port. Après la mise à jour de la configuration, exécutez le BPA pour mesurer les progrès et capter les nouvelles règles auxquelles aucun profil de sécurité n'est associé.

  Vous pouvez appliquer des profils WildFire à des règles sans licence WildFire. La couverture est limitée aux fichiers PE, mais cela fournit néanmoins une visibilité utile sur les fichiers malveillants inconnus.

- Dans le profil Antispyware, appliquez DNS Sinkhole à toutes les règles afin d'empêcher les hôtes internes compromis d'envoyer des requêtes DNS pour les domaines malveillants et personnalisés, d'identifier et de suivre les hôtes potentiellement compromis et d'éviter les interruptions de l'inspection DNS. L'activation de DNS Sinkhole protège votre réseau sans affecter la disponibilité. Vous pouvez et devriez donc l'activer immédiatement.
- Appliquez la protection URL Filtering (Filtrage des URL) et Credential Phishing Prevention (Prévention de l'hameçonnage des informations d'identification) à tout le trafic Internet sortant.

Dans Application & User Control Adoption Summary (Résumé de l'adoption des contrôles d'applications et d'utilisateurs) de Adoption Summary (Résumé de l'adoption), vérifiez les taux d'adoption des fonctionnalités suivantes. Utilisez les recommandations comme critères d'identification des failles. Si le taux d'adoption réel ne correspond pas aux recommandations, envisagez de remédier à la faille en procédant comme suit :

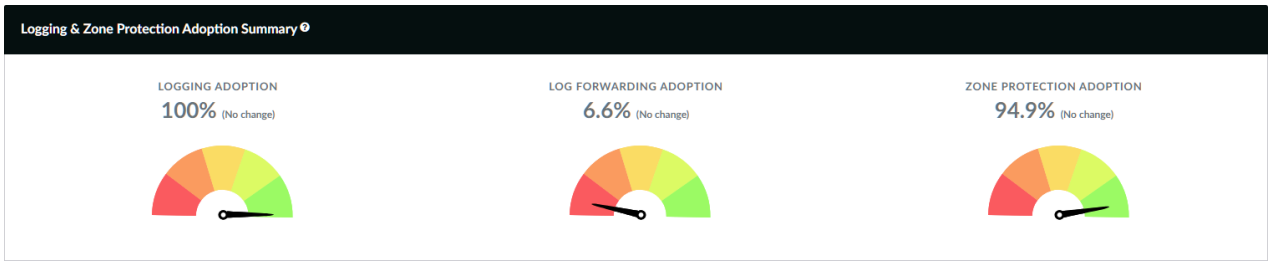


- Appliquez App-ID à 100 % des règles ou le plus près possible de 100 % des règles. Appliquez User-ID à toutes les règles avec des zones sources ou des plages d'adresses ayant une présence utilisateur (certaines zones peuvent ne pas avoir de sources utilisateur ; par exemple, les sources des zones de centre de données doivent être des serveurs et non des utilisateurs). Utilisez App-

ID et User-ID pour créer des politiques autorisant les utilisateurs appropriés sur les applications autorisées (et tolérées). Bloquez explicitement les applications malveillantes et indésirables.

- Ciblez une adoption de service/port à 100 % ou près de 100 %. N'autorisez pas les applications sur des ports non standard à moins que cela ne soit justifié par des raisons professionnelles.

Dans Logging & Zone Protection (Protection de zone et de la journalisation) de la section Adoption Summary (Résumé de l'adoption), vérifiez les taux d'adoption des fonctionnalités suivantes. Utilisez les recommandations comme critères d'identification des failles. Si le taux d'adoption réel ne correspond pas aux recommandations, envisagez de remédier à la faille en procédant comme suit :



- Ciblez une adoption à 100 % ou près de 100 % pour Logging Adoption (Adoption de la journalisation) et Log Forwarding Adoption (Adoption du transfert de journaux).
- Configurez les profils de protection de zone sur toutes les zones.

En résumé :

Fonctionnalité	Objectif d'adoption
WildFire	Le plus près possible de 100 % des règles de la politique de sécurité
Antivirus	Le plus près possible de 100 % des règles de la politique de sécurité
Antispyware	Le plus près possible de 100 % des règles de la politique de sécurité
Vulnérabilité	Le plus près possible de 100 % des règles de la politique de sécurité

Fonctionnalité	Objectif d'adoption
Blocage des fichiers	Le plus près possible de 100 % des règles de la politique de sécurité
URL Filtering (Filtrage des URL) et Credential Phishing Prevention (Prévention de l'hameçonnage des informations d'identification)	Tout le trafic Internet sortant
App-ID	Le plus près possible de 100 % des règles de la politique de sécurité
ID utilisateur	Toutes les règles avec des zones sources ou des plages d'adresses ayant une présence utilisateur
Service/port	Le plus près possible de 100 % des règles de la politique de sécurité
Journalisation	Le plus près possible de 100 % des règles de la politique de sécurité
Transfert des journaux	Le plus près possible de 100 % des règles de la politique de sécurité
Zone protection (Protection de zones)	Toutes les zones

Lorsque vous affichez la vue Adoption Heatmap (Carte thermique relative à l'adoption), utilisez **les filtres locaux** pour réduire la portée des résultats. Utilisez les informations obtenues pour identifier les failles dans les fonctionnalités de la politique de sécurité, les comparer aux critères d'identification des failles et affiner ou établir de nouveaux critères d'identification des failles pour une enquête plus approfondie. Par exemple, pour créer un filtre affichant l'adoption des règles contrôlant le trafic sur la Area of Architecture (Zone d'architecture) Internet, procédez comme suit :

