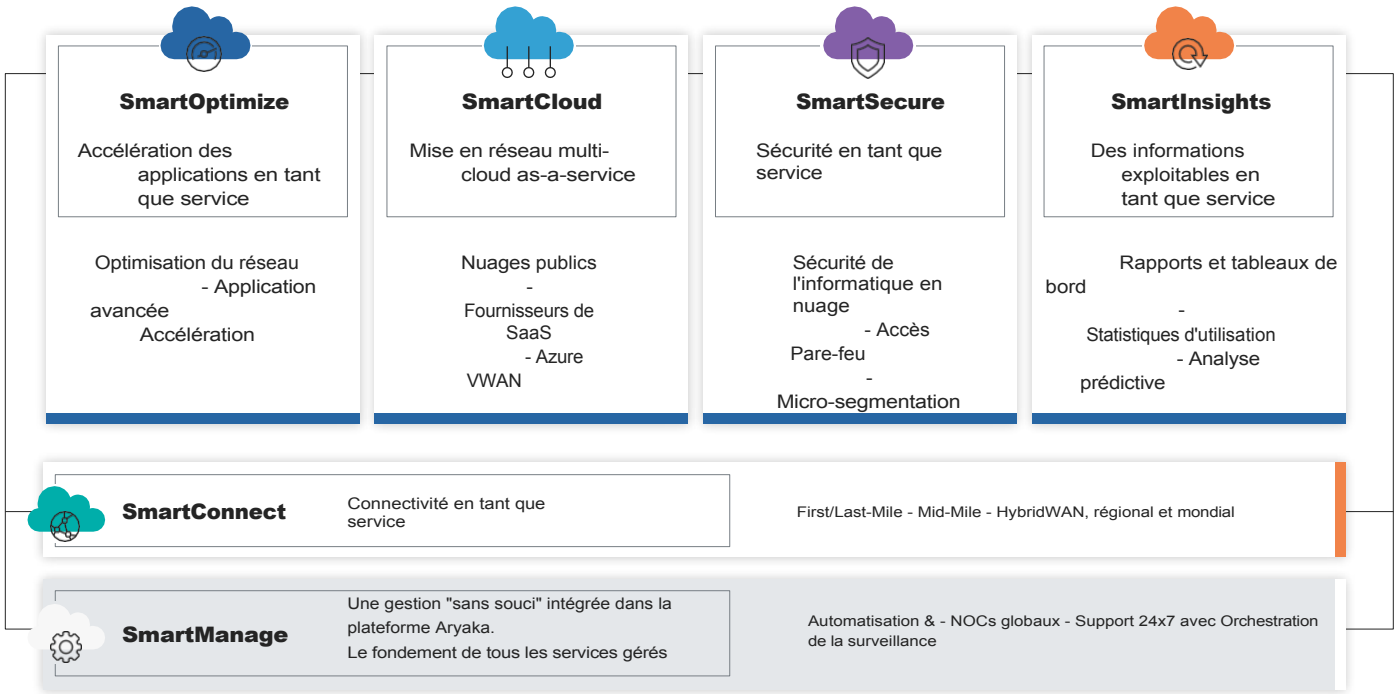
Fiche technique du point d'accès réseau Aryaka (ANAP)

Fiche technique ANAP

L'ANAP (Aryaka Network Access Point) d'Aryaka est une appliance qui offre une solution de branche virtuelle définie par logiciel (SD-Branch) et fait partie des SmartServices d'Aryaka. Il regroupe plusieurs connexions WAN et fournit des services de réseau convergents, notamment le routage, le cryptage, la sécurité et la gestion du trafic. ANAP prend également en charge la redondance avec des options de configuration de haute disponibilité.

Aperçu de la solution Aryaka



L'appliance ANAP d'Aryaka aide les entreprises à simplifier leurs succursales en consolidant le réseau et la sécurité en un seul dispositif défini par logiciel et géré dans le cloud, éliminant ainsi le besoin d'une multitude d'appliances distinctes et spécifiques à une fonction. L'ANAP d'Aryaka est la rampe d'accès au réseau global géré d'Aryaka.
La solution de réseau d'entreprise SD-WAN intègre des fonctions avancées de réseau, d'optimisation et d'accélération des applications ainsi que de sécurité.

