

Voir Comprendre Partager

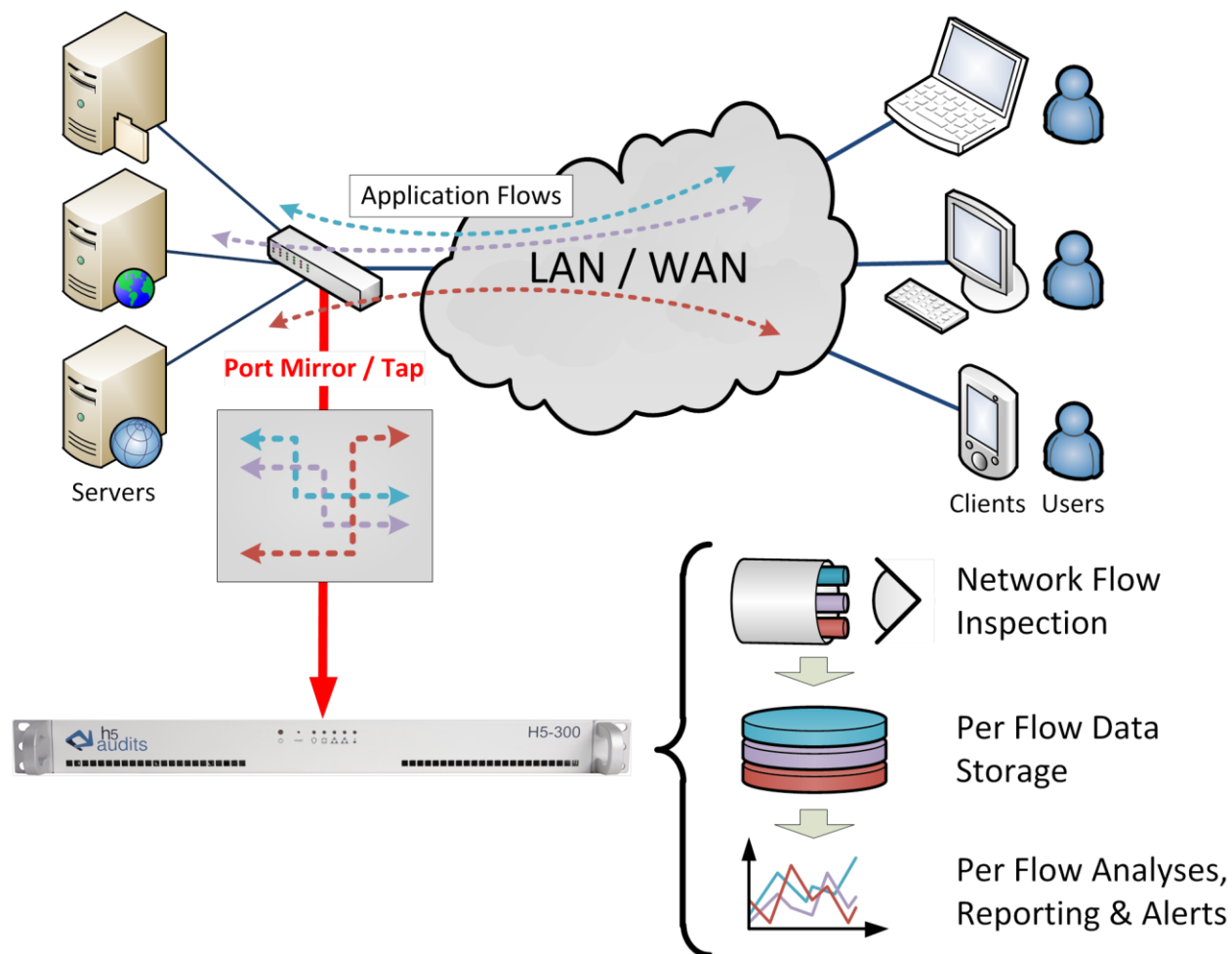
Un nouvel enjeu pour l'entreprise : une visibilité immédiate, complète et intuitive des flux du système d'information.