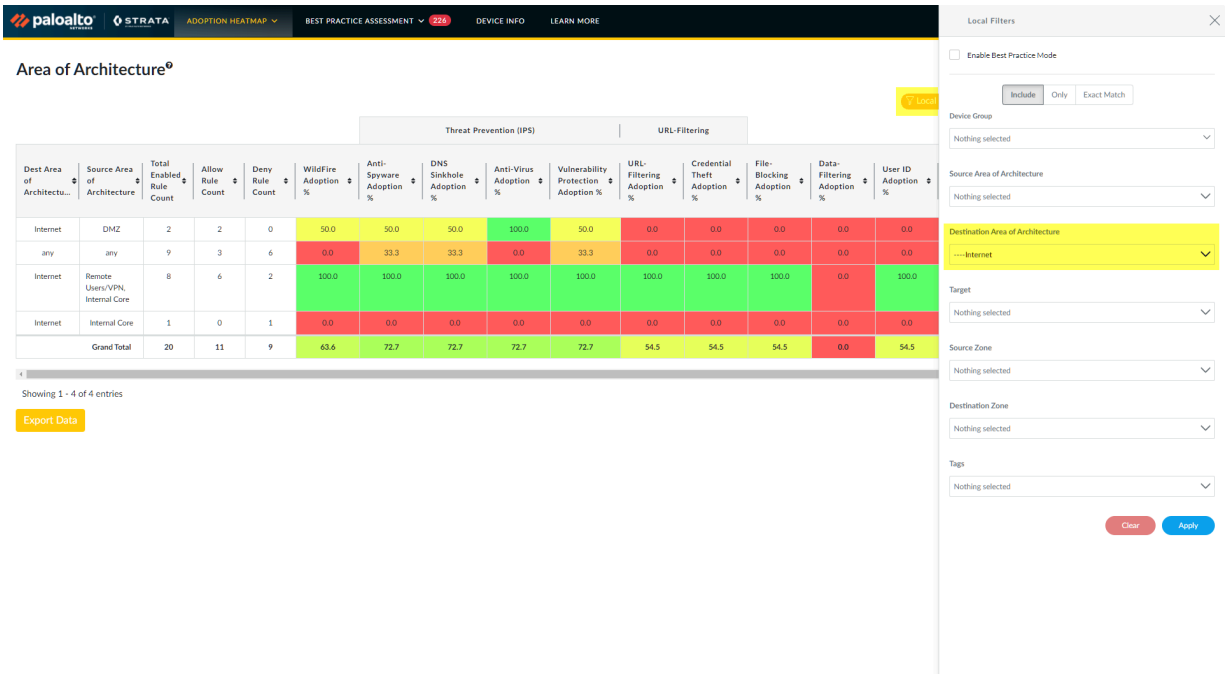
STEP 1 | Sélectionnez **Adoption Heatmap** > **Areas of Architecture**.

STEP 2 | Cliquez sur **Local Filters** (Filtres locaux) pour développer les options de filtrage.

STEP 3 | Définissez la **Destination Area of Architecture** (Zone d'architecture de destination) sur **Internet**.

STEP 4 | Cliquez sur **Apply (Appliquer)**.

Le BPA filtre les résultats :



Interprétez les résultats en fonction de vos objectifs et critères de sécurité. Par exemple, si votre objectif est d'appliquer WildFire à 100 % de vos règles d'autorisation, la carte thermique filtrée révèle que seulement 50 % de vos règles d'autorisation DMZ ont des profils WildFire. Vous avez donc identifié une faille à améliorer.

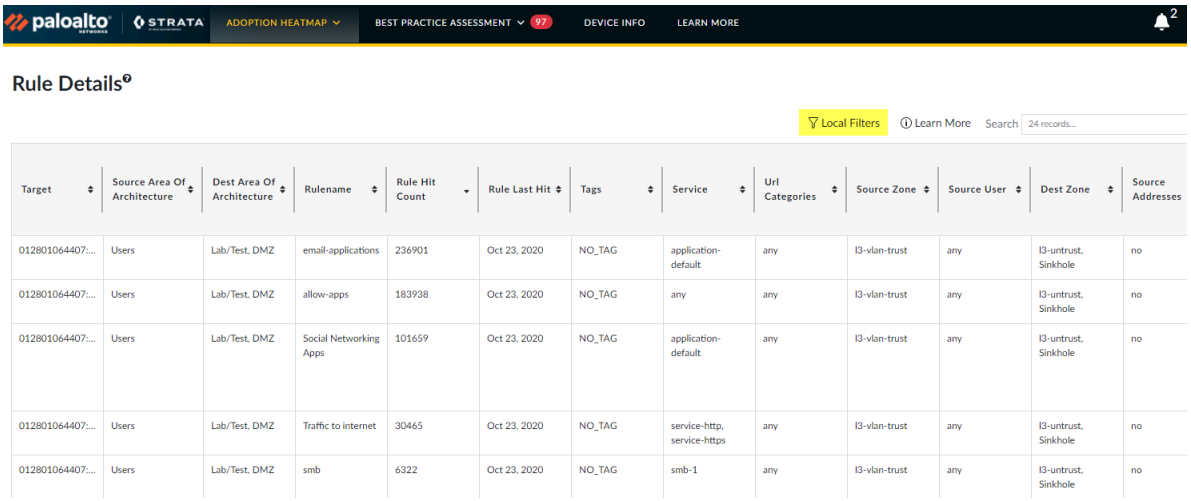
STEP 5 | Ensuite : Identification des règles à améliorer.

Identification des règles à améliorer

Une fois que vous avez identifié une faille dans l'adoption des fonctionnalités de la politique de sécurité, utilisez la vue **Adoption Heatmap** > **Rule Detail**pour répertorier les règles qui nécessitent une enquête ou une correction supplémentaire. Configurez **Local Filters** (Filtres locaux) pour correspondre aux critères d'identification des failles que vous avez élaborés lorsque vous avez procédé à l'identification des failles en matière d'adoption. Des listes de règles que vous pouvez exporter et transférer à l'équipe opérationnelle chargée de la politique de sécurité du pare-feu s'affichent alors.

Par exemple, pour créer un filtre Rule Detail (Détail de la règle) afin d'identifier les règles qui autorisent tout le trafic et pour lesquelles aucun profil de protection contre les vulnérabilités n'a été configuré, procédez comme suit :