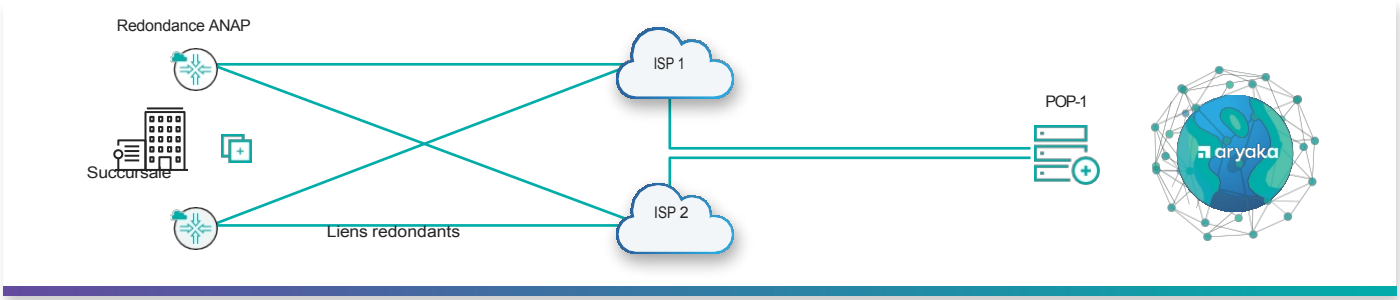
La famille de produits ANAP se compose d'appliances basées sur une architecture de boîte blanche extrêmement adaptable exécutant le système d'exploitation Linux standard de l'industrie, qui fournit une virtualisation intégrée (KVM) et une technologie de conteneurisation pour prendre en charge les fonctions de réseau virtuelles (VNF).

Grâce à l'ANAP d'Aryaka, les entreprises peuvent fournir une connectivité de niveau professionnel aux sites distants (qui manquent souvent de personnel informatique qualifié) en moins de 48 heures en tirant parti du modèle ZTD (Zero Touch Deployment) de l'ANAP. Déploiement sans contact
Le déploiement signifie que les appliances sont simplement envoyées à n'importe quel endroit sans qu'il soit nécessaire de les configurer au préalable. La solution SD-WAN gérée d'Aryaka aide les entreprises à réduire les dépenses d'investissement et les dépenses d'exploitation de leur infrastructure WAN et de leurs succursales, tout en assurant une performance supérieure des applications ainsi qu'une connectivité optimale au cloud.

Avantages

- **Simplicité de déploiement et conception intégrée :** L'ANAP d'Aryaka est préconfiguré et peut être facilement mis en œuvre grâce à un modèle de déploiement sans intervention.
- **Solution définie par logiciel :** Construit sur un système d'exploitation Linux renforcé, l'ANAP d'Aryaka met en œuvre des services de réseau, d'optimisation des applications et de sécurité en tant que fonctions logicielles, évitant ainsi l'obsolescence intégrée des architectures personnalisées.
- **SD-WAN intégré : l'**ANAP d'Aryaka fait partie intégrante des SmartServices d'Aryaka. Il aide les entreprises à tirer parti de n'importe quel transport du dernier kilomètre (MPLS, Internet renforcé) et peut tirer parti du réseau central de haute qualité d'Aryaka pour atteindre les niveaux de qualité de service MPLS.
- Support **HybridWAN** offrant des options Aryaka L2 Core, MPLS, internet site à site et internet public.
- Prise en charge **intégrée** du réseau étendu virtuel Azure.
- **Sécurité intégrée :** L'ANAP met en œuvre un pare-feu L3/4 avec état pour contrecarrer les attaques contre la succursale. Il met également en œuvre la segmentation du trafic de la succursale : le trafic de l'entreprise est strictement séparé des autres types de trafic tels que le trafic DMZ ou le trafic WiFi invité. L'ANAP prend également en charge les pare-feu virtuels basés sur NFV des fournisseurs de sécurité de niveau 1.
- **Redondance :** La prise en charge de la redondance des liens (doubles liens ISP) et des dispositifs (VRRP) permet de répondre aux exigences de très haute disponibilité (voir illustration). La fonction Fail-to-wire est prise en charge pour le mode inline.
- **Meilleure expérience utilisateur :** Performances déterministes et prévisibles pour les applications résidant dans le centre de données ou dans le nuage.
- **Solution multi-locataires :** L'ANAP d'Aryaka prend en charge jusqu'à 32 locataires grâce à la micro-segmentation.
- Options de **déploiement flexibles** pour **les succursales**, y compris en ligne, en mode routé simple, hybride et routé en périphérie.
- **Une plus grande souplesse :** Déploiement et exploitation plus rapides et plus faciles de votre SD-WAN géré, avec des performances accrues en utilisant moins de bande passante. Ajoutez de nouveaux services générateurs de revenus en quelques minutes et non en quelques mois.