Afin d'améliorer de l'administration de leur réseau IP qui doit supporter la convergence de communications et d'applications en proie à une évolution et une explosion des usages, les entreprises, les fournisseurs de services et les administrations ressentent un besoin vital de disposer d'une visibilité réseau instantanée, complète et intuitive. De plus la visibilité des flux réseau en croissance constante tant en terme de volume que de complexité doit pouvoir être fournie aux équipes informatiques à un coût d'investissement et d'exploitation réduit.

La Vision H5 Audits: une technologie dédiée à la visibilité des flux réseau.

Prenant appui sur 20 années d'expérience en audits et services de conseil sur le marché entreprise, les équipes recherche-développement de H5 audits ont mis au point une technologie innovante qui permet aux entreprises, aux fournisseurs de services et aux administrations d'étendre et d'améliorer la visibilité des applications qui circulent sur le réseau. Avec les appliances H5, les équipes informatiques peuvent déployer une architecture logicielle et matérielle complète et facile à utiliser qui leur permet de suivre en temps réel le comportement des applications réseau.

La solution introduite par les appliances H5 fournissent ainsi une solution de visibilité puissante à destination non seulement des équipes réseau mais aussi aux managers en charge de la construction et de l'évolution du réseau et au helpdesk responsable du support quotidien aux utilisateurs.



Managers	Réseau	Help Desk
<p>Réduction des risques</p> <p>Aide à la décision</p> <p>Amélioration de la collaboration entre les différentes fonctions de l'IT</p>	<p>Isolation des causes des incidents</p> <p>Optimisation de l'infrastructure</p> <p>Accélération de la résolution des incidents</p> <p>Réduction des risques opérationnels</p>	<p>Alerte rapide sur incident</p> <p>Amélioration de la productivité</p> <p>Optimisation des procédures d'escalade</p>

H5 appliance
Une architecture logicielle unique pour la visibilité réseau

L'appliance H5: la visibilité réseau sécurisée, intuitive et économique.

L'appliance H5 peut être déployée en quelques minutes; installée sur le port miroir d'un commutateur ou sur une Tap réseau, l'installation et la mise en service ne demandent aucune modification ni interruption du système d'information.

Avec l'inspection temps réel du trafic l'appliance H5 est capable, sans aucune configuration ni mise au point particulière, de fournir les premiers rapports et données de flux réseau immédiatement après installation.

L'appliance H5: architecture tout en un puissante et évolutive.

L'appliance H5 ne demande aucun portail de reporting ni stockage externe de données. L'extraction des données de flux réseau, leur stockage et leur présentation à l'utilisateur sont intégralement fournis par appliance.

L'appliance H5 capture et analyse le trafic, extrait et les données des applications pour chaque flux de chaque nœud IP actif sur le réseau jusqu'à 10Gbps sans aucune perte.

H5 audits

Energy 4, 155-159 rue du Docteur Bauer
93400 Saint-Ouen
Tel : +33 1 49 48 12 00
Fax : +33 1 49 48 12 04
info@h5audits.com

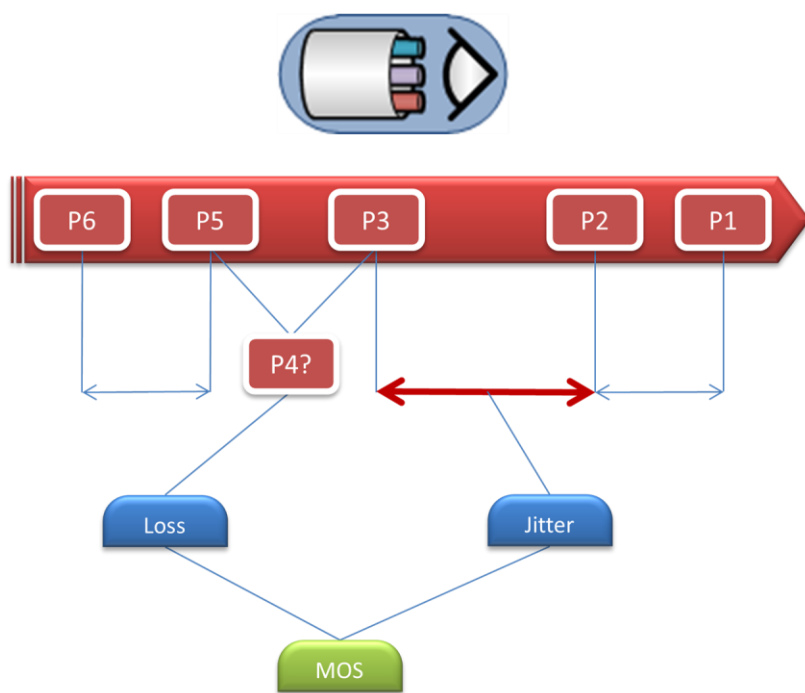
Le monitoring « Advanced Layer 4 » : une solution de visibilité réseau de bout en bout.