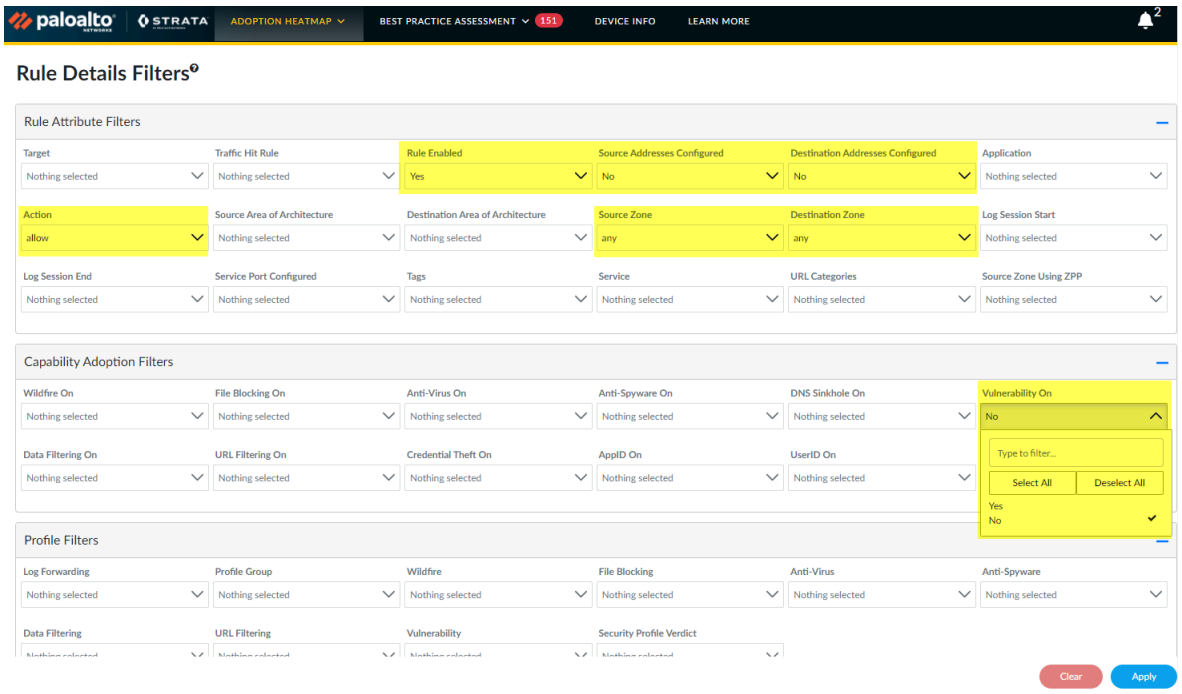
STEP 1 | À partir du menu Adoption Heatmap (Carte thermique relative à l'adoption), sélectionnez **Rule Detail** (Détails de la règle) pour voir la page Rule Details (Détails des règles).



Target	Source Area Of Architecture	Dest Area Of Architecture	Rulename	Rule Hit Count	Rule Last Hit	Tags	Service	Url Categories	Source Zone	Source User	Dest Zone	Source Addresses
012801064407:...	Users	Lab/Test, DMZ	email-applications	236901	Oct 23, 2020	NO_TAG	application-default	any	l3-vlan-trust	any	l3-untrust, Sinkhole	no
012801064407:...	Users	Lab/Test, DMZ	allow-apps	183938	Oct 23, 2020	NO_TAG	any	any	l3-vlan-trust	any	l3-untrust, Sinkhole	no
012801064407:...	Users	Lab/Test, DMZ	Social Networking Apps	101659	Oct 23, 2020	NO_TAG	application-default	any	l3-vlan-trust	any	l3-untrust, Sinkhole	no
012801064407:...	Users	Lab/Test, DMZ	Traffic to internet	30465	Oct 23, 2020	NO_TAG	service-http, service-https	any	l3-vlan-trust	any	l3-untrust, Sinkhole	no
012801064407:...	Users	Lab/Test, DMZ	smb	6322	Oct 23, 2020	NO_TAG	smb-1	any	l3-vlan-trust	any	l3-untrust, Sinkhole	no

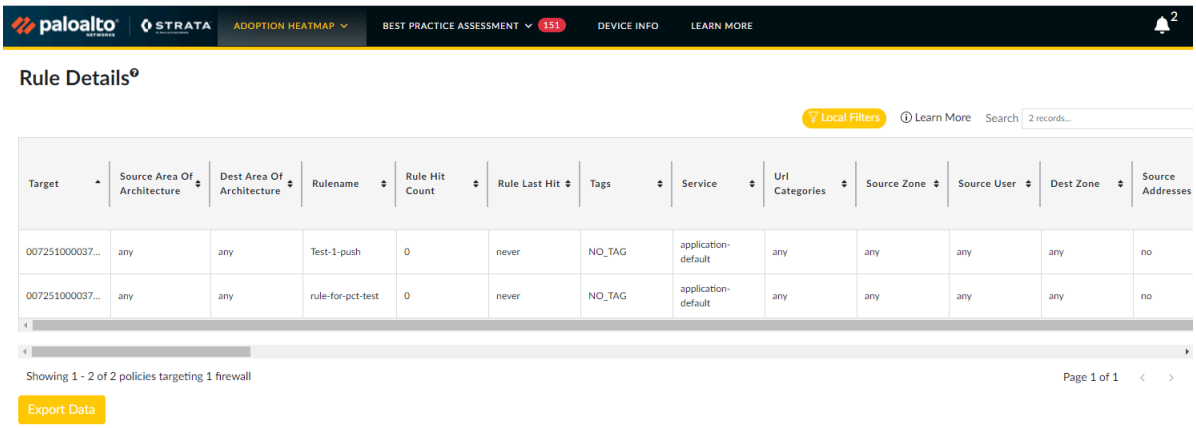
STEP 2 | Cliquez sur **Local Filters** (Filtres locaux) pour voir les options de filtre, puis sélectionnez les filtres suivants :

- Source Zone (Zone source) = **any** (tout)
- Destination Zone (Destination source) = **any** (tout)
- Source Address Configured (Adresse source configurée) = **No** (non)
- Destination Address Configured (Adresse de destination configurée) = **No** (non)
- Action = **allow** (autoriser)
- Rule Enabled (Règle activée) = **Yes** (oui)
- Vulnerability On (Vulnérabilité activée) = **No** (non)



STEP 3 | Cliquez sur **Apply Filter** (Appliquer le filtre).

Le BPA répertorie les règles correspondant aux filtres :



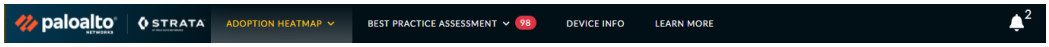
STEP 4 | Pour exporter la liste des règles filtrées dans un fichier .csv, cliquez sur **Export data** (Exporter les données).

STEP 5 | Ensuite : Évaluation de la configuration des meilleures pratiques.

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 et 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.

Dans les environnements gérés par Panorama, Panorama peut gérer un grand nombre de pare-feu nouvelle génération. Devez-vous exécuter le BPA sur Panorama ou sur chaque pare-feu individuel ? Le compromis est la rapidité et la commodité par comparaison à l'exhaustivité.

