Tests indépendants
sur les logiciels antivirus

Secure Access Service Edge

SASE Palo Alto Networks : le rapport comparatif

PÉRIODE DU TEST : DE SEPTEMBRE 2021 À FÉVRIER 2022

DERNIÈRE MODIFICATION : 14 AVRIL 2022

RÉDIGÉ POUR : PALO ALTO NETWORKS

WWW.AV-COMPARATIVES.ORG

Sommaire

Introduction

Réalisé à la demande de Palo Alto Networks, ce test comparatif a pour objectif d'évaluer le niveau de sécurité offert par les solutions SASE (Secure Access Service Access) leaders destinées à répondre aux besoins des effectifs hybrides d'aujourd'hui. Palo Alto Networks a choisi les produits à tester, la configuration utilisée pour sa solution et les scénarios couverts. Les deux produits concurrents testés ont été configurés conformément aux recommandations publiées par leurs fournisseurs respectifs. La modification de ces paramètres peut générer des résultats différents.

Dans l'économie mondiale actuelle, de nombreuses entreprises s'appuient sur des effectifs distribués entre plusieurs sites, par exemple entre leur siège et leurs succursales. Un état de fait amplifié par l'essor du télétravail, lui-même dicté par la pandémie de Covid-19. Où qu'ils se trouvent, les collaborateurs ont besoin d'accéder à des services IT, des applications et des données, eux aussi répartis entre plusieurs sites physiques : réseau LAN d'entreprise, data center (cloud privé), cloud public, etc. Les solutions déployées par l'entreprise doivent permettre aux utilisateurs distants d'accéder à ces ressources autorisées de manière sécurisée, ce qui complique la tâche des départements IT.

Auparavant, il fallait parfois une multitude de produits pour contrôler l'accès de ces utilisateurs aux données distribuées, avec pour conséquence un système de gestion complexe et un manque de visibilité sur les politiques d'accès et les mesures de sécurité. Destinées à simplifier ce processus, les solutions SASE (*Secure Access Service Edge*) permettent aux administrateurs IT de gérer toutes les mesures de sécurité et autorisations d'accès nécessaires à partir d'une seule et même architecture/interface cloud de gestion.

Les solutions SASE peuvent sécuriser, optimiser et automatiser l'accès aux applications et aux workloads dans le cloud en étendant la sécurité et les réseaux SDN aux principaux fournisseurs IaaS et SaaS. Le SASE offre un accès sécurisé et unifié à partir d'une seule plateforme de gestion, quelle que soit la localisation de vos utilisateurs et de vos applications.

La SASE nécessitait autrefois de choisir entre contrôle et rapidité. Ce n'est désormais plus le cas grâce aux progrès réalisés dans le domaine. De fait, les outils SASE modernes allient priorités en matière de trafic et de sécurité réseau, sécurisation des données et protection intégrale contre les menaces, tout en permettant aux entreprises de bénéficier de connexions réseau directes ultrarapides vers le cloud.

Une solution SASE doit pouvoir protéger tous les utilisateurs de manière cohérente, quels que soient leur localisation ou l'application et le port/protocole utilisés. Elle doit également détecter et bloquer les activités malveillantes entrantes et sortantes pour neutraliser les menaces internes et éviter le risque qu'un utilisateur peu méfiant se connecte à partir d'un hôte déjà infecté. Les fonctionnalités globales de protection contre les menaces et l'exhaustivité de la couverture de la surface d'attaque (plusieurs vecteurs) sont donc primordiales, tant pour les télétravailleurs que pour les utilisateurs de sites distants. Il en va de même pour la distinction entre trafic autorisé et malveillant, les délais de prévention, d'identification et de détection des menaces, le reporting et la visibilité.

Solutions SASE testées

Les produits suivants ont été testés dans leur version la plus récente, sur une période de six mois (de septembre 2021 à février 2022) :

- Cisco Umbrella
- Palo Alto Networks Prisma Access Enterprise
- Zscaler Internet Access

Déploiement et configuration du test SASE

Les solutions SASE ont été configurées conformément aux bonnes pratiques fournies par Palo Alto Networks pour son propre produit, et en fonction des bonnes pratiques publiées par les deux autres fournisseurs pour leurs solutions respectives. Les configurations SASE couvraient de multiples applications de sécurité et de conformité – filtrage des URL, antivirus, protection avancée contre les menaces, sandboxing, pare-feu, prévention des pertes de données, sécurité des applications cloud, gestion de la bande passante, etc. – intégrées à un seul et même système transparent. Les fonctionnalités de prévention et de protection (capacité à bloquer la menace) étaient activées. La mise à jour des produits était autorisée. Dans la mesure du possible, nous avons exécuté tous les scénarios de test dans leur intégralité.

