WAAS : WIDE AREA APPLICATIONS SYSTEMS OPTIMISATION DES APPLICATIONS

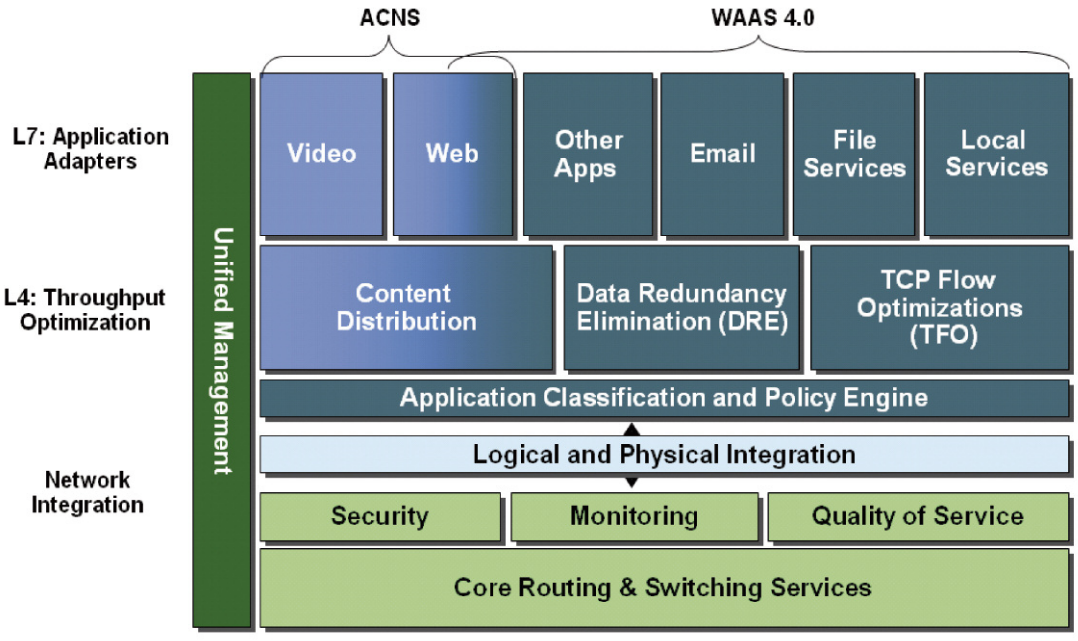
PRESENTATION DE L'OFFRE CISCO WAAS

Introduction

Cisco travaille sur l'accélération applicative et l'optimisation des réseaux longue distance depuis plus de 8 ans. D'abord orienté vers les technologies de caching Internet et vidéo, puis de distribution de contenu à grande échelle avec l'offre ACNS (Application and Content Networking System), la stratégie de Cisco Systems a pris une nouvelle dimension avec l'acquisition de la société Actona Technologies en Août 2004. Les technologies conçues par cette société ont très vite donné naissance à toute une nouvelle gamme de produits connue sous le nom de WAFS (Wide Area File Services). Celle-ci avait pour but essentiel d'optimiser les performances d'accès aux serveurs de fichiers à travers CIFS, protocole « bavard » et donc très sensible à la latence, inéluctable sur les réseaux WAN.

Les fonctionnalités WAFS n'ont cessé de s'enrichir pour aboutir à l'évidence de la complémentarité du caching Internet/vidéo, de l'accélération des accès aux NAS, ainsi que de l'optimisation applicative pour tous les flux basés sur TCP. C'est de cette constatation que la stratégie WAAS (Wide Area Application System) a vu le jour. Bien qu'aujourd'hui les deux trains logiciels WAAS et ACNS soient indépendants (voir REF _Ref130202060 \h Figure 1 : Services WAAS et ACNS), la synergie des deux technologies est en route.

Figure 1 : Services WAAS et ACNS



La technologie WAAS s'appuie sur un ensemble de devices appelé 'wide area application engines' (WAEs) qui travaillent ensemble afin d'optimiser le trafic TCP qui circule sur le réseau. Lorsqu'un client et un serveur applicatif essayent de communiquer ensemble, **le réseau intercepte et redirige ce trafic sur les WAE,** qui peuvent alors agir en se faisant passer pour le client et le serveur destinataire. Les WAEs examinent le trafic et utilisent les politiques applicatives configurées pour déterminer si le trafic doit être optimisé ou doit juste traverser le réseau sans optimisation.