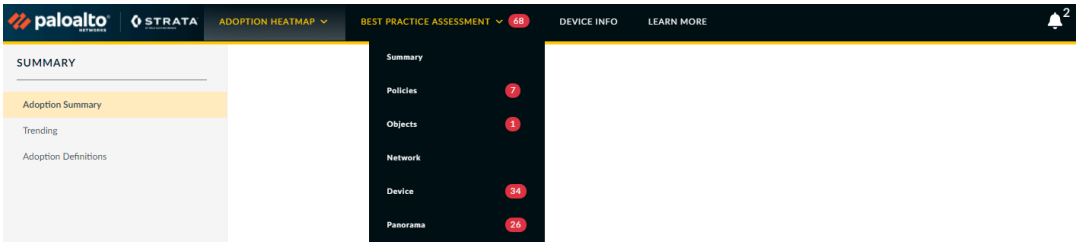
L'exécution du BPA sur Panorama est rapide et pratique ; cela permet d'évaluer la plupart des capacités des pare-feu gérés, mais cela n'examine pas les remplacements de pare-feu locaux.

L'exécution du BPA sur chaque pare-feu géré permet d'évaluer la configuration complète (y compris les remplacements locaux), mais est plus chronophage.

La méthode la plus pratique consiste à exécuter d'abord le BPA sur Panorama. Examinez les résultats afin d'identifier des appareils gérés particuliers, puis exécutez le BPA sur ces appareils. Cette méthode vous permet de gagner du temps et de vous concentrer sur les informations pertinentes qui vous permettent d'améliorer votre posture de sécurité.

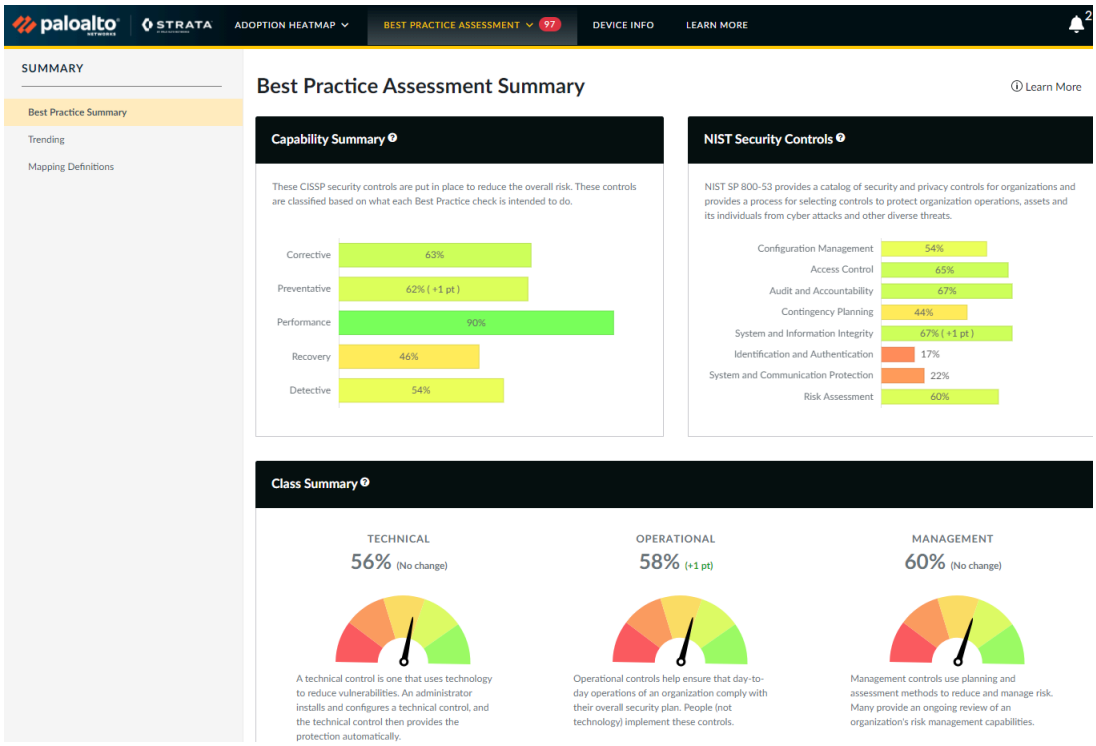
Examinez et analysez les informations pour trouver les domaines à améliorer sur lesquels vous concentrer :

- Examen du résumé des meilleures pratiques
- Examen de la configuration de la politique en matière de meilleures pratiques
- Examen de la configuration des objets de meilleures pratiques
- Examen de la configuration réseau des meilleures pratiques
- Examen de la configuration de la gestion des périphériques et de Panorama, relative aux meilleures pratiques



Examen du résumé des meilleures pratiques

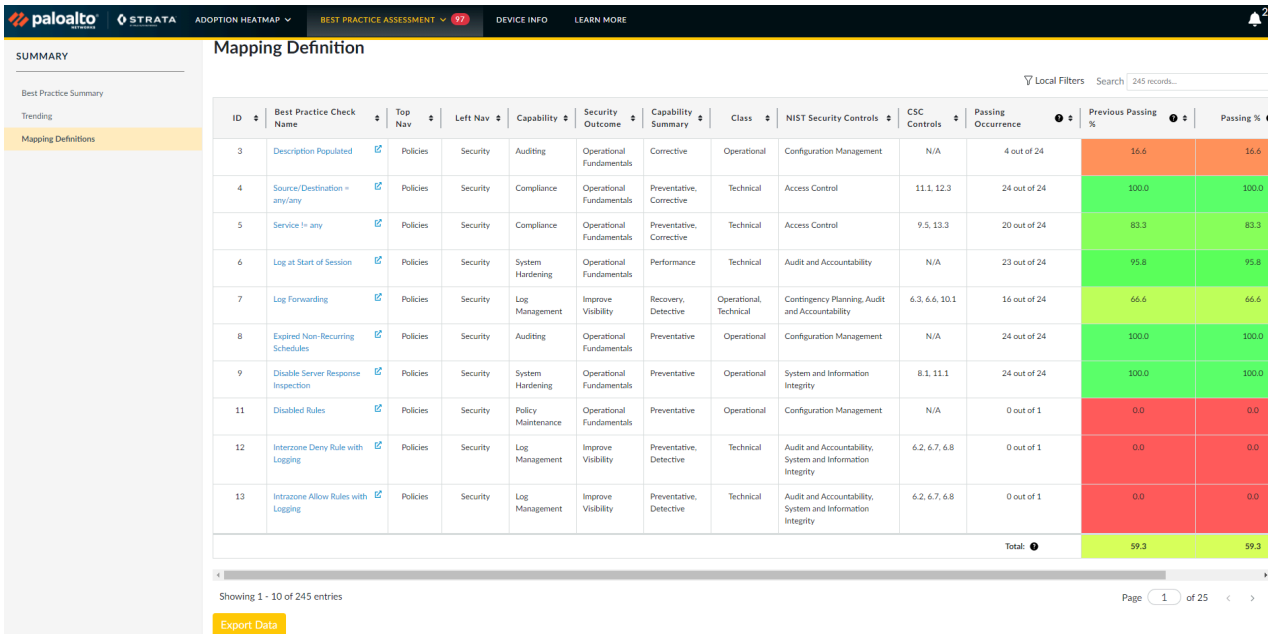
Sélectionnez **Summary** (Résumé) dans le menu **Best Practice Assessment** pour voir le résumé des meilleures pratiques.