Le test SASE en bref

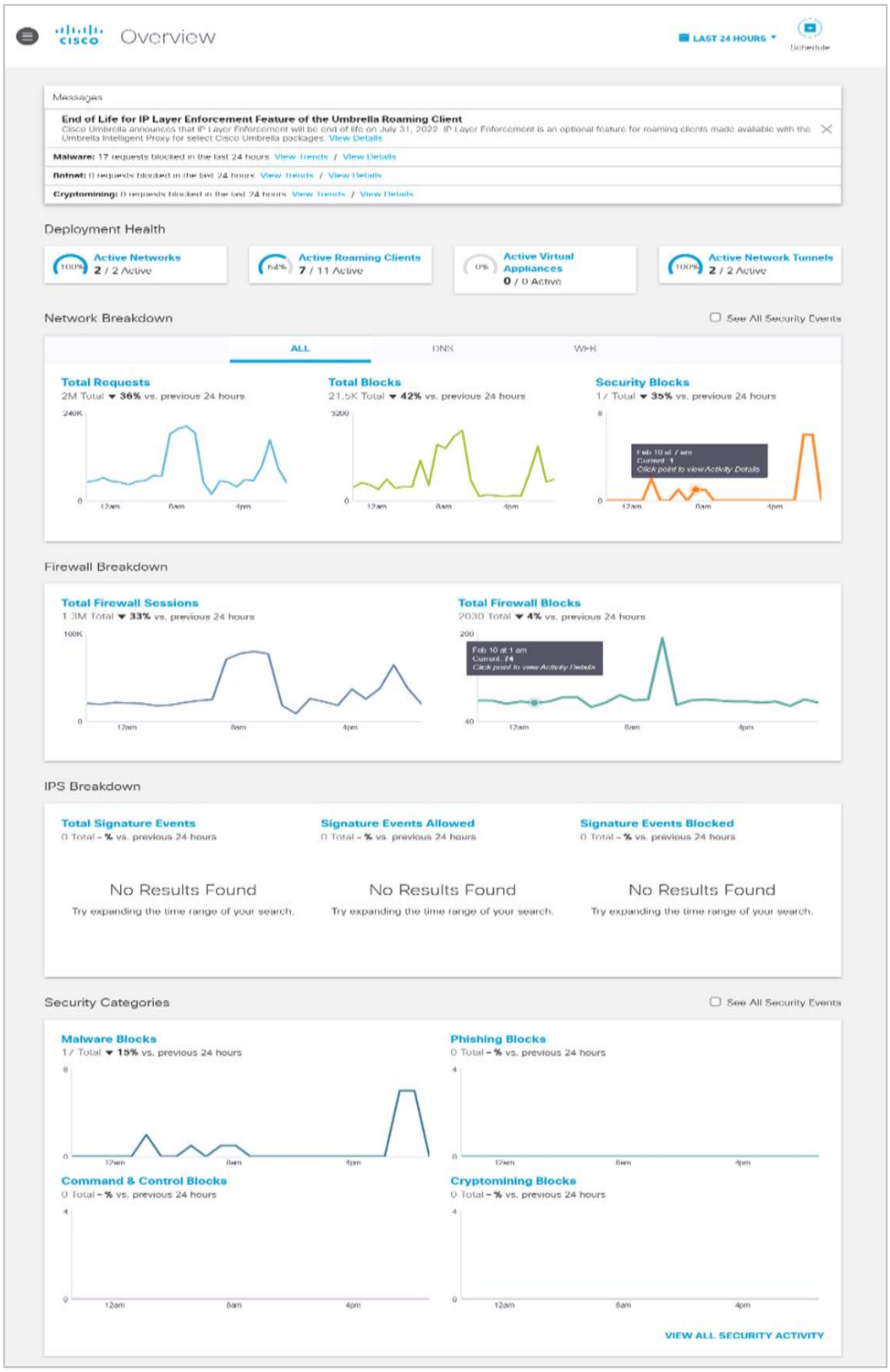
La procédure de test globale comprenait huit sous-tests différents, chacun couvrant une fonctionnalité clé des produits SASE dans un scénario concret donné. Les sous-tests de la protection web par filtrage d'URL, de la sécurité DNS et de la protection antimalware étaient eux-mêmes divisés en plusieurs catégories, indiquées ci-dessous entre parenthèses :

1. Protection web par filtrage d'URL (taux de blocage des communications CnC, des malwares et des attaques de phishing, taux moyen de catégorisation des URL inoffensives)
2. Sécurité DNS (prévention contre le DNS Tunneling, taux de protection contre les DGA)
3. Protection antimalware (durée d'analyse de la sandbox, protection contre les malwares modifiés, protection antimalware via les protocoles de messagerie, extraction d'artefacts, transfert de fichiers)
4. Sécurité des applications SaaS publiques
5. Sécurité des applications SaaS privées
6. Protection contre les vulnérabilités
7. Protection contre les techniques de contournement
8. Prévention des vols d'identifiants

Vous trouverez plus loin dans ce rapport les résultats détaillés de ces tests pour chaque solution. Les paramètres appliqués à chaque produit figurent dans la section « Paramètres des produits » de l'annexe.

Aperçu des différents produits

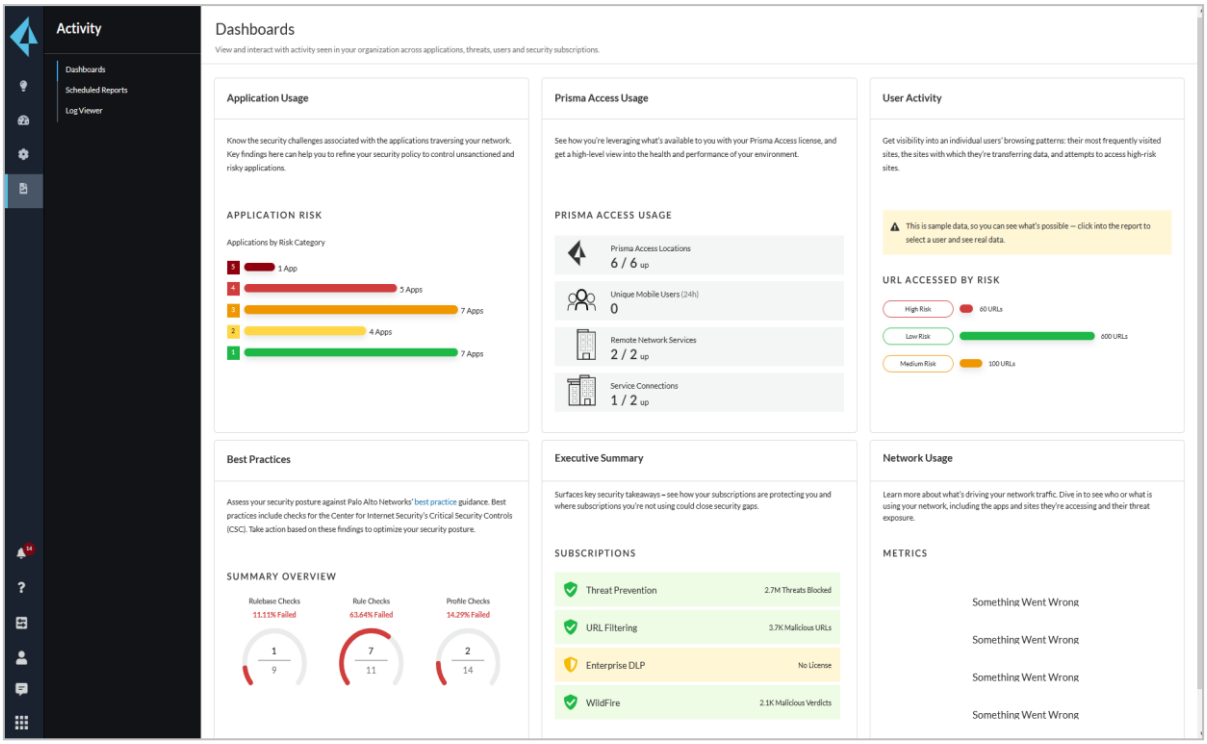
Cisco Umbrella



Cisco Umbrella

La solution SASE de Cisco a obtenu d'excellents résultats dans les catégories suivantes : prévention contre le DNS Tunneling et protection contre les malwares inconnus ; protection contre les malwares modifiés.