- **Il n'y a pas d'encapsulation des flux entre les WAE (pas de mode tunnel), la gestion est transparente et ne remet donc pas en cause les politiques de sécurité ou de QOS déjà établies sur le réseau.**

La technologie **WAAS (Wide Area Application Services)** a pour objectif d'améliorer à la fois les performances applicatives, mais aussi les accès aux serveurs de fichier, au travers du WAN, permettant ainsi une consolidation sur un site central des serveurs auparavant éparpillés dans les filiales des entreprises.

Grâce à des mécanismes évolués d'**optimisation des flux de données sur les réseaux étendus,** elle évite, par exemple, d'avoir à positionner des serveurs de fichiers ou d'impression sur chaque site distant. Ainsi, l'administration de l'infrastructure de service de fichiers est grandement facilitée : **les coûts de stockage des données sont réduits** tout en tirant partie de **la haute disponibilité** des serveurs de fichiers centralisés de type NAS, et **l'accès aux données pour les utilisateurs distants offre des performances pouvant être jusqu'à similaires à celles d'un réseau local.**

Le principe d'une architecture WAAS consiste à **centraliser les données des filiales ou sites distants sur un site central** et à en permettre l'accès de façon transparente, performante et fiable au travers du WAN. Les sites de périphérie sont mis en relation avec les serveurs de fichiers ou serveurs applicatifs par l'intermédiaire d'appliances **WAE (Wide Area Engine)** disposées dans chaque agence (fonction WAAS «edge») ainsi que sur le site central (fonction WAAS «core»).

Dans le cas des accès aux serveurs de fichiers, les boîtiers WAE s'appuient sur une technologie de cache et de compression qui permet de ne faire transiter que les données réellement modifiées. Ils proposent également des mécanismes d'optimisation des flux applicatifs beaucoup plus génériques tels que :

- DRE (Data redundancy Elimination) qui consiste à ne pas réémettre des données redondantes,
- Compression LZ (Lempel Zip), qui permet de compresser toutes les données qui doivent transiter sur le WAN,
- TFO (TCP Flow Optimization), qui permet une meilleure utilisation de la bande passante en optimisant les mécanismes de TCP.

Enfin, les appliances WAE offrent des services locaux au site tels que le serveur d'impression intégré, le pré-positionnement de fichiers (idéal pour les télédistributions) ou encore le filtrage de l'accès aux NAS centraux.

Les grandes caractéristiques de la technologie WAAS sont les suivantes :

- **Utiliser le WAN le moins possible —** En effet, il est préférable de gérer le maximum d'opérations à distance. La solution WAAS diminue le nombre de transactions effectuées via le WAN (par les mécanismes de proxy CIFS avec la technologie Wafs), et protège aussi efficacement les utilisateurs des désagréments causés par celui-ci (essentiellement du à la latence).
- **Utiliser le WAN de manière optimale —** WAAS fait appel à la fois à des techniques élaborées en ce qui concerne le cache et la compression, ainsi qu'à des technologies réseau optimisées, tout ce qui permet d'utiliser le WAN de manière optimale. Certaines fonctions telles que le pré-positionnement nocturne de fichiers permettent d'utiliser la bande passante aux heures de moindre charge.
- **Préserver la sémantique protocolaire du file system —** Pour l'optimisation de l'accès aux serveurs de fichier par CIFS, la solution WAAS utilise son propre protocole propriétaire au sein du WAN, tout en conservant l'intégrité totale de la sémantique des commandes protocolaires standard du système de fichiers.
- **Rendre la solution transparente aux utilisateurs —** Les meilleures solutions sont celles qui se font oublier, sans interférer avec les utilisateurs finaux, ou en les forçant à changer leurs habitudes de travail. La solution WAAS ne nécessite pas l'installation d'un logiciel, ni sur le serveur, ni sur le client, et de ce fait, ne demande pas à l'utilisateur de se former sur un nouveau produit. En résumé, les utilisateurs bénéficient d'un data center sécurisé sans changer le moins du monde leurs habitudes de travail.