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.

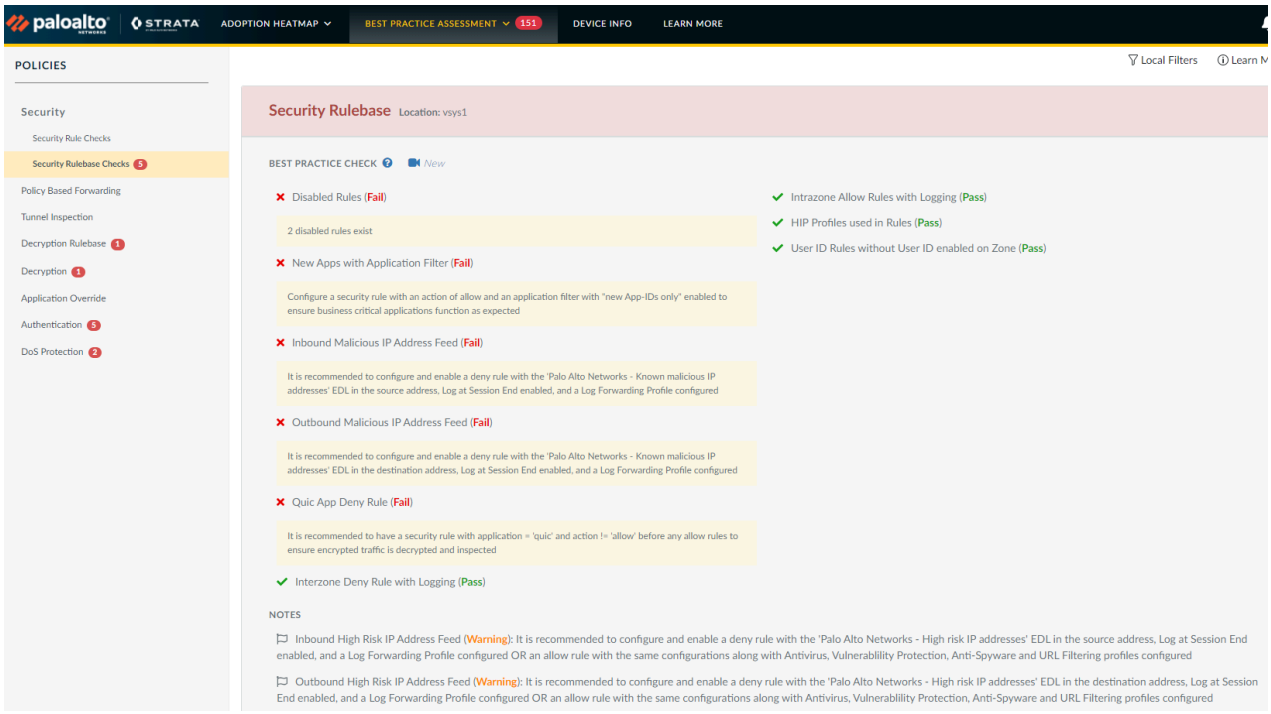


ID	Best Practice Check Name	Top Nav	Left Nav	Capability	Security Outcome	Capability Summary	Class	NIST Security Controls	CSC Controls	Passing Occurrence	Previous Passing %	Passing %
3	Description Populated	Policies	Security	Auditing	Operational Fundamentals	Corrective	Operational	Configuration Management	N/A	4 out of 24	16.6	16.6
4	Source/Destination = any/any	Policies	Security	Compliance	Operational Fundamentals	Preventative, Corrective	Technical	Access Control	11.1, 12.3	24 out of 24	100.0	100.0
5	Service != any	Policies	Security	Compliance	Operational Fundamentals	Preventative, Corrective	Technical	Access Control	9.5, 13.3	20 out of 24	83.3	83.3
6	Log at Start of Session	Policies	Security	System Hardening	Operational Fundamentals	Performance	Technical	Audit and Accountability	N/A	23 out of 24	95.8	95.8
7	Log Forwarding	Policies	Security	Log Management	Improve Visibility	Recovery, Detective	Operational, Technical	Contingency Planning, Audit and Accountability	6.3, 6.6, 10.1	16 out of 24	66.6	66.6
8	Expired Non-Recurring Schedules	Policies	Security	Auditing	Operational Fundamentals	Preventative	Operational	Configuration Management	N/A	24 out of 24	100.0	100.0
9	Disable Server Response Inspection	Policies	Security	System Hardening	Operational Fundamentals	Preventative	Operational	System and Information Integrity	8.1, 11.1	24 out of 24	100.0	100.0
11	Disabled Rules	Policies	Security	Policy Maintenance	Operational Fundamentals	Preventative	Operational	Configuration Management	N/A	0 out of 1	0.0	0.0
12	Interzone Deny Rule with Logging	Policies	Security	Log Management	Improve Visibility	Preventative, Detective	Technical	Audit and Accountability, System and Information Integrity	6.2, 6.7, 6.8	0 out of 1	0.0	0.0
13	Intrazone Allow Rules with Logging	Policies	Security	Log Management	Improve Visibility	Preventative, Detective	Technical	Audit and Accountability, System and Information Integrity	6.2, 6.7, 6.8	0 out of 1	0.0	0.0
										Total:	59.3	59.3

