The bridge to possible

Tableau comparatif des solutions SD-WAN

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Réseau							
Prise en charge du routage classique et du SD-WAN sur la même plateforme	✓ Services de routage classiques complets. Une migration fluide avec des fonctionnalités pertinentes pour le SD-WAN sur la même plateforme. Image unifiée commune au routage classique et au SD-WAN.	✗ Pas de protection des investissements pour une migration plus fluide par rapport au SD-WAN sur la même plateforme. Ensemble limité de fonctionnalités classiques pour le routage.	✓ L'utilisation d'un SD-WAN ne nécessite ni ajout de composant à votre infrastructure ni modification.	✗ Pas de protection des investissements pour une migration plus fluide par rapport au SD-WAN sur la même plateforme. Ensemble limité de fonctionnalités classiques pour le routage.	✗ L'utilisation d'un SD-WAN nécessite l'ajout de matériel.	✗ L'utilisation d'un SD-WAN ne nécessite ni ajout de composant à votre infrastructure ni modification. Ensemble limité de fonctionnalités classiques pour le routage.	✓ Migration fluide vers le SD-WAN sur la même plateforme. Services de routage classiques complets.
SD-WAN au cœur du réseau, à la périphérie et dans le cloud	✓ Appliances conçues pour le cœur du réseau, la périphérie et le cloud. Grand choix de formats avec des offres physiques et virtuelles.	✓ Appliances conçues pour le cœur du réseau, la périphérie et le cloud.	✓ Appliances conçues pour le cœur du réseau, la périphérie et le cloud.	✓ Appliances conçues pour le cœur du réseau, la périphérie et le cloud.	✓ Appliances conçues pour le cœur du réseau, la périphérie et le cloud.	✓ Appliances conçues pour le cœur du réseau, la périphérie et le cloud.	✓ Appliances conçues pour le cœur du réseau, la périphérie et le cloud.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Architecture SD-WAN personnalisée	Des composants d'évolutivité et de performance dédiés pour le plan de contrôle, le plan de données et le plan de gestion, offrant une architecture compatible SDN. Flexibilité pour adapter l'architecture à l'objectif de l'entreprise. Déploiement cloud et géré par l'équipe Cisco Cloud Ops.	Les composants intégrés des plans de contrôle et de données limitent la flexibilité.	Ancienne architecture basée sur un pare-feu.	Ancienne architecture combinant plan de contrôle et de données.	Des composants dédiés pour le plan de contrôle, le plan de données et le plan de gestion.	Les composants intégrés des plans de contrôle et de données limitent la flexibilité.	Les composants intégrés des plans de contrôle et de données limitent la flexibilité.
Provisionnement réellement automatique	Authentification mutuelle à plusieurs facteurs avec provisionnement automatique de tous les composants. Provisionnement facile pour les réseaux isolés et les fournisseurs de services managés (MSP).	**Capacité limitée** Le provisionnement nécessite des étapes d'authentification supplémentaires.	Plusieurs points de contact pour le processus de provisionnement automatique. Puisqu'il est basé sur un SD-WAN avec pare-feu, les politiques doivent être configurées manuellement.	**Capacité limitée** Les équipements EdgeConnect sont préconfigurés, mais requièrent des étapes d'authentification supplémentaires pour le provisionnement.	Plusieurs points de contact.	Les équipements ION sont préconfigurés pour s'authentifier sur le portail et prennent en charge le déploiement et le provisionnement automatiques.	**Capacité limitée** Le provisionnement nécessite des étapes d'authentification supplémentaires.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Topologie SD-WAN à routeur double actif-actif	Débit et fiabilité plus élevés avec une technologie de réseau active-active. Évolutivité horizontale avec des fonctionnalités faciles à utiliser.	Ne prend pas en charge les connexions actives-actives.	**Capacité limitée** Nécessite un commutateur WAN supplémentaire, ce qui crée des dépendances.	**Capacité limitée** Prend en charge le réseau actif-actif, mais nécessite un commutateur supplémentaire, ce qui crée des dépendances.	Ne prend pas en charge les connexions actives-actives.	Ne prend pas en charge les connexions actives-actives.	Prend en charge les connexions actives-actives.