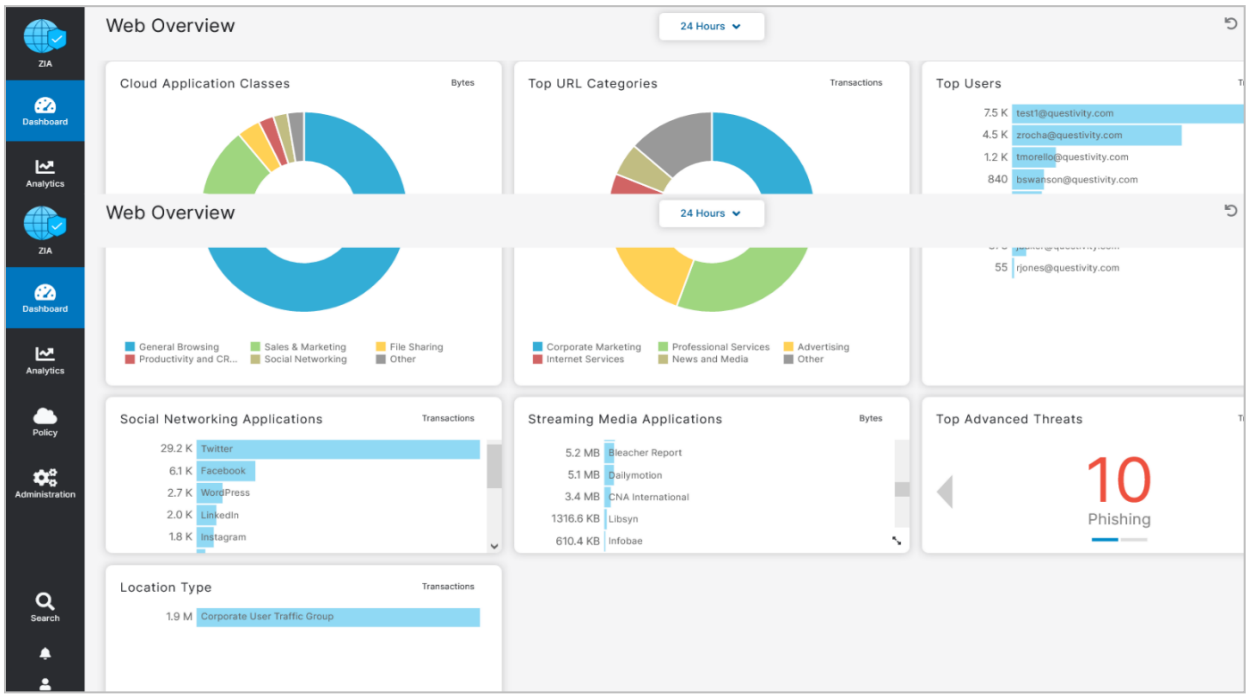
Palo Alto Networks Prisma Access Enterprise



Palo Alto Networks Prisma Access Enterprise

La solution SASE de Palo Alto Networks s'est illustrée dans la plupart des tests, notamment : taux de blocage des URL de serveurs CnC ; taux de blocage des URL de malwares ; taux de blocage des URL de phishing ; taux moyen de catégorisation des URL inoffensives ; prévention contre le DNS Tunneling; taux de protection contre les DGA ; protection contre les malwares modifiés ; protection antimalware via les protocoles de messagerie ; transfert de fichiers ; sécurité des applications SaaS publiques ; sécurité des applications SaaS privées ; protection contre les vulnérabilités ; protection contre les techniques de contournement ; prévention des vols d'identifiants. En ce qui concerne la protection antimalware via les protocoles de messagerie, Palo Alto Networks couvrait les protocoles IMAP et SMTP. Côté extraction d'artefacts, Palo Alto Networks prenait en charge les formats PPT et PDF.

Zscaler Internet Access



Zscaler Internet Access

Zscaler affichait un excellent taux moyen de catégorisation des URL inoffensives.

Notre analyse comparative des solutions SASE

Le tableau ci-dessous récapitule les principaux résultats des trois produits testés dans les huit catégories de notre procédure de validation.

Catégories de fonctions de sécurité SASE	Cisco	Palo Alto Networks	Zscaler
1. Protection web par filtrage d'URL			
Taux de blocage des communications CnC	37 %	**91 %**	63 %
Taux de blocage des malwares	37 %	**84 %**	66 %
Taux de blocage des attaques de phishing	23 %	**78 %**	35 %
Taux moyen de catégorisation des URL inoffensives	81 %	**98 %**	97 %
2. Sécurité DNS			
Journalisation et prévention contre le DNS Tunneling	100 %	**100 %**	75 %
Taux de protection contre les DGA	64 %	**100 %**	76 %
3. Protection antimalware			
Fonction de protection contre les malwares inconnus de la sandbox	N/A	**Oui**	Oui
Protection contre les malwares modifiés	85 %	**100 %**	16 %
Protection antimalware via les protocoles de messagerie	SMTP	**IMAP/SMTP**	-
Extraction d'artefacts	PDF	**PDF/PPT**	PDF
Transfert de fichiers	N/A	**Oui**	N/A
Sécurité des applications SaaS			
4. Sécurité des applications SaaS publiques	Oui	**Oui**	Oui
5. Sécurité des applications SaaS privées	N/A	**Oui**	-
6. Protection contre les vulnérabilités	71 %	**100 %**	29 %
7. Protection contre les techniques de contournement	50 %	**100 %**	100 %
8. Prévention des vols d'identifiants	N/A	**Oui**	N/A