Redondance ANAP



Spécifications du matériel

	ANAP 1500	ANAP 2500/2600	ANAP 3000	ANAP 10000
Largeur de bande	Jusqu'à 150 Mbps	Jusqu'à 650 Mbps	Jusqu'à 1 Gbps	Jusqu'à 3Gbps
Type d'interface	Cuivre	Cuivre	Cuivre/fibre	Cuivre/fibre
Capacité NFV	Non	Non/oui	Oui	Oui
QoS / WAN	Oui	Oui	Oui	Oui
Optimisation	Oui	Oui	Oui	Oui
Routage	Oui	Oui	Oui	Oui
Sécurité des bords	Oui	Oui	Oui	Oui
Sécurité de l'informatique en nuage	Oui	Oui	Oui	Oui
Connecteurs	Oui	Oui	Oui	Oui
Contrôle	Oui	Oui	Oui	Oui
Recommandé pour	Petits sites	Sites de taille moyenne	Grands sites	Grands sites

Points forts de l'architecture ANAP

- Qualité de service

Classification et marquage	Marquage IP basé sur 5 tuiles Classification basée sur DSCP/ToS Recherche DNS Recherche SNI DPI (Deep Packet Inspection)
Mise en forme des classes de service Mise en forme TCP/IP	5 classes de service avec réservation/limites de bande passante File d'attente et mise en forme hiérarchiques basées sur un panier de jetons Mise en forme avancée au niveau du flux TCP-IP avec deux classes Partage de la capacité de liaison ASN inutilisée avec le trafic internet de faible priorité Pris en charge par ERM uniquement et activé par défaut
Qualité de service adaptative	

- Optimisation du réseau étendu

TCP Boost réseau étendu (WAN)	Minimiser la latence et éviter la congestion sur le dernier kilomètre grâce au contrôle du débit du
ARR	Algorithmes brevetés de compression et de déduplication des données

- Routage

eBGP	Support eBGP avec sélection du chemin préféré en utilisant les attributs AS PATH Prepend et MED (Multi-Exit Discriminator) Prise en charge des communautés MP-BGP et BGP
RIP allégé (T-RIP)	Annonces de routage conformes à RIPv2.0 pour simplifier la configuration du routage
Routage statique	Configuration d'itinéraires statiques pour les sous-réseaux locaux, la passerelle par défaut et la passerelle du tunnel IPSec Décision de transfert basée sur des critères de correspondance de 6 tuiles et/ou sur le DNS
Routage basé sur des règles	- Renvoi vers le réseau local - Renvoi vers Internet - Renvoi vers Aryaka - Abandon
Routage basé sur la politique de l'adresse source	Transférer les paquets en fonction de l'adresse source IP
Filtres de routes d'Internet.	Contrôle granulaire de la politique de 6-tuple pour transférer/abandonner le trafic d'Aryaka et

- Redondance

Redondance des bords	Double tunnel IPSec vers différents FAI pour la redondance des liaisons
VARP (Virtual ANAP Redundancy Protocol)	Modèle de type VRRP pour la redondance ANAP dans le modèle actif-standby
Tunnels de sauvegarde ANAP-to-ANAP	Tunnels IPSEc directs entre ANAP sur l'internet dans le cas improbable où le tunnel primaire Aryaka échoue.
Redondance des liens ISP	SMARTlink permet l'utilisation de 2 liens ISP dans une configuration active-active • Sélection du chemin : Routage sélectif à travers les liens • Équilibrage de la charge : Distribuer le trafic sur les liaisons en fonction des paquets. • FEC : Réplique ou duplication du trafic sur les liaisons pour récupérer les paquets perdus. • Relecture temporisée : les flux peuvent être rejoués au sein d'une liaison après un certain délai, afin de récupérer les paquets perdus. • Récupération de la perte de chemin (PLR) : Introduit un mécanisme de retour d'information entre le POP et l'ANAP pour déterminer les paquets exacts perdus pendant la transmission et récupérer ces paquets.
Redondance des liens MPLS	Double tunnel MPLS avec déploiement redondant de l'ANAP