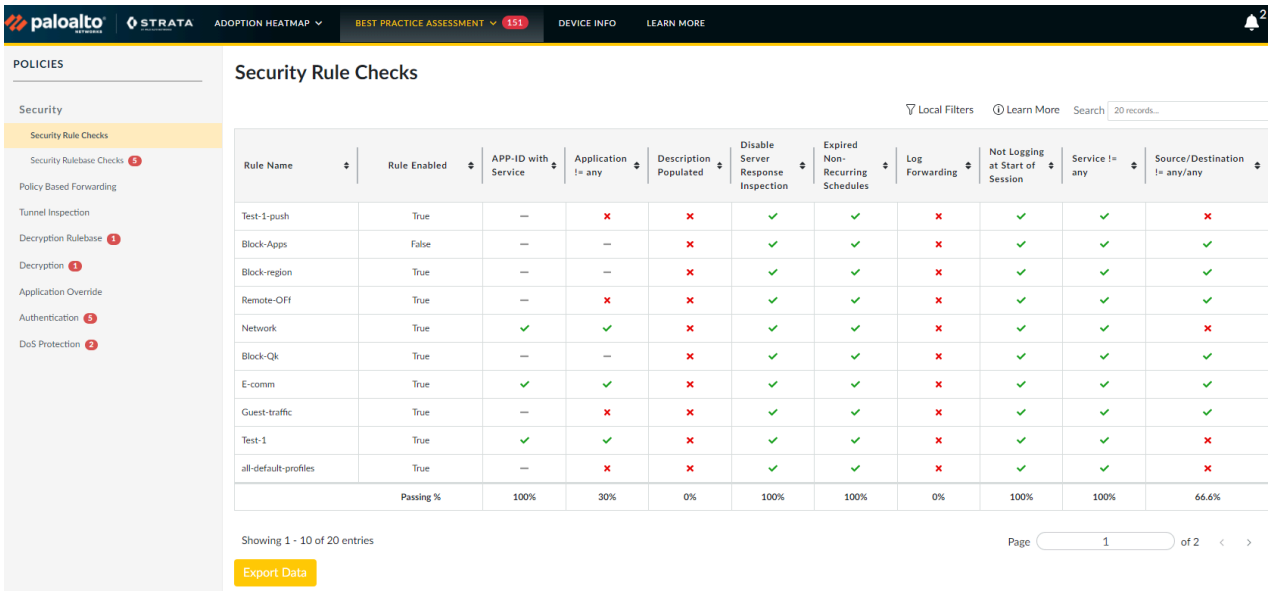
Ensuite : Examen de la configuration de la politique en matière de meilleures pratiques.

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.

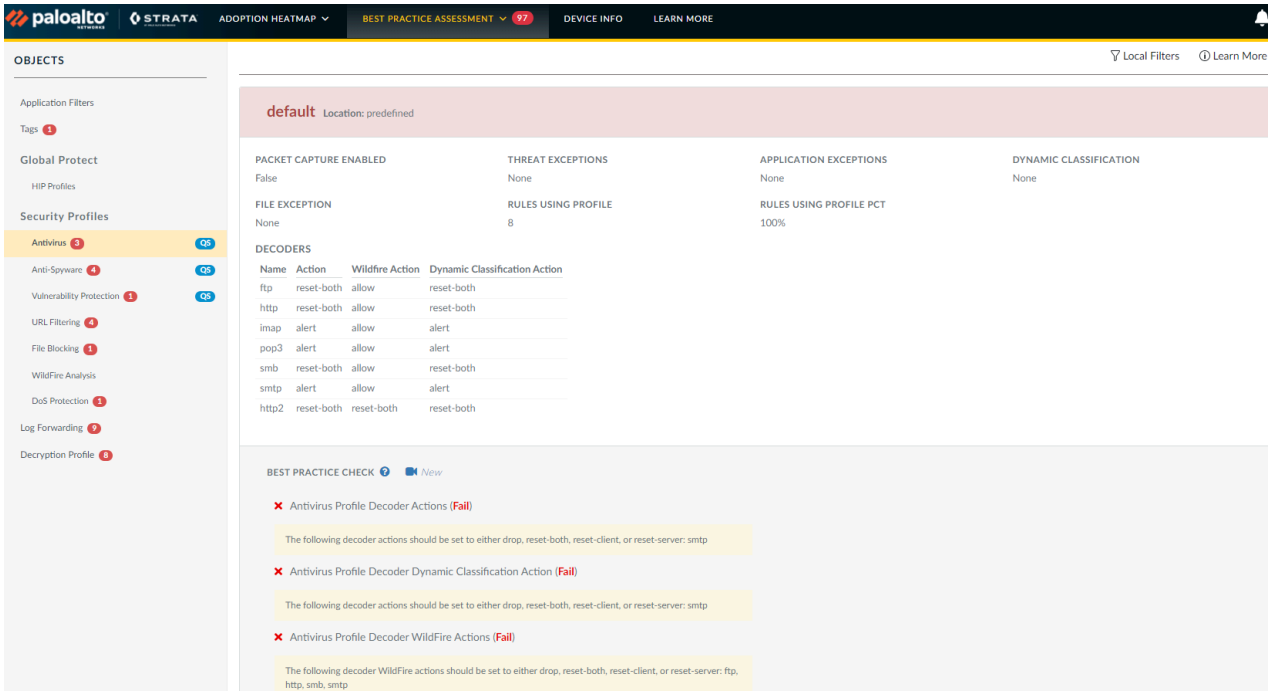
  L'exception est le trafic TLSv1.3 que vous choisissez de ne pas déchiffrer en appliquant une politique de non-décryptage au trafic. Lorsque vous joignez un profil de non-décryptage à la politique, le profil vérifie les informations de certification et bloque les sessions de décryptage qui utilisent de 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 simple propre à l'entreprise pour pouvoir Amélioration de la visibilité sur le trafic et inspecter les applications et le contenu que ces règles contrôlent.

Ensuite : Examen de la configuration des objets de meilleures pratiques.

Examen de la configuration des objets de meilleures pratiques

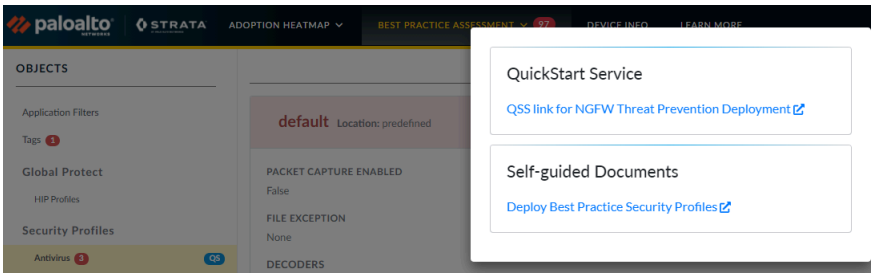
Best Practice Assessment > **Objects** montre toutes les vérifications liées aux différents types d'objet de pare-feu, et commence sur la page **Application Filters** (Filtres d'application). Sélectionnez l'objet à examiner pour comprendre la configuration existante et identifier les failles potentielles dans la configuration des meilleures pratiques liée aux Application Filters (Filtres d'application), Tags (Balises), GlobalProtect, Security Profiles (Profils de sécurité), Log Forwarding (Transfert des journaux) et Decryption profiles (Profil de décryptage). L'exemple suivant montre le résultat lorsque vous sélectionnez l'objet du profil de sécurité antivirus.