Conclusion

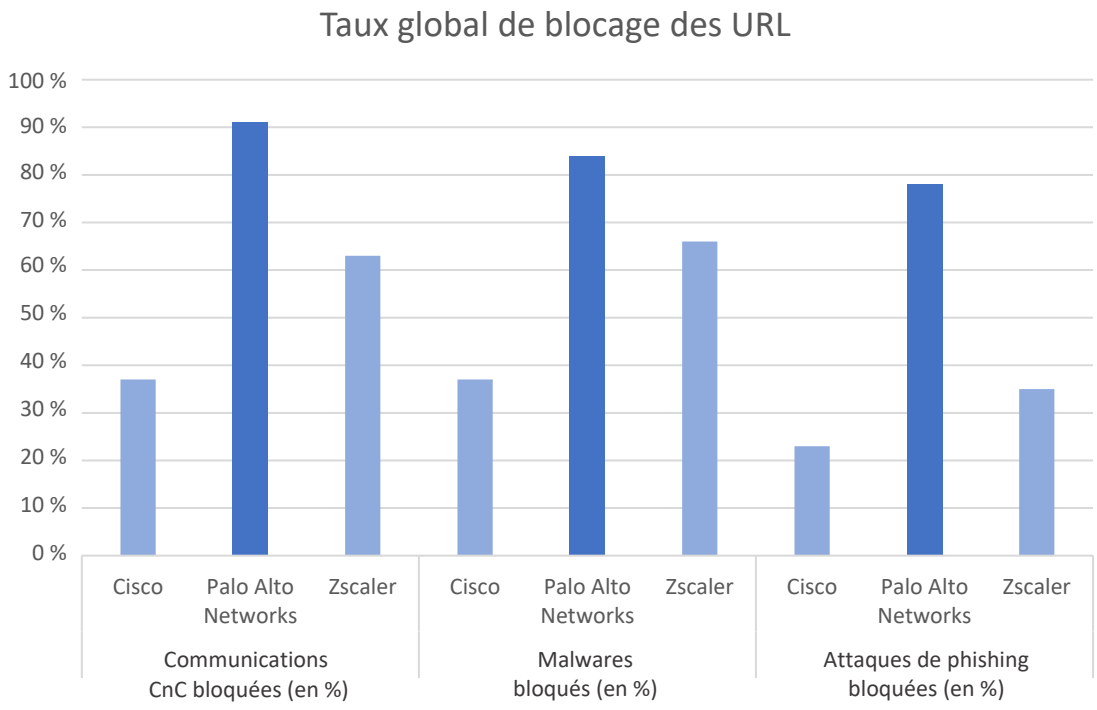
Réalisé à la demande de Palo Alto Networks, ce test comparatif de produits SASE couvrait un large éventail de fonctionnalités de protection des effectifs hybrides, y compris le filtrage d'URL, la sécurité DNS, la protection antimalware, la protection contre les vulnérabilités et la prévention des vols d'identifiants. Dans la plupart de ces catégories, Palo Alto Networks obtenait les meilleurs résultats ou finissait ex æquo avec l'un de ses concurrents. Lors des tests des fonctionnalités de filtrage d'URL, Palo Alto Networks affichait le taux de protection le plus élevé dans les quatre sous-catégories. La solution Palo Alto Networks était également la seule à intégrer des fonctions de prévention des vols d'identifiants et de protection antimalware via le protocole de messagerie IMAP.

Les sous-tests

Dans les paragraphes qui suivent, nous détaillons les résultats de chaque sous-test de notre analyse globale.

1. Protection web par filtrage d'URL

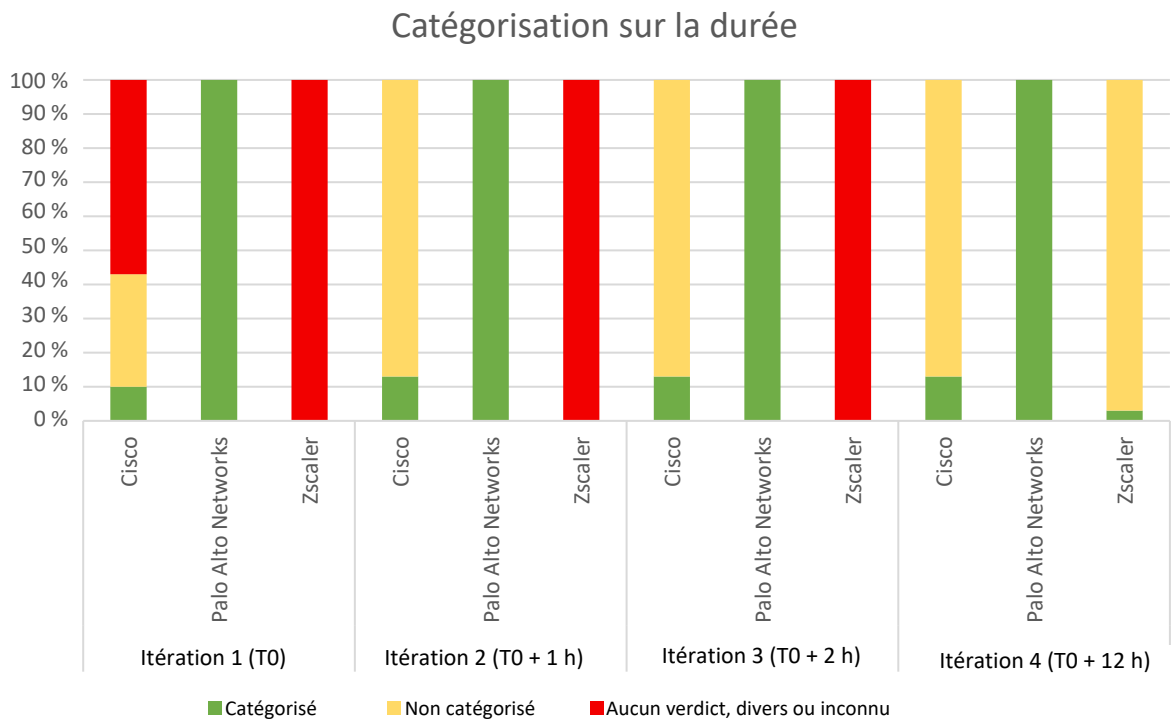
Les entreprises étant responsables du trafic réseau qu'elles autorisent, il leur incombe de contrôler les comportements de leurs collaborateurs sur Internet. Les solutions SASE efficaces savent identifier correctement les contenus et bloquer ceux qui vont à l'encontre de la politique de l'organisation. Les solutions SASE utilisées dans les environnements d'entreprise actuels doivent pouvoir distinguer différentes catégories d'URL, mais aussi offrir un contrôle à la demande sur ces catégories. S'il est essentiel de bloquer les URL malveillantes afin de protéger les entreprises contre les menaces, il est tout aussi important de permettre aux utilisateurs d'accéder aux catégories d'URL autorisées et inoffensives.