Prise en charge du NAT	Suivi des flux en fonction des politiques NAT • Prise en charge de la NAT à la source - NAT 1 à 1, IP et port dynamiques

Pare-feu et segmentation des branches	Pare-feu à états L3/ L4 pour le pare-feu périmétrique et la segmentation Est-Ouest Segmentation
Multi-Tenancy	Prise en charge de l'utilisation multiple grâce à la microsegmentation basée sur VRF
Check Point	Hosted VM Next Generation Firwewall as VNF (Virtual Network Function) Palo Alto
Networks	Hosted VM Next Generation Firwewall comme VNF (Virtual Network Function) Zscaler
	Support IPSec IKev1 (en plus des tunnels GRE)
VLAN privés Durcissement de l'ANAP SEC-2	Possibilité de regrouper un ensemble de VLAN et de restreindre l'accès à l'internet Processus d'amorçage ANAP sécurisé avec image ANAP sécurisée

- Connecteurs de sécurité pour l'informatique en nuage

Check Point	Tunnels IPsec IKEv1, IKEv2 ou GRE
	Routage basé sur des règles entre le trafic lié à Internet, Aryaka et Check Point CloudGuard Connect
CloudGuard Connect	MyAryaka pour la surveillance de la connectivité des tunnels vers Cloudguard Connect
Zscaler	Prise en charge des tunnels GRE redondants Routage basé sur une politique entre Internet, Aryaka et le trafic lié à Zscaler Prise en charge de MyAryaka pour la visibilité et la configurabilité
Palo Alto Prisma Prisma	Tunnel IPsec basé sur IKEv1 Routage basé sur une politique entre Internet, Aryaka et Palo Alto
	Alto Prisma bound traffic MyAryaka support pour la visibilité et la configurabilité
Symantec	Tunnel IPsec basé sur IKEv1 Routage basé sur des règles entre Internet, Aryaka et le trafic lié à Symantec Prise en charge de MyAryaka pour la visibilité et la configurabilité

- Contrôle

Syslog	Journaux de flux pour les paquets acheminés entre le réseau local, l'internet et les
	sites d'Aryaka Journaux de flux pour les paquets abandonnés en raison de
	politiques ou de règles de pare-feu Journaux système
	Prise en charge de la RFC 5424
	Enregistrement d'attributs basé sur des paires de clés et de valeurs
	pour une analyse plus facile Prise en charge de la connectivité UDP et
	TCP avec le collecteur
Netflow	Prise en charge des versions 1,5 et 9 de NDE. La valeur par défaut est 9.
	Possibilité de surveiller le trafic du réseau local, de l'Internet, des connecteurs de sécurité dans le nuage et d'Aryaka. Taux d'échantillonnage 1:1
	Les informations sur le débit sont téléchargées vers ANAP et MyAryaka toutes les 300 secondes.

- Prise en charge de la fonction de réseau virtuel

Machine virtuelle hébergée (VM)	Prise en charge de machines virtuelles tierces via Linux KVM

aryaka +1.888.692.7925 |info@aryaka.com

Réserver une démonstration Voir la démo interactive

Aryaka est le leader dans la fourniture de SASE unifié en tant que service, une solution entièrement intégrée combinant le réseau, la sécurité et l'observabilité. Conçue pour répondre aux exigences de l'IA générative ainsi qu'au monde hybride multi-cloud d'aujourd'hui, Aryaka permet aux entreprises de transformer leur réseau sécurisé pour offrir des performances, une agilité, une simplicité et une sécurité sans compromis. Les options de livraison flexibles d'Aryaka permettent aux entreprises de choisir leur approche préférée pour la mise en œuvre et la gestion. Des centaines d'entreprises internationales, dont plusieurs figurent dans le classement Fortune 100, font confiance à Aryaka pour leurs solutions de réseaux sécurisés. Pour plus d'informations sur Aryaka, veuillez consulter le site www.aryaka.com.

À propos d'Aryaka