Pour chaque profil antivirus, le rapport indique la configuration actuelle et le nombre de règles utilisant le profil. Le rapport affiche les résultats de la vérification des meilleures pratiques en dessous de la configuration actuelle avec le statut Pass (Réussite)/Fail (Échec) et des recommandations pour les échecs de vérification des meilleures pratiques. Cliquez sur l'aide pour afficher la justification de chaque vérification et sur les liens vers la documentation sur les meilleures pratiques.

Lorsqu'une ou plusieurs vérifications échouent, l'intitulé du profil devient rouge. Le rapport répertorie les profils inutilisés en bas avec un intitulé jaune.

Le bouton « QS » situé à côté de certains liens des pages de profil à gauche de l'écran vous redirige vers les options QuickStart Service. L'option **QuickStart Service** vous permet d'améliorer vos performances de sécurité et d'investissements en vous aidant à planifier et à intégrer votre pare-feu en tant que plate-forme. Les **Self-guided Documents** (Documents didactiques) vous aident à comprendre, créer et déployer l'objet.



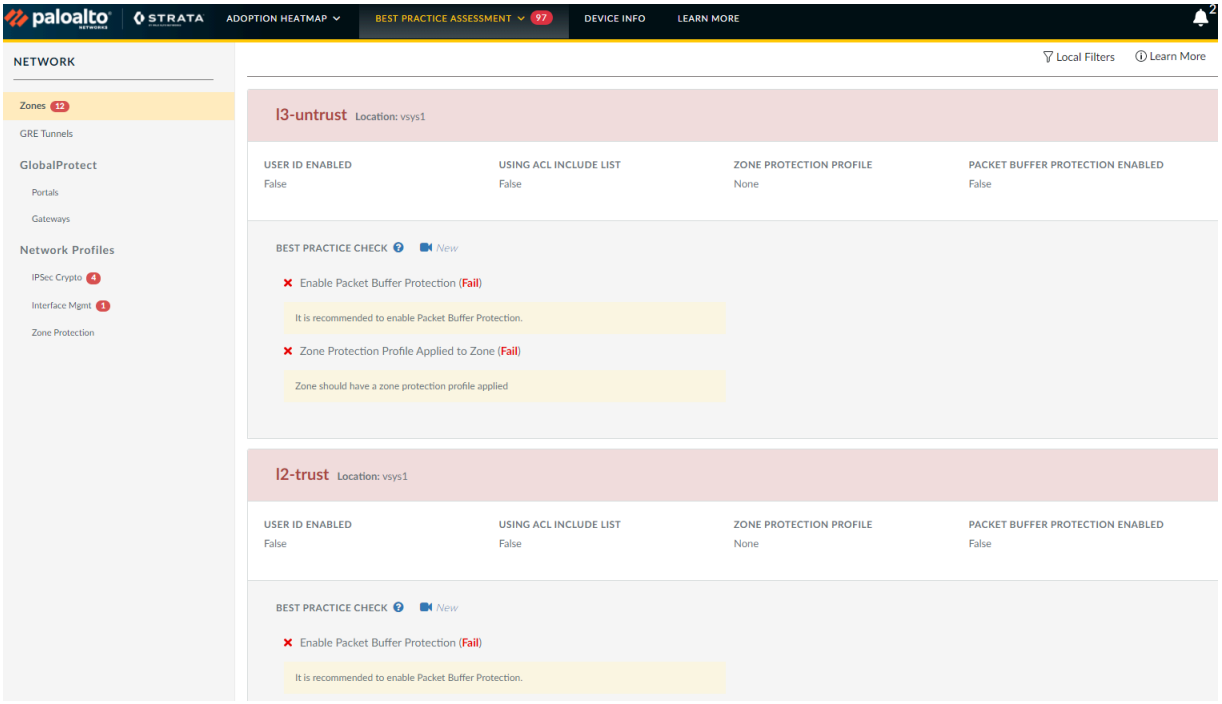
Lorsque vous examinez l'onglet **Objects** (Objets), examinez au minimum les éléments suivants pour vous aider à comprendre la portée potentielle de la correction :

- **Antivirus** : actions du décodeur pour Antivirus et WildFire.
- **Anti-Spyware** : profil Strict, DNS Sinkhole.
- **Vulnerability Protection** (Protection contre les vulnérabilités) : profil Strict.
- **URL Filtering** (Filtrage des URL) : pour savoir si les catégories connues comme malveillantes sont bloquées.
- **WildFire Analysis** (Analyse WildFire) : types de fichiers de profil (tous les types doivent être envoyés à WildFire pour analyse).
- **Log Forwarding** (Transfert des journaux) : pour savoir si tous les types de journaux sont transférés (transfère tous les types de journaux).

Ensuite : Examen de la configuration réseau des meilleures pratiques.

Examen de la configuration réseau des meilleures pratiques

Best Practice Assessment > **Network** montre toutes les vérifications pour la configuration liée au réseau et commence sur la page **Zones**. Dans le menu de gauche, sélectionnez la vérification de réseau que vous souhaitez examiner pour comprendre la configuration existante et identifier les failles potentielles dans la configuration des meilleures pratiques liée aux Zones, aux GRE Tunnels (Tunnels GRE), ainsi qu'aux profils GlobalProtect, IPsec Crypto (Crypto IPSec) Interface Management (Gestion de l'interface) et Zone Protection (Protection de zone). L'exemple suivant montre le résultat pour les Zones.



Le rapport affiche la configuration actuelle pour chaque élément. Les résultats de la vérification des meilleures pratiques pour chaque élément apparaissent sous sa configuration actuelle. Vous pouvez spécifier un **Device Group** (Groupe d'équipement) et/ou un **Template** (Modèle) pour limiter la portée des informations affichées.

Chaque vérification a le statut Pass (Réussite)/Fail (Échec) et des recommandations pour les échecs de vérification des meilleures pratiques. Cliquez sur l'aide pour afficher la justification de chaque vérification et sur les liens vers la documentation sur les meilleures pratiques. Lorsqu'une ou plusieurs vérifications échouent, l'intitulé de l'élément devient rouge.