Taux global de blocage des URL

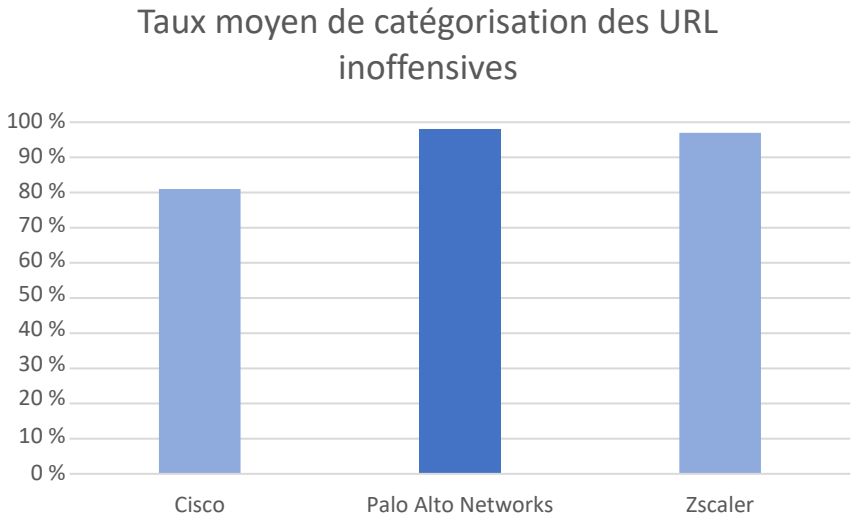
AV-Comparatives a soumis plus de 1 700 URL aux fonctionnalités de protection contre le phishing, les malwares et les communications de commande et contrôle (CnC) malveillantes. Nous tenons également à rappeler que toutes les fonctionnalités nécessaires au respect des bonnes pratiques recommandées par les différents fournisseurs étaient activées tout au long du test. Le filtrage web allie souvent le filtrage DNS et d'URL. Les fonctionnalités de sécurité DNS sont donc restées actives pour toute la durée du test afin de refléter les scénarios et bonnes pratiques en conditions réelles. Ainsi, lors de ce test, certaines URL ont peut-être été bloquées au niveau du DNS. Le graphique ci-dessus illustre les taux de blocage des URL pour chaque fournisseur dans chaque catégorie de test.

D'après ce graphique, Palo Alto Networks offrait un niveau de protection contre les URL malveillantes supérieur à celui de ses concurrents, et ce toutes catégories confondues (CnC, malware et phishing).



Catégorisation de nouveaux domaines/URL sur la durée

Le graphique ci-dessus illustre la catégorisation de 30 URL nouvellement créées sur une durée donnée. Le test des fonctions de catégorisation a débuté dans les 24 heures suivant leur création. T0 correspond à la première analyse des nouvelles URL. Les itérations suivantes sont respectivement intervenues une heure, deux heures et 12 heures après T0. Palo Alto Networks est parvenue à catégoriser tous les domaines/URL au cours de la première itération. Au même moment, les fonctionnalités d'alerte et de catégorisation de Cisco en classaient environ 45 %, tandis que Zscaler ne se prononçait pas du tout. Au cours des trois itérations suivantes, Cisco et Zscaler ont progressivement amélioré leurs résultats.



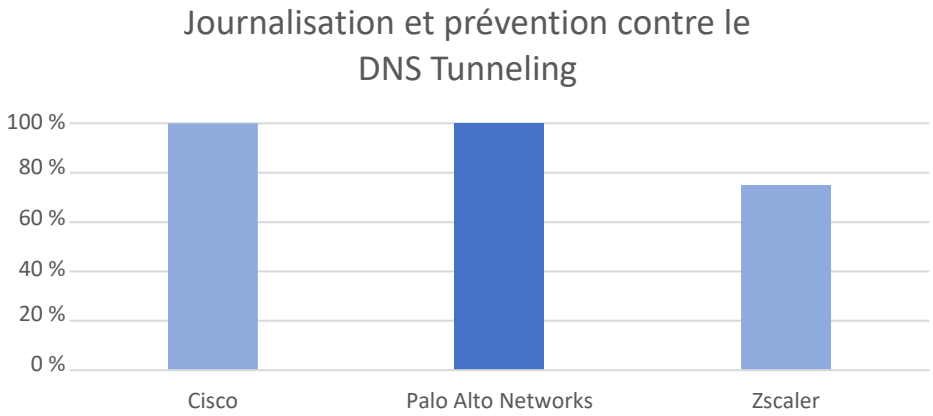
Taux moyen de catégorisation des URL inoffensives (en %)

Dans le graphique ci-dessus, nous nous intéressons au taux moyen de catégorisation des URL inoffensives, calculé à partir de 429 cas. Avec une moyenne de 97 % dans les sept catégories évaluées, les fonctionnalités de Zscaler dans ce domaine étaient excellentes, tant pour les télétravailleurs que pour les utilisateurs de sites distants. Quant aux fonctionnalités de Cisco, elles affichaient un taux moyen de catégorisation des URL inoffensives de 81 %. Enfin, Palo Alto Networks surclassait ses concurrents avec un taux de réussite de 98 %.

2. Sécurité DNS

Prévention contre le DNS Tunneling

Les attaquants utilisent régulièrement les protocoles DNS pour exfiltrer des données, propager des malwares et communiquer avec des serveurs de commande et contrôle. Or, il est rare que les entreprises surveillent le trafic DNS entrant et sortant de leur infrastructure IT. Les solutions SASE doivent donc protéger ces organisations contre le DNS Tunneling et détecter l'utilisation d'algorithmes de génération de domaines (DGA). Le graphique ci-dessous recense les résultats des trois produits face à quatre méthodes de DNS Tunneling basées sur des outils publics. Pour ce test, nous avons utilisé des ports standards.

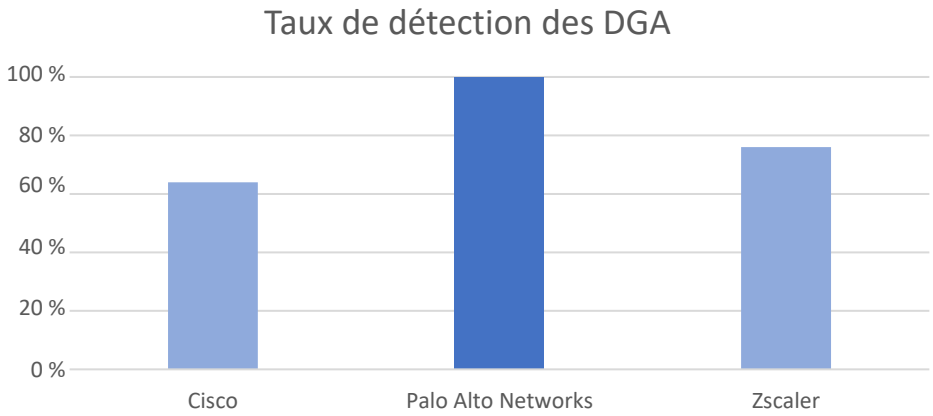


Journalisation et prévention contre le DNS Tunneling

Parmi les produits testés, deux sont parvenus à contrecarrer les quatre méthodes.