Un monitoring efficace de la performance des applications réseau dépend de la bonne exécution de deux tâches essentielles: le calcul en temps réel, des métriques de performance applicative et la détection et le suivi des objets réseau à une profondeur et une granularité appropriées.

Le choix de H5 audits s'est porté sur le développement exhaustif d'un ensemble de métriques de couche 4 en conformité avec les standards IETF (TCP, UDP, RTP, etc.) largement acceptés est utilisés dans l'industrie. Les métriques calculées par les appliances H5 permet ainsi aux administrateurs de mettre en place des stratégies évoluées de surveillance et de suivi de leurs applications réseau sans risque de s'enfermer dans une technologie propriétaire.

Par ailleurs, les appliances H5 identifient les nœuds réseau par leur adresse IP et le marquage VLANs de leur trafic et enregistrent et agrègent 100% des conversations les plus importantes sur le réseau sans la perte d'information inhérente aux solutions d'analyse de session propriétaires, complexes et moins fiables.

Fort de ces deux choix structurants, H5 audits a su bâtir une solution fiable et puissante où une seule appliance permet de suivre en temps réel le comportement des applications réseau mais aussi d'analyser dans le détail les événements et les situations du système d'information en temps réel ou différé et en collaboration avec les outils de monitoring des applications et de l'infrastructure.



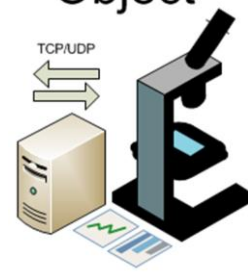
Métriques RTP pour la voix sur IP

Agrégation des données au cours du temps

Une fois calculées les métriques des conversations IP sont immédiatement insérées en base de données pour une exploitation immédiate. La rétention de ces informations au cours de grandes périodes de temps est assurée par un processus d'agrégation temporelle robuste intelligent. Ce processus réduit la granularité temporelle des données de chaque conversation. Les équipes réseau peuvent ainsi suivre le trafic de nœuds IP sur plusieurs mois et effectuer des comparaisons de comportement sur différents intervalles de temps.