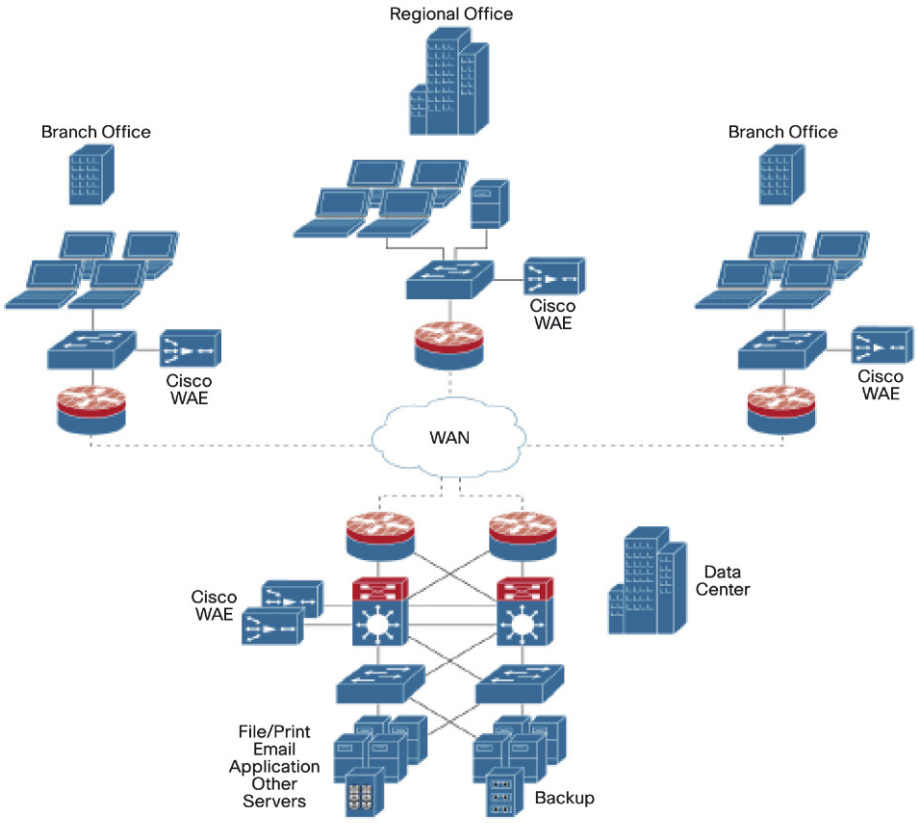
Principe de fonctionnement

L'entreprise doit faire face à un problème technique récurrent : la **latence !**

La plupart des applicatifs et des protocoles de partage de ressources comme CIFS, n'ont pas été conçus pour fonctionner sur un réseau distant (WAN). Compte tenu de leur caractère extrêmement transactionnel, les performances se dégradent fortement dès que la latence dépasse 15 à 20 ms, et l'augmentation de la bande passante ne change pas le problème.

L'utilisation conjointe de technologies de compression, de cache, d'optimisation du protocole de transport, permet d'obtenir une vitesse de transfert des données plus proche de celle atteinte sur un réseau local (LAN) et apporte une fiabilité, une sécurité, et un partage des fichiers entre les utilisateurs distants sans remettre en cause l'architecture en place.

Figure 2 : Architecture WAAS type



Pour la partie optimisation des accès aux fichiers, le principe est le suivant : lorsqu'un utilisateur accède à un fichier, le système WAAS vérifie si une copie intégrale de ce fichier ou certains segments de données le composant sont déjà présents localement dans le boitier WAAS installé à l'agence. Si ce n'est pas le cas, une copie à jour de l'ensemble du fichier ou simplement des segments requis est rapatriée depuis le site central pour être mise à disposition de l'utilisateur.