Protection contre les DGA

Cela fait longtemps que bon nombre de cybercriminels utilisent les algorithmes de génération de domaines (DGA) dans le cadre de leurs activités de commande et contrôle (CnC). De fait, c'est l'une des méthodes les plus efficaces pour le contournement des fonctions de sécurité basées sur la réputation. Pour ce test, nous avons sélectionné des familles de malwares qui proliféraient à l'époque et nous avons généré cinq DGA basés sur ces familles, avec chacun cinq échantillons. Vous trouverez ci-dessous les taux de détection et de blocage de ces DGA par les solutions SASE.



Taux de protection contre les DGA

Comme le montre le graphique ci-dessus, Palo Alto Networks a su identifier, catégoriser et bloquer efficacement les domaines DGA malveillants. La solution de Cisco affichait un taux de réussite de 64 % face aux techniques DGA testées. Quant à Zscaler, il offrait un taux de détection et de blocage de 76 %.

3. Protection antimalware

Malwares inconnus

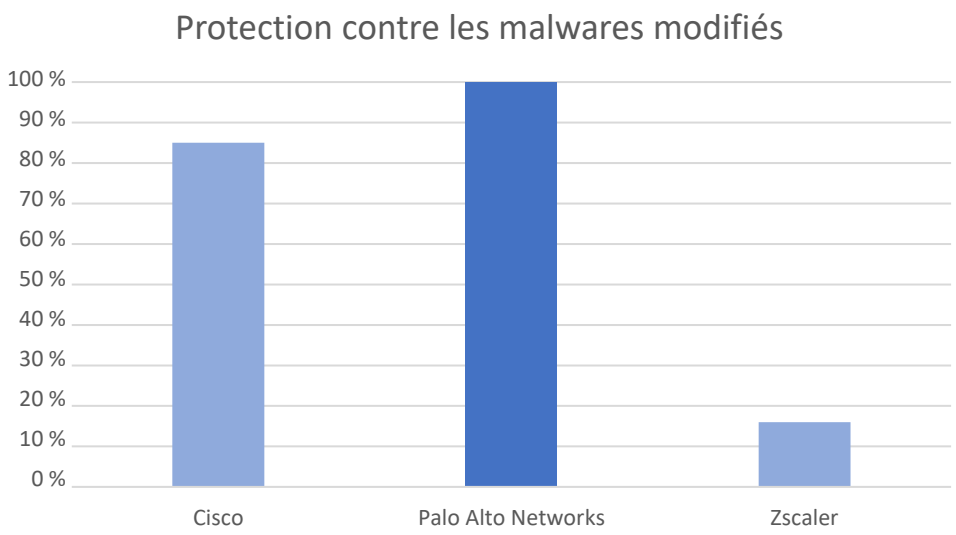
Le blocage des malwares inconnus fait partie des fonctionnalités clés des solutions SASE. En effet, il protège les utilisateurs contre les attaques inconnues que d'autres technologies ne parviennent pas à contrer. Pour combattre ce type de menaces, les solutions SASE s'appuient notamment sur le sandboxing. En plus de fournir des informations sur ces attaques, elles doivent permettre impérativement d'en déduire les mesures de protection appropriées. Tant Palo Alto Networks que Zscaler intègrent une fonctionnalité de sandboxing pour traiter les menaces inconnues.

	Cisco	Palo Alto Networks	Zscaler
Fonctionnalité de sandboxing pour protéger les entreprises contre les menaces inconnues	-	✓	✓

Fonctionnalité de sandboxing

Malwares modifiés

Les attaquants transforment les menaces de base, celles déjà observées, à l'aide de mécanismes destinés à contourner les signatures, l'heuristique et les analyses comportementales. Dans la même veine, AV-Comparatives a eu recours à différents mécanismes de modification de fichiers pour tenter de contourner les fonctions de sécurité des solutions SASE.



Protection contre les malwares modifiés

Cisco et Palo Alto Networks ont fait preuve de résilience face à ces attaques.

Protection antimalware via les protocoles de messagerie

Les solutions SASE doivent pouvoir prendre en charge les protocoles de messagerie courants. Elles doivent permettre d'extraire des informations pertinentes à partir des menaces propagées par e-mail sous la forme d'URL, de techniques de packaging et de paramètres d'interface de ligne de commande. Les fonctionnalités de protection de Palo Alto Networks couvraient tant le protocole de messagerie IMAP que SMTP, tandis que Cisco n'était efficace que sur le second. Quant à Zscaler, elle ne protégeait aucun de ces protocoles. Le tableau ci-dessous offre un aperçu des résultats obtenus par les fonctions de protection via les protocoles de messagerie :

Fournisseur	Protection IMAP	Protection SMTP
Cisco	-	✓
Palo Alto Networks	✓	✓
Zscaler	-	-

Protection antimalware via les protocoles de messagerie

Dans le tableau suivant, nous nous penchons sur la capacité des différents fournisseurs à extraire des informations pertinentes sur les menaces à partir de deux types de fichiers bien connus :

Fournisseur	Extraction d'artefacts des PDF	Extraction d'artefacts des PPT
Cisco	✓	-
Palo Alto Networks	✓	✓
Zscaler	✓	-

Capacités d'extraction d'informations pertinentes sur les menaces

Transfert de fichiers

Les solutions SASE doivent protéger l'entreprise contre le transfert bidirectionnel de fichiers malveillants. Le protocole SMB figure parmi les plus utilisés par les attaquants pour ce type de transferts. À cet égard, Palo Alto Networks a démontré des capacités de protection contre les malwares propagés via le protocole SMB, contrairement à Cisco et Zscaler.

Fournisseur	Protection contre les transferts de fichiers via SMB
Cisco	-
Palo Alto Networks	✓
Zscaler	-

Protection contre les transferts de fichiers via le protocole SMB

4. Sécurité et accès aux applications SaaS du cloud public

Pour être complète, une solution SASE Zero Trust doit procéder à une inspection approfondie du contenu du trafic entrant et sortant, sur n'importe quels port et protocole, mais aussi offrir un accès aux applications SaaS publiques dans le cloud, quelle que soit la localisation de l'utilisateur. Elle doit pouvoir soumettre les utilisateurs qui accèdent à ces applications à un contrôle granulaire.