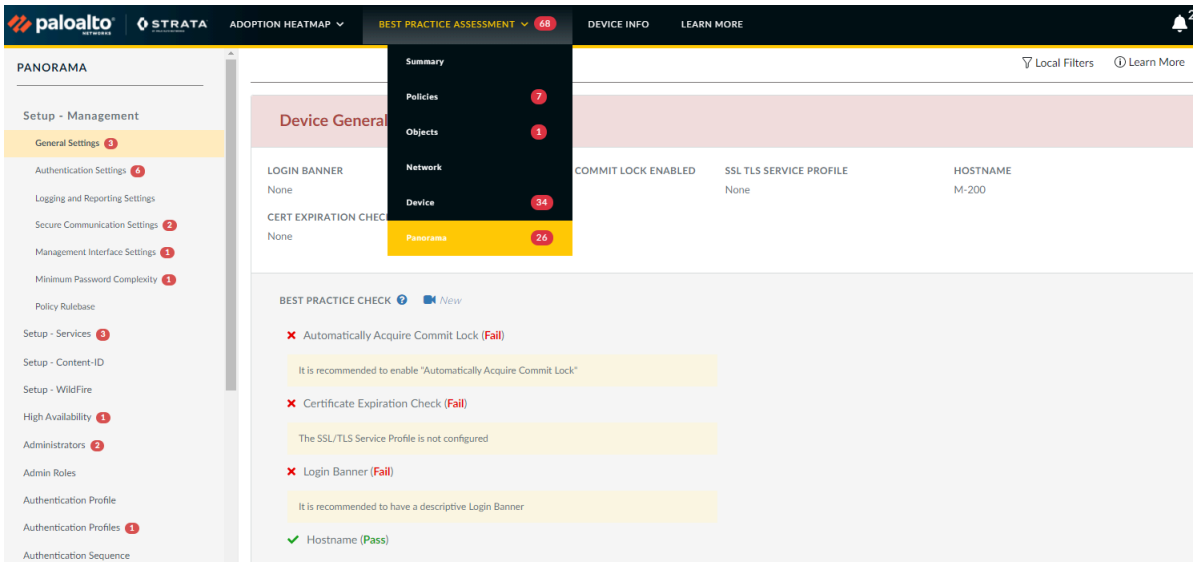
Lorsque vous examinez l'onglet **Network** (Réseau), examinez au minimum les éléments suivants pour vous aider à comprendre la portée potentielle de la correction :

- **Zones** : pour savoir si la Packet Buffer Protection (Protection de la mémoire tampon de paquets) est activée dans chaque zone et si son profil est Zone Protection (Protection de zone).
- **Zone Protection** (Protection de zone) : pour savoir si Flood Protection (Protection contre les inondations) et la Packet-Based Attack Protection (Protection contre les attaques basées sur des paquets) sont activées.

Ensuite : Examen de la configuration de la gestion des périphériques et de Panorama, relative aux meilleures pratiques.

Examen de la configuration de la gestion des périphériques et de Panorama, relative aux meilleures pratiques

Les pages **Best Practice Assessment** > **Device** et **Best Practice Assessment** > **Panorama** montrent toutes les vérifications relatives à la configuration de la gestion des périphériques. Sur les pare-feu autonomes, **Best Practice Assessment** > **Device** commence sur la page des paramètres généraux pour configurer la gestion du pare-feu du périphérique. Sur Panorama, **Best Practice Assessment** > **Device** commence sur la page des paramètres généraux pour chaque pile de modèles. **Best Practice Assessment** > **Panorama** commence sur la page des paramètres généraux pour configurer la gestion. Sélectionnez la vérification que vous souhaitez examiner pour comprendre la configuration existante et identifier les failles potentielles dans la configuration des meilleures pratiques liée à la gestion des équipements Panorama et du pare-feu. L'exemple suivant montre le résultat pour les paramètres généraux pour un périphérique Panorama.



Le rapport affiche la configuration actuelle pour chaque élément. Les résultats de la vérification des meilleures pratiques pour chaque élément apparaissent sous sa configuration actuelle. Lors de la visualisation d'informations pour un **Device** (Équipement), vous pouvez spécifier un **Template** (Modèle) pour limiter la portée des informations affichées.

Chaque vérification a le statut Pass (Réussite)/Fail (Échec) et des recommandations pour les échecs de vérification des meilleures pratiques. Cliquez sur l'aide pour afficher la justification de chaque vérification et sur les liens vers la documentation sur les meilleures pratiques. Lorsqu'une ou plusieurs vérifications échouent, l'intitulé de l'élément devient rouge.

Lorsque vous examinez l'onglet **Device** (Équipement), ou **Panorama**, examinez au minimum les éléments suivants pour vous aider à comprendre la portée potentielle de la correction :

- **Dynamic Updates** (Mises à jour dynamiques) : mises à jour Antivirus, Apps, Threats (Menaces) et WildFire.
- **Management Interface Settings** (Paramètres de l'interface de gestion) : Network Connectivity Services (Services de connectivité réseau), Permitted IP Addresses (Adresses IP autorisées).

- **Administrators** (Administrateurs) : Local Admins (Administrateurs locaux), Administrator Password profil (profil de mot de passe administrateur). Vérifiez **Device (Périphérique)** > **Administrators (Administrateurs)** ou **Panorama** > **Administrators (Administrateurs)** pour vous assurer que les mots de passe des administrateurs sont configurés avec la complexité minimale requise.
- **Minimum Password Complexity** (Complexité minimale du mot de passe) : vérification des exigences de complexité minimale du mot de passe.

Ensuite : Hiérarchisation des modifications des meilleures pratiques.

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.

Dans les environnements gérés par Panorama, Panorama peut gérer un grand nombre de pare-feu nouvelle génération. Devez-vous exécuter le BPA sur Panorama ou sur chaque pare-feu individuel ? Le compromis est la rapidité et la commodité par comparaison à l'exhaustivité.

L'exécution du BPA sur Panorama est rapide et pratique ; cela permet d'évaluer la plupart des capacités des pare-feu gérés, mais cela n'examine pas les remplacements de pare-feu locaux.

L'exécution du BPA sur chaque pare-feu géré permet d'évaluer la configuration complète (y compris les remplacements locaux), mais est plus chronophage.

La méthode la plus pratique consiste à exécuter d'abord le BPA sur Panorama. Examinez les résultats afin d'identifier des appareils gérés particuliers, puis exécutez le BPA sur ces appareils. Cette méthode vous permet de gagner du temps et de vous concentrer sur les informations pertinentes qui vous permettent d'améliorer votre 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 en matière d'accès administratif pour éviter tout accès non autorisé et non sécurisé à l'interface de gestion du périphérique.
- 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.

Ensuite : 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 Examen du résumé de l'adoption et identifié les 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.

Ensuite : 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 Examen du résumé de l'adoption et identifié les 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.

Ensuite : 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 Prisma Access 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.