Protocoles de routage avancés pour les intégrations Brownfield	Étend les informations sur le routage avancé, comme les protocoles EIGRP, OSPF, RIP et BGP, aux environnements cloud, permettant une connectivité plus rapide et plus fiable aux workloads cloud. Pris en charge par la pile double. Possibilité de routage sous-jacent/superposé. Prise en charge flexible des politiques et des attributs pour faciliter la manipulation du routage.	**Capacité limitée** Prend en charge les protocoles de routage avancés, comme BGP, OSPF, mais ne fournit pas la sélection de chemin d'accès la plus efficace.	Prend en charge les protocoles de routage avancés, comme BGP, OSPF, mais ne fournit pas la sélection de chemin d'accès la plus efficace.	**Capacité limitée** Prend en charge les protocoles de routage avancés comme BGP, mais ne prend pas en charge le routage avancé pour les protocoles tels qu'OSPF.	Prend en charge les protocoles de routage avancés, notamment BGP et OSPF.	**Capacité limitée** Prend en charge les protocoles de routage avancés, comme BGP, mais ne prend pas en charge les protocoles tels qu'OSPF.	Prend en charge les protocoles de routage avancés, dont BGP et OSPF, mais ne fournit pas la sélection de chemin d'accès la plus efficace.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Modèle de politique évolutif	La sélection dynamique du chemin permet aux applications critiques d'éviter automatiquement les problèmes de réseau. La microsegmentation et la gestion des politiques basée sur l'identité favorisent l'application cohérente des politiques multidomaines pour homogénéiser l'expérience des utilisateurs.	**Capacité limitée** Les politiques peuvent être transmises sous la forme de profils propres à chaque appareil, mais l'ingénierie du trafic pour le plan de données est limitée.	Les politiques pour le SD-WAN et le pare-feu sont gérées séparément, ce qui complique l'ingénierie du trafic et la transmission de politiques centralisées pour les plans de contrôle et de données.	**Capacité limitée** Les politiques peuvent être créées et réutilisées pour servir l'objectif de l'entreprise, mais la microsegmentation et l'application des politiques multidomaines sont limitées.	**Capacité limitée** Ingénierie de trafic possible sur la base de politiques sensibles aux applications, mais l'application des politiques multidomaines est limitée.	**Capacité limitée** Ingénierie de trafic possible sur la base de politiques sensibles aux applications, mais l'application des politiques multidomaines et les capacités de segmentation sont limitées.	Ingénierie de trafic possible sur la base des attributs de routage, de la politique de sécurité et de la politique applicative, mais l'application des politiques multidomaines est limitée.
Intégration SD-WAN/ SASE complète	Enregistrement et création automatisés des tunnels IPsec sur la passerelle Internet sécurisée Umbrella avec des workflows guidés sur vManage. Intégration complète avec Cisco AnyConnect, Cisco Duo, etc.	**Capacité limitée** À venir : workflows pour les fournisseurs de passerelles Internet sécurisées natives.	Pas de workflows guidés pour les intégrations de passerelles Internet sécurisées.	Aucune prise en charge de l'enregistrement automatique ou de la création de tunnels IPsec pour le SASE, car ils s'appuient sur des intégrations tierces.	Prise en charge de l'intégration SASE complète.	**Capacité limitée** Prise en charge de l'intégration SASE complète avec Prisma SD-WAN et Prisma Access. Intégration CloudBlades par API complexe. Pas de workflows guidés pour l'intégration de passerelles Internet sécurisées.	**Capacité limitée** Prise en charge de l'intégration SASE complète avec PAN-OS NGFW avec SD-WAN et Prisma Access. Pas de workflows guidés pour l'intégration de passerelles Internet sécurisées.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Optimisation WAN	Fournit des services d'optimisation WAN : optimisation TCP, élimination de la redondance des données, FEC et duplication des paquets.	**Capacité limitée** Fournit des services limités d'optimisation WAN, y compris FEC.	**Capacité limitée** Fournit des services limités d'optimisation WAN, y compris FEC.	Fournit des services d'optimisation WAN : optimisation TCP, élimination de la redondance des données et FEC.	**Capacité limitée** Fournit des services limités d'optimisation WAN, y compris FEC.	Ne fournit pas de services d'optimisation WAN.	**Capacité limitée** Fournit des services limités d'optimisation WAN : optimisation TCP, duplication des paquets et FEC.