Application SaaS publique	Cisco	Palo Alto Networks	Zscaler
Distinction systématique entre la version entreprise de Google Drive et sa version grand public	-	-	-
Distinction systématique entre la version entreprise de OneDrive et sa version grand public	-	✓	✓

Contrôle des applications SaaS

Lorsque nous avons évalué la capacité des solutions SASE à identifier des types d'applications cloud spécifiques afin d'en contrôler l'accès, nous avons pu constater qu'aucun des fournisseurs testés ne peut faire systématiquement la distinction entre les versions entreprise et grand public de Google Drive. Toutefois, cette lacune ne semble pas nuire aux capacités de prévention. Cisco est le seul fournisseur n'ayant pas pu différencier la version entreprise de OneDrive de sa version grand public (cf. tableau ci-dessus).

Efficacité de la sécurité – Chargement			
Application SaaS publique	Cisco	Palo Alto Networks	Zscaler
Box	-	✓	✓
DropBox	-	✓	✓
Google Drive	-	✓	-
OneDrive	-	✓	✓

Transferts malveillants de l'utilisateur vers les applications SaaS publiques

Palo Alto Networks a démontré d'excellentes capacités de détection et de blocage chaque fois qu'un utilisateur tentait de transférer des échantillons malveillants (format de fichier et autres) vers des applications SaaS hébergées dans le cloud public. En revanche, Cisco n'est parvenu à détecter aucun de ces transferts vers le cloud. Enfin, Zscaler affichait également un taux de détection et de blocage élevé sur Dropbox et OneDrive, mais n'avait aucune visibilité sur les transferts vers Google Drive (cf. tableau ci-dessus).

Efficacité de la sécurité – Téléchargement			
Application SaaS publique	Cisco	Palo Alto Networks	Zscaler
Box	✓	✓	✓
DropBox	✓	✓	✓
Google Drive	-	✓	-
OneDrive	✓	✓	✓

Transferts malveillants des applications SaaS publiques vers l'utilisateur

Palo Alto Networks affichait systématiquement un taux de détection et de blocage élevé pour les transferts malveillants des applications SaaS publiques vers les utilisateurs. Sur Box et Dropbox, Cisco démontrait également d'excellentes capacités de détection et de blocage. Toutefois, sa visibilité sur Google Drive et OneDrive restait limitée, voire inexistante. Zscaler offrait une couverture correcte et homogène de Box, Dropbox et OneDrive, mais n'est parvenu à détecter aucun transfert en provenance de Google Drive. Le tableau ci-dessus indique quels fournisseurs ont été capables de sécuriser les applications SaaS publiques testées.

5. Sécurité et accès aux applications SaaS internes/privées

Scénario d'inspection	Cisco	Palo Alto Networks	Zscaler
Menace interne	N/A	✓	-
Exploitation d'un utilisateur distant	N/A	✓	-
Protection antimalware bidirectionnelle (ports standards)	N/A	✓	-
Protection antimalware bidirectionnelle (ports non standards)	N/A	✓	-

Inspection du contenu d'applications SaaS internes/privées par Palo Alto Networks

Remarque : au moment du test, la solution de Cisco n'intégrait pas une telle fonctionnalité, d'où la mention « non applicable ». Bien que la fonctionnalité concernée de Zscaler ait été configurée, sa solution n'a pas su détecter la menace dans les scénarios du tableau ci-dessus.

Palo Alto Networks est parvenue à empêcher l'exploitation d'un utilisateur distant vulnérable par une application malveillante, ainsi que l'exploitation d'une application vulnérable par un utilisateur distant (dans le cas d'une menace interne). Seule la solution de Palo Alto Networks a démontré des capacités de protection antimalware bidirectionnelles, depuis un utilisateur distant et vers ce dernier, sur les ports standards et non standards.

	Cisco	Palo Alto Networks	Zscaler
Contrôle des applications en fonction de l'utilisateur	N/A	✓	✓

Contrôle des applications en fonction de l'utilisateur

Remarque : au moment du test, la solution de Cisco n'intégrait pas une telle fonctionnalité, d'où la mention « non applicable ». Tant Palo Alto Networks que Zscaler ont pu appliquer différentes politiques d'accès granulaire à une application en fonction de l'utilisateur (cf. tableau ci-dessus).

6. Protection contre les vulnérabilités

Malgré la migration des ressources en dehors du périmètre de l'entreprise, les architectures modernes continuent de faire transiter l'intégralité du trafic via son réseau. Où qu'ils se trouvent, les utilisateurs doivent donc systématiquement passer par le backhaul de leur organisation. C'est pourquoi les solutions SASE doivent offrir une protection contre les vulnérabilités côté serveur et côté client au score CVSS (Common Vulnerability Scoring System) élevé, voire très élevé. Lors de ce test, nous avons utilisé sept vulnérabilités dont le score CVSS était supérieur à 7,5.

Protection contre les vulnérabilités	Cisco	Palo Alto Networks	Zscaler
Taux de protection contre les vulnérabilités récentes	100 %	100 %	50 %
Taux de protection des utilisateurs distants	100 %	100 %	50 %
Taux de protection des applications distantes	33 %	100 %	0 %
Taux global de protection contre les vulnérabilités	**71 %**	**100 %**	**29 %**

Protection contre les vulnérabilités

Palo Alto Networks et Cisco ont su détecter et identifier les deux vulnérabilités récentes afin de déployer leurs capacités de protection. Au moment du test, Zscaler n'était efficace que contre l'une des vulnérabilités récentes.

Tant Palo Alto Networks que Cisco pouvaient protéger les utilisateurs distants contre une éventuelle compromission lorsqu'ils tentaient d'accéder à des applications compromises ou malveillantes hébergées sur l'Internet public. En revanche, dans ce cas de figure, Zscaler affichait un taux de protection de 50 % seulement (cf. taux de protection des utilisateurs distants dans le tableau ci-dessus).

Dans tous les scénarios et cas d'usage testés, en cas d'exploitation d'applications vulnérables sur l'Internet public, Palo Alto Networks protégeait aussi bien les télétravailleurs que les utilisateurs des sites distants. Le tableau ci-dessus (taux de protection des applications distantes) montre que Palo Alto Networks affichait encore une fois un taux de réussite de 100 % lorsqu'il s'agissait de prévenir l'exploitation des applications vulnérables. Ce cas d'usage témoigne d'une capacité essentielle : empêcher les utilisateurs non autorisés ou les systèmes d'utilisateur distant compromis d'exploiter une application ou des services distants hébergés sur l'Internet public. À cet égard, le taux de réussite de Cisco n'est que de 33 %, tandis que Zscaler n'offre aucune protection.

En clair, d'après les scénarios ci-dessus, si Cisco et Zcaler pouvaient protéger les utilisateurs distants contre des applications malveillantes, ils n'ont pas été en mesure de protéger les applications publiques contre des utilisateurs compromis et des menaces internes.