Watched Object



Business Flow

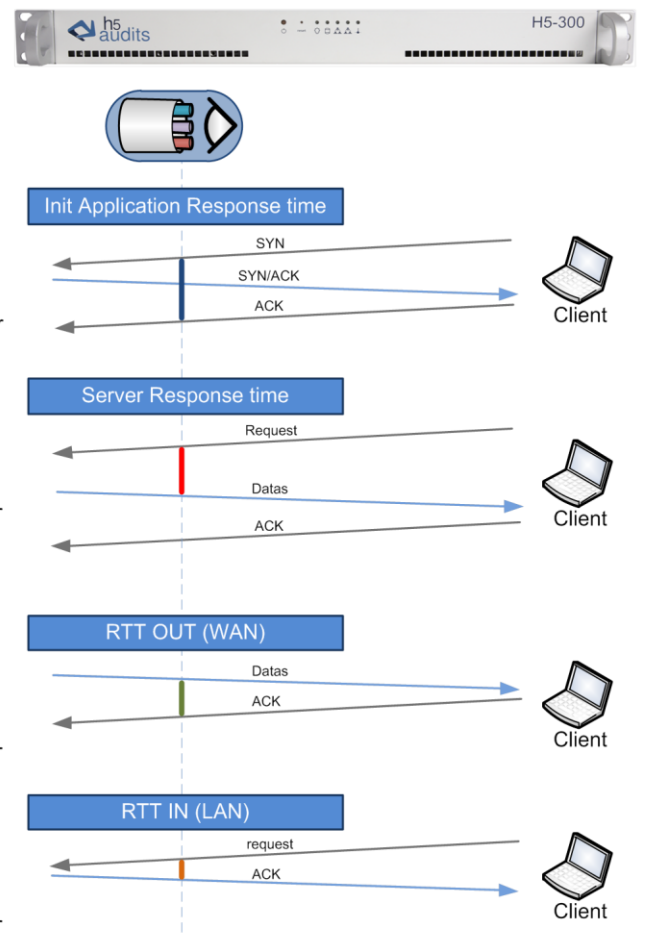
Objets surveillés et flux métier

Par défaut, toutes les conversations IP sont traitées de manière égalitaire, l'appliance H5 mettant naturellement en valeur les conversations au volume de trafic le plus important. Afin d'obtenir une visibilité qui reflète l'architecture réseau et l'organisation d'entreprise l'appliance H5 propose deux solutions complémentaires :

Avec les **objets surveillés** les administrateurs réseau peuvent importer sur l'appliance H5 l'ensemble de leur plan d'adressage. Les sites distants, les filiales ou les fermes de serveurs, même sur un faible volume de trafic, peuvent ainsi faire l'objet d'un suivi particulier et d'un calcul de métriques associé au groupe de nœuds IP qu'ils représentent.

Avec les **flux métier**, en complément ou non avec les objets surveillés, les managers réseau peuvent isoler une application particulière et suivre son comportement au cours du temps.

Les objets surveillés et les métiers permettent tout deux à l'entreprise de personnaliser la base de données de monitoring H5 et les rapports qui en découlent.



Métriques TCP pour la performance des applications Performance Applicative

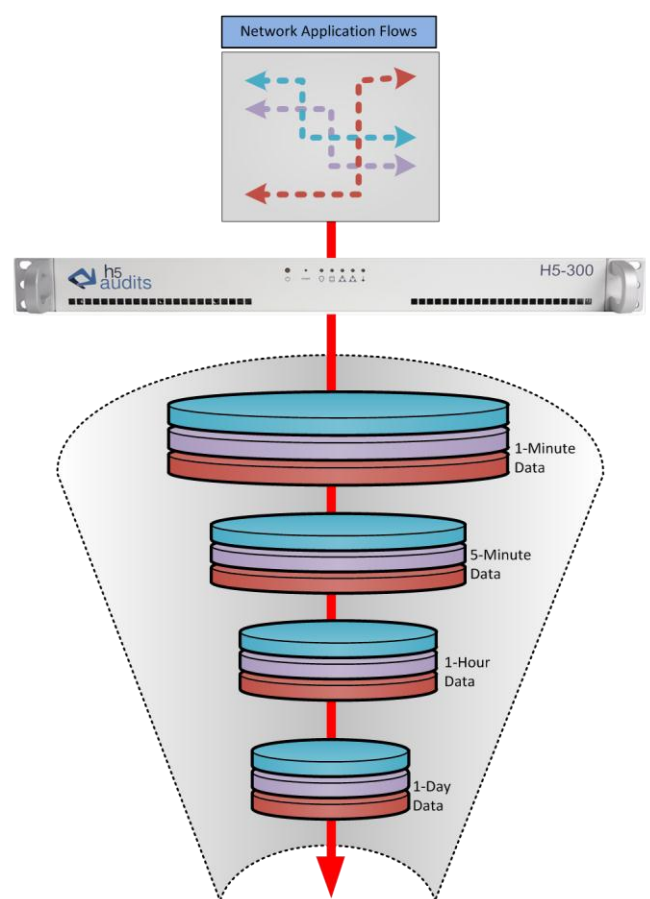
Avec plus de 50 métriques TCP et UDP calculées en temps réel à partir de chaque flux applicatif sur le réseau, les appliances H5 fournissent aux équipes réseau l'information la plus fiable et la plus efficace sur le comportement et la qualité de service perçue par chaque utilisateur.

Les pics des métriques TCP « Temps de réponse serveur » et « Temps d'aller et retour réseau » permettent aux équipes réseau d'isoler, sur la durée et dans un nuage de milliers de conversations les situations de trafic anormal et de performances dégradées.