Sécurité							
Services de sécurité on-premise pour sites distants et succursales (ROBO)	Des fonctionnalités de sécurité UTM entièrement intégrées dans vManage, y compris un pare-feu d'entreprise sensible aux applications, un système de prévention des intrusions Snort, le filtrage des URL, l'analyse de fichier AMP, la fonction de sandboxing Threat Grid, la sécurité Cisco Umbrella DNS, SSL et la Threat Intelligence de Talos.	**Capacité limitée** Pare-feu de base stateful	Fonctionnalités de pare-feu de nouvelle génération (NGFW) intégrées avec capacités de prévention des intrusions (IPS), d'IDS, de contrôle des applications et AMP.	Aucune fonctionnalité de sécurité dans la console SD-WAN.	Fonctionnalités de pare-feu de nouvelle génération (NGFW) intégrées avec capacités de prévention des intrusions (IPS), d'IDS, de contrôle des applications et AMP.	**Capacité limitée** Offre uniquement un pare-feu de base basé sur les zones. Aucune fonctionnalité de sécurité intégrée comme l'IPS, l'IDS, AMP et le filtrage d'URL.	Fonctionnalités de pare-feu de nouvelle génération intégrées avec fonctionnalités d'IPS, d'IDS, de contrôle des applications, AMP, de filtrage des URL et de sécurité DNS. Nécessite une licence supplémentaire.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Circuits intégrés personnalisés	La technologie « Silicon root of trust » personnalisée dans le matériel fournit une protection intégrée contre les attaques visant les fondations du réseau et les portes dérobées. Les routeurs Cisco vEdge sont équipés d'une puce Trusted Platform Module (TPM) installée en usine avec un certificat signé. Cette sécurité intégrée assure l'authentification automatisée et infaillible de tout nouveau routeur vEdge se connectant au réseau et constitue un atout majeur lors du déploiement de dizaines de milliers de terminaux.	**Capacité limitée** Matériel professionnel standard prêt à l'emploi sans solution de protection intégrée connue.	**Capacité limitée** Circuits intégrés personnalisés avec protection intégrée inconnue.	Matériel professionnel standard prêt à l'emploi sans solution de protection fiable connue.	Matériel professionnel standard prêt à l'emploi sans solution de protection fiable connue.	Matériel professionnel standard prêt à l'emploi sans solution de protection fiable connue.	Matériel professionnel standard prêt à l'emploi sans solution de protection fiable connue.
Segmentation	Une segmentation complète de type MPLS/VRF ayant fait ses preuves, avec prise en charge des topologies multisegments et de la mutualisation.	**Capacité limitée** Segmentation de type VRF, sans création de topologies multisegments dynamiques et flexibles.	**Capacité limitée** Capacités de segmentation limitées avec configurations VDOM complexes, sans création de topologies multisegments dynamiques et flexibles.	**Capacité limitée** Segmentation de type VRF, routage limité avec le protocole OSPF et priorité des pairs.	Segmentation éprouvée et évolutive de type MPLS/VRF de la couche 2 à la couche 7.	**Capacité limitée** Fonctionnalités de segmentation limitées.	**Capacité limitée** Offre une segmentation évolutive de type VRF, mais pas de création de topologies multisegments flexibles.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Analyse du trafic chiffré	Peut détecter les malwares en faisant correspondre les modèles SHA chiffrés sans déchiffrement.	Détection impossible des malwares chiffrés.	**Capacité limitée** Solution d'analyse du trafic chiffré pas assez robuste pour les infrastructures/ périphériques réseau.	Détection impossible des malwares chiffrés.	Assure le chiffrement du trafic TLS/SSL.	Détection impossible des malwares chiffrés.	Peut détecter les malwares en déchiffrant, inspectant et contrôlant les connexions SSL et SSH entrantes et sortantes.
Threat Intelligence	Une solution de Threat Intelligence mondialement reconnue (TALOS) avec la possibilité de déployer des services de réponse aux incidents.	Aucune solution de Threat Intelligence.	Fonctionnalités de Threat Intelligence.	Aucune solution de Threat Intelligence.	Threat Intelligence et surveillance des menaces.	Aucune solution de Threat Intelligence.	Fonctionnalités de Threat Intelligence sous la forme de module complémentaire.