7. Protection contre les techniques de contournement

Les techniques de contournement permettent aux attaquants de dissimuler leurs malwares et leurs exploits via un protocole de transport ou de modifier leur contenu afin de berner les contrôles de sécurité. Elles leur permettent également de réutiliser des attaques existantes. Dans cette section, nous examinons la capacité des produits testés à contrecarrer ces techniques dans le cadre de six catégories d'attaques courantes.

Techniques de contournement	Cisco	Palo Alto Networks	Zscaler
Combinaison de techniques	50 %	100 %	100 %
Téléchargements drive-by	50 %	100 %	100 %
Contournement par HTML	50 %	100 %	100 %
Contournement par HTTP	50 %	100 %	100 %
Obscurcissement de scripts	50 %	100 %	100 %
Contournement par TCP/IP	50 %	100 %	100 %

Taux de protection contre les techniques de contournement
(somme des résultats sur les ports standards et non standards)

Pour chaque technique de contournement, nous avons utilisé deux scénarios, l'un avec des ports standards, l'autre avec des ports non standards. Les trois produits ont su contrecarrer ces techniques sur les ports standards. Toutefois, sur les six catégories d'attaques testées, Cisco n'en a stoppé aucune lorsque l'attaquant utilisait un port non standard.

8. Prévention des vols d'identifiants

Les informations et les identifiants des utilisateurs d'une entreprise ne doivent surtout pas être transmis à des sites non légitimes ni faire l'objet de fuites de données. Les solutions SASE doivent donc pouvoir identifier et détecter les attaques de phishing, puis détecter et prévenir tout envoi de noms d'utilisateur et de mots de passe. Le tableau ci-dessous recense les résultats des différentes solutions face à de multiples menaces de phishing d'identifiants. Pour cette fonctionnalité, nous avons utilisé deux scénarios.

Vol d'identifiants – Type de validation	Cisco	Palo Alto Networks	Zscaler
Identifie et détecte les attaques de phishing dans le contexte d'une tentative de vol d'identifiants	N/A	✓	N/A
Détecte et bloque la transmission d'un nom d'utilisateur sur les sites de phishing	N/A	✓	N/A
Détecte et bloque la transmission des identifiants de collaborateurs	N/A	✓	N/A

Prévention des vols d'identifiants

Au moment du test, Cisco et Zscaler n'intégraient aucune fonction de prévention des vols d'identifiants.

Annexe

Paramètres des produits

Vous trouverez ci-dessous les différents paramètres et configurations utilisés ainsi que les fonctionnalités activées lors de l'évaluation de ces solutions SASE. Palo Alto Networks a choisi la configuration à utiliser dans Prisma Access conformément à ses bonnes pratiques. Nous avons configuré les deux autres produits testés en fonction des bonnes pratiques publiées par leurs fournisseurs respectifs. La modification des paramètres sur ces deux produits est susceptible de générer des résultats différents.

Palo Alto Networks :
Filtrage d'URL : « high-risk » (risque élevé), « adult » (adulte), « command-and-control » (commande et contrôle), « copyright-infringement » (atteinte aux droits d'auteur), « dynamic-dns » (DNS dynamique), « extremism » (extrémisme), « gambling » (paris), « grayware », « hacking » (piratage), « insufficient-content » (contenu insuffisant), « malware », « newly-registered-domain » (domaine récemment enregistré), « parked » (en parking), « peer-to-peer », « phishing », « proxy-avoidance-and-anonymizers » (contournement par proxy et proxy anonymiseur), « questionable » (douteux), « unknown » (inconnu) et « weapons » (armes).
Sécurité DNS : « Command and Control Domains » (domaines de commande et contrôle), « Dynamic DNS Hosted Domains » (domaines hébergés à DNS dynamique), « Grayware Domains » (domaines hébergeant des graywares), « Malware Domains » (domaines hébergeant des malwares), « Newly Registered Domains » (domaines récemment enregistrés), « Parked Domains » (domaines en parking), « Phishing Domains » (domaines de phishing) et « Proxy Avoidance and Anonymizers » (contournement par proxy et proxy anonymiseur).
Protection antimalware : activée.
Protection IPS : activée pour l'évaluation des fonctions de protection contre les vulnérabilités.

Cisco :
Filtrage d'URL : « Command & Control Callbacks » (rappels du serveur de commande et contrôle) et « Phishing Attack » (attaque de phishing).
Sécurité DNS : « Malware », « Newly Seen Domains » (domaines récemment observés), « Command and Control Callbacks » (rappels du serveur de commande et contrôle), « Phishing Attacks » (attaques de phishing), « Dynamic DNS » (DNS dynamique), « Potentially Harmful Domains » (domaines potentiellement malveillants), « DNS Tunneling VPN » (VPN de DNS Tunneling) et « Cryptomining » (cryptominage).
Protection antimalware : activée.
Protection IPS : activée pour l'évaluation des fonctions de protection contre les vulnérabilités.

Zscaler :

Filtrage d'URL : « Anonymizers » (anonymiseurs), « Browser Exploits » (exploits sur navigateur), « Command & Control Servers » (serveurs de commande et contrôle), « Command & Control Traffic » (trafic de commande et contrôle), « Cookie Stealing » (vol de cookies), « Cryptomining » (cryptominage), « File Format Vulnerabilities » (vulnérabilités des formats de fichiers), « IRC Tunneling » (tunnels IRC), « Known Adware & Spyware Sites » (sites de spyware et adware connus), « Known Phishing Sites » (sites de phishing connus), « Malicious Content & Sites » (sites et contenus malveillants), « Potentially Malicious Requests » (requêtes potentiellement malveillantes), « Spyware Callback » (rappel de spyware), « SSH Tunneling » (tunnels SSH), « Suspected Phishing Sites » (sites de phishing potentiels), « Vulnerable ActiveX Controls » (contrôles ActiveX vulnérables), « Web Spam » (spam web), « Viruses » (virus), « Unwanted Applications » (applications indésirables), « Trojans » (chevaux de Troie), « Worms » (vers), « Ransomware », « Adware » et « Spyware ».
Sécurité DNS : « Phishing », « Malicious Content » (contenu malveillant), « Newly Registered Domains » (domaines récemment enregistrés) et « DNS Over HTTPS Services » (DNS sur services HTTPS).
Protection antimalware : activée.
Protection IPS : activée pour l'évaluation des fonctions de protection contre les vulnérabilités.

Droit d'auteur et avertissement

Pour en savoir plus sur AV-Comparatives et nos méthodologies de test, rendez-vous sur notre site web.

AV-Comparatives
(avril 2022)