Les métriques asymétriques – ayant une signification différente dans le sens WAN et dans le sens LAN ou encore dans le sens client et dans le sens serveur permettent quant à eux en corrélation avec les outils de monitoring d'infrastructure d'isoler et de circonscrire le périmètre des incidents réseaux.

La mesure de qualité perçue voix sur IP

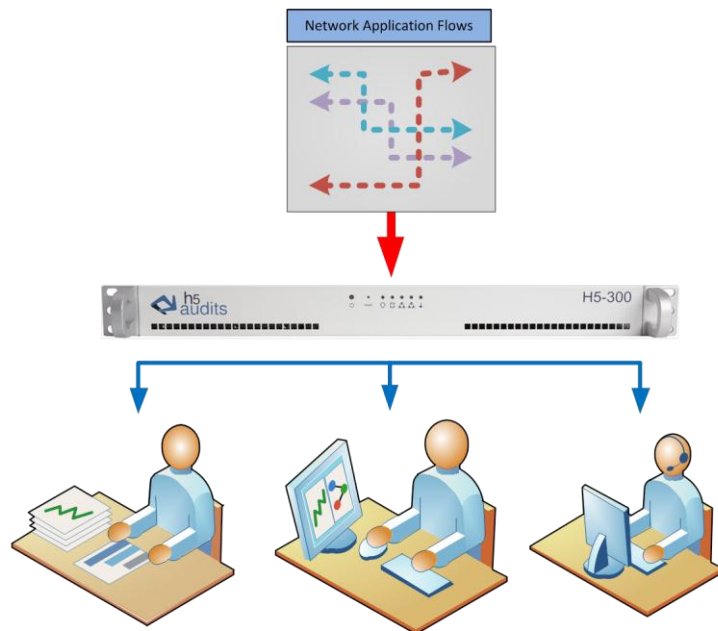
Le transport de la voix sur IP repose sur le protocole sans connexion RTP (Real Time Protocol) qui présente un comportement sensiblement différent de TCP. L'appliance H5 produit donc un ensemble spécifique de métriques VoIP et RTP pour chaque appel transitant sur le réseau. Ces métriques incluent notamment le MOS qui permet aux équipes réseau d'évaluer la qualité de service perçue par les utilisateurs VoIP sans avoir à déployer solution de monitoring VoIP spécifique.



Agrégation temporelle des données avec persistance par conversation

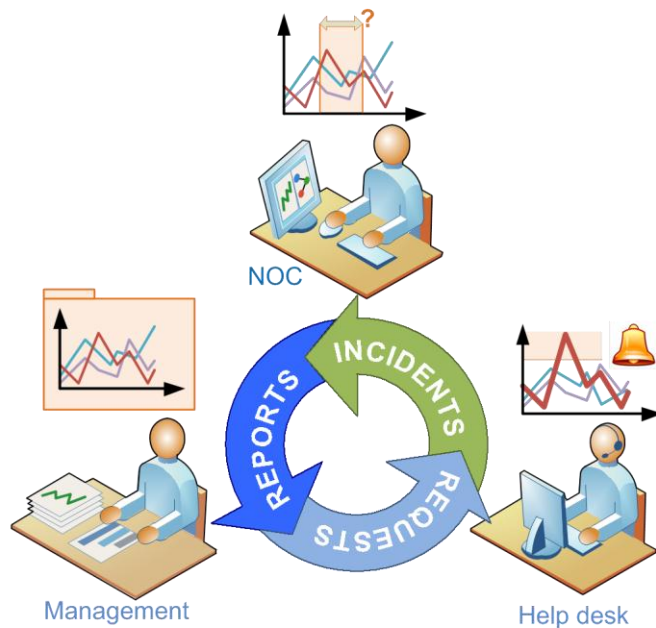
H5: une appliance multiservice.

L'appliance H5 fournit un service d'accès aux données à toutes les équipes IT sans recourir à un logiciel ou à une machine tierce. Si l'interface temps réel Java H5-Dock permet aux équipes réseau d'analyser et de forer dynamiquement les données, le portail de reporting Web permet aux managers de générer des rapports rapides et disponibles à tout instant et les alertes SNMP ou e-mail permettent au help desk d'être immédiatement averti d'un incident d'une situation anormale.