Cloud							
Connectivité SaaS	L'indépendance du transport permet de sélectionner de manière intelligente les chemins vers les principales applications SaaS en fonction des indicateurs de performance et du meilleur chemin, notamment Office 365, la passerelle Internet sécurisée, l'équilibrage de la charge, Cisco Webex, etc.	**Capacité limitée** Optimisation SaaS basée sur la création manuelle de règles d'application grâce aux chemins d'accès haut débit DIA vers les data centers partagés.	**Capacité limitée** Optimisation SaaS de base avec création manuelle de SLA pour chaque application.	L'indépendance du transport permet la sélection intelligente des chemins vers les principales applications SaaS en fonction des indicateurs de performance et de la sélection du meilleur chemin.	**Capacité limitée** Optimisation SaaS de base avec création manuelle de SLA pour chaque application.	**Capacité limitée** Optimisation SaaS de base avec création manuelle de règles pour chaque application.	**Capacité limitée** Optimisation SaaS de base avec création manuelle de SLA pour chaque application. L'optimisation SaaS avancée nécessite une plateforme de sécurité SaaS supplémentaire.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Connectivité IaaS	Workflows guidés pour le déploiement automatisé de Cisco SD-WAN Cloud OnRamp pour la connectivité IaaS.	**Capacité limitée** Soit des passerelles manuelles, soit des ressources partagées. Automatisation uniquement avec Microsoft Azure vWAN.	Configuration manuelle de la passerelle.	**Capacité limitée** Soit des passerelles manuelles, soit des ressources partagées.	**Capacité limitée** Soit des passerelles manuelles, soit des ressources partagées.	**Capacité limitée** Passerelles manuelles, ressources partagées ou intégration d'API complexe via CloudBlades.	**Capacité limitée** Soit des passerelles manuelles, soit des ressources partagées.
Passerelles de data center partagé/cloud	Gestion simplifiée du réseau avec agrégation du trafic via les concentrateurs de data center partagé vers les workloads cloud, avec workflows guidés pour le déploiement automatisé.	**Capacité limitée** Agrégation colocalisée limitée.	**Capacité limitée** Agrégation colocalisée limitée.	**Capacité limitée** Agrégation colocalisée limitée.	**Capacité limitée** Agrégation colocalisée limitée.	**Capacité limitée** Agrégation colocalisée limitée.	**Capacité limitée** Agrégation colocalisée limitée.
Connectivité multicloud	Processus guidé pour un déploiement automatisé sur les clouds de plusieurs fournisseurs, comme Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).	**Capacité limitée** Partenariat avec Microsoft Azure vWAN. Workflows guidés.	Workflows limités pour la connectivité multicloud.	**Capacité limitée** Déploiement manuel sur les clouds de différents fournisseurs.	**Capacité limitée** Déploiement manuel sur les clouds de différents fournisseurs.	**Capacité limitée** Déploiement manuel sur les clouds de différents fournisseurs ou via une intégration complexe de l'API CloudBlades.	**Capacité limitée** Déploiement manuel sur les clouds de différents fournisseurs.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Périphérie							
Stockage	Fournit une automatisation IoT/OT avec capacités de stockage et de calcul intégrées pour les sites distants. Pris en charge par la gamme de commutateurs Cisco Catalyst 8200.	**Capacité limitée** Possibilité de déployer des VNF sur les appliances VMware SD-WAN Edge.	Aucune fonctionnalité d'hébergement de VNF en périphérie du réseau.	Aucune fonctionnalité d'hébergement de VNF en périphérie du réseau.	**Capacité limitée** Possibilité de déployer des VNF sur les appliances Versa SD-WAN Edge.	Aucune fonctionnalité d'hébergement d'applications en périphérie du réseau.	Aucune fonctionnalité d'hébergement d'applications en périphérie du réseau.