L'appliance H5: un outil de collaboration pour les équipes IT.

L'ensemble des services fournis par l'appliance H5 sont étroitement intégrés et permettent aux équipes IT de collaborer efficacement. Par exemple, un ingénieur réseau peut en un click, au milieu d'une session de recherche de panne sur H5-Dock, générer un rapport à destination du manager ou créer une alerte liée au même contexte ; nul besoin de quitter son interface et son contexte de travail.



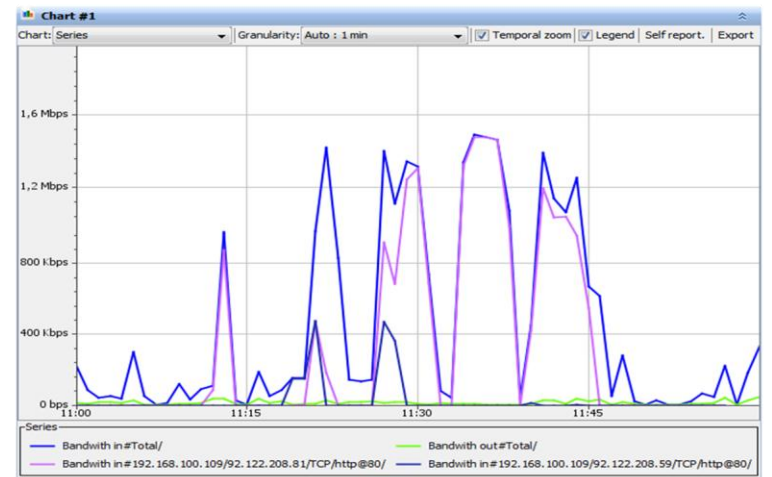
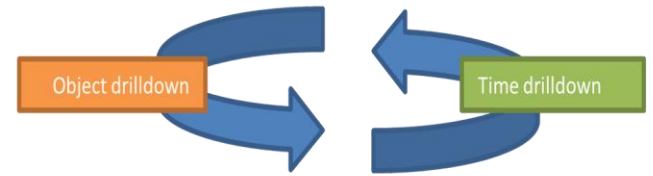
L'appliance H5: les objets d'agrégation de conversation réseau.

La fonctionnalité clé pour les stratégies de forage et d'investigation des appliances H5 est l'objet d'agrégation. Pour arriver à afficher une vue pertinente d'une problématique donnée l'appliance H5 permet à l'ingénieur réseau de partir de l'objet de plus haute agrégation fournissant une information globale de la situation du réseau et de forer rapidement la base de données, souvent jusqu'à la conversation IP individuelle, pour atteindre le niveau de granularité optimal à la qualification des incidents et des comportements.

Objets d'agrégation supportés par l'appliance H5	
Trafic total	Trafic global capturé par l'appliance.
Top adresses IP	Top adresses IP émettrices par volume (Octet).
Top Conversations IP	Top conversations IP unidirectionnelles par volume.
VLANs	VLANs 802.1Q détectés sur le trafic capturé.
Protocoles IP	Applications détectées par port TCP, UDP depuis le trafic capturé.
Protocoles RTP	Services RTP détectés par l'appliance H5 sur le trafic capturé, les objets d'agrégation RTP permettent l'affichage des métriques RTP et VoIP (gigue, délai inter paquets, MOS ...).
Objets Surveillés	Les objets surveillés configurés par l'utilisateur (sites distants, groupes de serveurs, etc.)
Flux métier	les flux métier configurés par l'utilisateur (applications métier, etc.)

H5-Dock: une puissante interface Java dédiée à l'analyse des flux réseau.

Type	Description	Bandwidth in	Bandwidth out	Volume in	Volume out	Connectio...	Server res...
Total	Total	453,52 Kbps	13,6 Kbps	202,62 Mo	6,08 Mo	2 050	517,91 ms
TCP	TCP	451,12 Kbps	11,02 Kbps	201,55 Mo	4,92 Mo	2 050	517,91 ms
http@80	http@80	440,33 Kbps	8,19 Kbps	196,73 Mo	3,66 Mo	1 666	209,74 ms
192.168.100.109	laurent-dev.hsaudits.local	392,55 Kbps	2,7 Kbps	175,38 Mo	1,21 Mo	634	168,03 ms
92.122.208.81	a92-122-208-81.deploy.ak...	306,17 Kbps	540,74 bps	136,79 Mo	241,59 KB	16	99,58 ms
92.122.208.59	a92-122-208-59.deploy.ak...	26,54 Kbps	92,73 bps	11,86 Mo	41,43 KB	16	96,24 ms
77.238.187.168	usdv01.atlas.cdn.us.yimg...	19,69 Kbps	1,42 bps	8,8 Mo	650 o	2	225,42 ms
95.131.137.147	95.131.137.147	10,08 Kbps	196,3 bps	4,51 Mo	87,7 KB	27	223,27 ms
208.122.31.16	208.122.31.16	10,07 Kbps	3,37 bps	4,5 Mo	1,51 KB	2	158,31 ms
206.132.73.17	206.132.73.17	4,13 Kbps	27,78 bps	1,85 Mo	12,41 KB	3	134,42 ms
208.65.155.99	208.65.155.99	3,8 Kbps	9,27 bps	1,7 Mo	4,14 KB	1	107,38 ms
68.232.35.229	68.232.35.229	2,18 Kbps	80,9 bps	996,41 KB	36,14 KB	7	227,12 ms
213.186.33.4	cluster003.ovh.net	1,87 Kbps	35,91 bps	853,95 KB	16,04 KB	15	296,78 ms
88.190.253.247	pf7-web.online.net	1,18 Kbps	64,67 bps	540,57 KB	28,89 KB	12	108,07 ms
68.232.34.223	68.232.34.223	868,64 bps	26,24 bps	388,09 KB	11,72 KB	11	407,66 ms
95.131.136.161	95.131.136.161	835,77 bps	68,02 bps	373,41 KB	30,39 KB	14	168,38 ms
178.249.137.64	soundcloud.com	441,36 bps	90,2 bps	197,19 KB	40,3 KB	25	441,61 ms
98.139.197.254	storage6.fldr.vip.bf1.yah...	394,69 bps	13,02 bps	176,34 KB	5,82 KB	8	225,14 ms
76.13.18.77	storage4-dsr.fldr.vip.ac4...	390,14 bps	8,7 bps	174,31 KB	3,89 KB	5	214,84 ms
80.65.238.16	80.65.238.16	356,93 bps	40,17 bps	159,47 KB	17,95 KB	21	199,5 ms



Le client Java H5-Dock est la principale interface homme-machine graphique fourni par l'appliance H5 à destination des ingénieurs réseau. Le client est directement chargé depuis l'appliance H5 via Web Start et s'exécute sur toute station de travail supportant une machine virtuelle Java. H5-Dock charge en temps réel les données de la base de données de flux réseau de l'appliance et affiche dynamiquement sous forme de tableaux et de graphiques les valeurs des métriques pour les objets réseau détectés au configurés.

Une instance H5-Dock permet de configurer de multiples vues permettant d'explorer l'ensemble des flux réseau depuis plusieurs appliances sur plusieurs zones géographiques et intervalles de temps. L'interface homme-machine H5-Dock comprend de puissants outils d'analyse de données et en particulier des outils de zoom temporel et de forage de données permettant de détecter et d'isoler les conditions de trafic anormal sur un intervalle de temps important et parmi des milliers de conversations réseau.

De plus les ingénieurs réseau peuvent facilement élaborer des scénarios de recherche de pannes, les sauvegarder et les partager avec les équipes IT. Les situations anormales et les incidents réseaux et système récurrents peuvent ainsi être suivis et référencés dans une base de connaissance et de support qui s'améliore au fil du temps.