Visibilité multicloud	Visibilité sur les environnements Internet, cloud et SaaS avec l'intégration native de Cisco ThousandEyes sur les plateformes Cisco Catalyst 8200 et Cisco Catalyst 8300 Edge compatibles.	**Capacité limitée** Aucune fonctionnalité d'hébergement d'applications en périphérie du réseau. Possibilité de déployer des VNF sur les appliances VMware SD-WAN Edge.	Aucune fonctionnalité d'hébergement d'applications en périphérie du réseau.	Aucune fonctionnalité d'hébergement d'applications en périphérie du réseau.	**Capacité limitée** Aucune fonctionnalité d'hébergement d'applications en périphérie du réseau. Possibilité de déployer des VNF sur les appliances Versa SD-WAN Edge.	Visibilité sur Internet, dans le cloud et le SaaS avec l'intégration native de Prisma Access ADEM.	**Capacité limitée** Intégration avec Prisma Access nécessaire pour profiter d'une bonne visibilité sur Internet, le cloud et le SaaS via ADEM, ce qui complexifie l'intégration.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Aucune intégration VoIP native.	Les plateformes Cisco Catalyst 8000 Edge offrent des services VoIP complets dans le SD-WAN et pour les piles de fonctions logicielles IOS XE classiques. Cisco est le seul fournisseur de SD-WAN à intégrer nativement une adresse IP analogique/numérique directement dans un CPE unique. En mode SD-WAN, les commutateurs Cisco Catalyst 8300 évitent également les interruptions internes et externes via le mécanisme SRST. Cette gamme prend toujours en charge une longue liste de scénarios d'utilisation IOS XE classiques.	**Capacité limitée** Aucune fonctionnalité d'hébergement d'applications en périphérie du réseau. Possibilité de déployer des VNF sur les appliances VMware SD-WAN Edge.	Aucune fonctionnalité d'hébergement d'applications en périphérie du réseau.	Aucune intégration native de la voix.	Aucune intégration native de la voix.	Aucune intégration native de la voix.	Aucune intégration native de la voix.
Solutions LTE avancées	Fonctionnalités cellulaires avancées en tant que principale liaison de transport prises en charge grâce à la flexibilité de déploiement permise par le module intégré, la carte ou la passerelle externe de la gamme Cisco Catalyst 8000.	Fonctionnalités cellulaires en tant que liaison de transport.	Fonctionnalités cellulaires en tant que liaison de transport.	Aucune prise en charge cellulaire majeure.	**Capacité limitée** Aucune prise en charge cellulaire majeure. Prise en charge cellulaire sur certains modèles (CSG1000).	**Capacité limitée** Prise en charge cellulaire sur certains modèles (un modèle ION 1200).	Prise en charge des fonctionnalités cellulaires dans les pare-feu de nouvelle génération 5G.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
SD-WAN industriel	✓ Options de SD-WAN renforcées pour les environnements industriels et difficiles.	✗ Aucune option de SD-WAN renforcée.	✓ Options de SD-WAN renforcées.	✗ Aucune option de SD-WAN renforcée.	✗ Aucune option de SD-WAN renforcée.	✗ Aucune option de SD-WAN renforcée.	✓ Options de SD-WAN renforcées.
Compatibilité Wi-Fi/5G	✓ Utilise une technologie avancée de protocole et de fréquence sans fil.	✓ Utilise une technologie avancée de protocole et de fréquence sans fil.	✓ Utilise une technologie avancée de protocole et de fréquence sans fil.	✗ Aucune fonctionnalité sans fil avancée.	✓ Utilise une technologie avancée de protocole et de fréquence sans fil.	✗ Aucune fonctionnalité sans fil avancée. Dépendance vis-à-vis de tiers pour l'activation des fonctionnalités.	✗ Aucune fonctionnalité sans fil avancée. Dépendance vis-à-vis de tiers pour l'activation des fonctionnalités. Dispose de pare-feu de nouvelle génération compatibles avec la 5G.
Intégration du data center (politiques communes entre les domaines)	✓ Intégrations interdomaines, politiques QoS communes entre Cisco ACI et SD-WAN. Extension des balises des groupes de sécurité (SGT) et des métadonnées TrustSec du réseau WAN jusqu'au réseau local et au data center.	✓ Unification des politiques du data center et des besoins à la périphérie du réseau.	✗ Aucune intégration du data center.	✗ Aucune intégration du data center.	✗ Aucune intégration du data center.	✓ Aucune intégration interdomaine.	✓ Aucune intégration interdomaine.

The bridge to possible

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
Microsegmentation	Prise en charge de la microsegmentation et de l'application des politiques via des balises de groupe évolutives pour les groupes d'utilisateurs.	**Capacité limitée** Microsegmentation de la couche 2 et application des politiques minimales.	**Capacité limitée** Microsegmentation de la couche 2 et application des politiques minimales.	Prise en charge de la microsegmentation et de l'application des politiques via des zones évolutives.	Prise en charge de la microsegmentation et de l'application des politiques via des zones évolutives.	Pas de microsegmentation ni d'application des politiques.	Prise en charge de la microsegmentation et de l'application des politiques via des zones évolutives.

C83-743414-01 11/21