Métriques TCP/UDP supportées (extrait)

Débit (Kbps)	La somme des débits en kilo bit par seconde.
Volume (Octets)	La somme des volumes en Octets.
Requêtes de connexion (#)	Nombre de requêtes de connexion TCP (trames SYN) qui ont circulé dans le trafic pendant l'intervalle de mesure.
Tps de connexion (ms)	Temps moyen en milliseconde d'établissement des connexions TCP (durée du « 3 way handshake » : SYN – SYN ACK – ACK) pour les SYN.
Taux d'échec de connexion (%)	Taux des connexions TCP initiées et non abouties, relativement à la totalité des connexions initiées.
Paquets dupliqués (#)	Nombre de trames dupliquées (trames identiques, avec le même n° de séquence) observé pendant l'intervalle de mesure.
Connexions établies (#)	Nombre de nouvelles connexions TCP établies (SYN – SYN ACK – ACK) pendant l'intervalle de mesure.
Paquets perdus (#)	Nombre de paquets manquants sur le flux circulant pendant l'intervalle de mesure.
Taux de perte (%)	Ratio en % du nombre de paquets manquants sur le nombre total ayant circulé pendant l'intervalle de mesure.
Paquets (#)	Nombre total de paquets réseau qui ont circulé pendant l'intervalle de mesure.
Charge utile TCP (Octets)	La volumétrie totale des données transportées par les segments TCP (la somme de la charge utile des paquets TCP).
Resets TCP (#)	Nombre de segment RST (Reset) du protocole TCP qui ont été vus pendant l'intervalle de mesure.
Tps de retrans. (ms)	Temps moyen écoulé dans le sens in entre le passage d'un segment (réel ou virtuel) et l'arrivée de sa retransmission.
RTT (ms)	Mesure du temps moyen d'acquittement par le récepteur local des segments TCP circulant dans le sens in, en millisecondes (les acquittements circulent dans le sens out).
Tps de réponse serveur in (ms)	Mesure du temps de réponse moyen du serveur aux pseudo-requêtes circulant dans le sens in, en millisecondes.
Débit de paquets vifs lfe (pps)	Nombre moyen de paquets par seconde (pps) ayant circulé pendant l'intervalle de mesure.




Métriques VoIP/RTP supportées (extrait)

RTP Délai inter-paquets (ms)	Temps moyen entre deux paquets RTP consécutifs dans une conversation établie pour le flux.
RTP Gigue (ms)	Variation moyenne du délai inter-paquets dans une conversation établie pour le flux.
RTP Paquets dupliqués (#)	Nombre de paquets RTP dupliqués détectés sur le flux circulant pendant l'intervalle de mesure.
RTP Paquets hors séquence (#)	Nombre de paquets RTP hors séquence détectés sur le flux circulant pendant l'intervalle de mesure.
RTP Paquets perdus (#)	Nombre de paquets RTP manquants sur le flux circulant pendant l'intervalle de mesure.
RTP Taille des bursts (#)	Taille moyenne des rafales de paquets perdus sur le flux circulant pendant l'intervalle de mesure en nombre de paquets.
MOS calculé	« Mean Opinion Score », variant de 1 à 5 représentant la qualité sonore de l'appel, calculée à partir des caractéristiques techniques du flux selon un algorithme basé sur le E-model.

La gamme des appliances H5:

La gamme des appliances H5 donne aux administrateurs réseau la possibilité de maintenir 100% de visibilité réseau alors que le trafic à surveiller est en constante croissance. Le logiciel H5 fonctionne de manière identique sur toutes les appliances H5. Le modèle de la plateforme matérielle ne dépend que du volume du trafic à observer de quelques mégabits par seconde à 10Gbps.

De plus, le support des VLAN permet aux équipes réseau de construire une solution de monitoring multi client ou multi lien efficace basé sur des tapes intelligentes et le marquage de paquets. Par exemple une seule appliance H5-700 être installée sur de multiples réseaux 1Gbps agrégés sur un seul lien 10Gbps avec une totale séparation du trafic.

H5 200		10Mbps - 200Mbps	PME/PMI Filiale
H5 300		100Mbps – 1Gbps	Entreprise
H5 700		500Mbps – 10Gbps	Data Center Fournisseur de services

La gamme H5 appliance

H5 audits

Energy 4, 155-159 rue du Docteur Bauer
93400 Saint-Ouen
Tel : +33 1 49 48 12 00
Fax : +33 1 49 48 12 04
info@h5audits.com