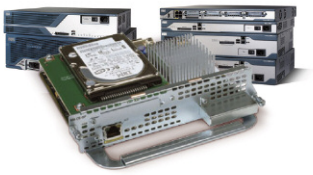
L'accès multi utilisateurs est totalement géré. Lorsqu'un utilisateur ouvre un fichier pour le modifier, ses droits d'accès sont vérifiés de manière transparente auprès du serveur de fichier central. Ensuite le serveur central est prévenu de cette action et ce fichier n'est alors pas modifiable par un autre utilisateur avant que le premier utilisateur ne l'ait libéré (gestion des accès concurrents).

Appliances Cisco WAE

Cisco WAE (Wide Area Engine) représente une gamme complète d'appliances évolutives et performantes dédiées à l'optimisation des applications, du stockage et de la distribution de contenu au travers de réseaux étendus (WAN). Cette gamme d'appliance est complétée par un Network Module (NM) pour les routeurs de la gamme ISR (28xx et 38xx). Aujourd'hui, ces appliances et NM supportent les logiciels suivants :

- WAAS pour l'optimisation applicative des flux TCP, l'accès aux systèmes de fichiers et la télédistribution.
- ACNS pour le caching (web, FTP,…), le pré-positionnement de masse, ainsi que la diffusion vidéo, qu'elle soit temps-réel ou à la demande.

Figure 3 : Gamme des appliances Cisco WAE et NM pour ISR



NM-WAE Router-Integrated Network Module for the Cisco Integrated Services Router

NM-WAE Module

NME-WAE-302:
- Jusqu'à des connexions WAN de 4Mbps
- 200 optimized TCP connections
- 512MB of RAM, 80GB of disk
- license Transport uniquement (pas de CIFS)

NME-WAE-502:
- Jusqu'à des connexions WAN de 4Mbps
- 500 optimized TCP connections
- 1GB of RAM, 120GB of disk

WAE-512 Remote Office Appliance

WAE-512 Appliance

- Remote office appliance platform
- Jusqu'à des connexions WAN de 20Mbps
- 1500 optimized TCP connections
- 250GB RAID-1 disk capacity
- Utilisation en coupure, WCCPv2, PBR ou CSM/ACE

WAE-612 Regional Hub and Data Center Appliance

WAE-612 Appliance

- Regional hub and medium data center deployments
- Jusqu'à des connexions WAN de 155Mbps
- 6000 optimized TCP connections
- 300GB RAID-1 SAS disk capacity
- Utilisation en coupure, WCCPv2, PBR ou CSM/ACE

WAE-7326 Enterprise Data Center Appliance

WAE-7326 Appliance

- Enterprise data center deployments
- Jusqu'à des connexions WAN de 310Mbps
- 7500 optimized TCP connections
- 900GB RAID-1 SCSI disk capacity
- Utilisation en coupure, WCCPv2, PBR ou CSM/ACE

Les appliances WAE ont été conçues pour une intégration optimale dans le réseau de l'entreprise. Elles sont chacune équipées de 2 ports 10/100/1000 et peuvent être directement sollicitées par le réseau (redirection transparente) ou les applicatifs clients (simulation d'un file serveur local). Les WAE acceptent aussi une carte additionnelle avec 4 ports RJ45 (avec gestion d'un bypass physique) pour un fonctionnement en coupure. (voir chapitre 3 pour les détails sur les méthodes d'insertion des WAE dans le réseau).

Une version spécifique sous forme de Network Module s'insère dans les routeurs Cisco ISR (Integrated Services Routers) de type 2800 et 3800 pour offrir les fonctions WAAS de manière complètement intégrée. Cette architecture réservée aux petites configurations tire parti de la souplesse de ces gammes de routeurs sans introduire là-encore un point de panne additionnel. En effet, le network module dispose de mécanismes lui permettant de rester indépendant de la machine qui l'héberge. Un dysfonctionnement du module WAAS ne perturbe pas son routeur hôte.

Tableau 1 : Fiches techniques des appliances Cisco WAE

	NME-WAE-302	NME-WAE-502	Cisco WAE-512	Cisco WAE-612	Cisco WAE-7326
CPU	-	-	One 3.0 GHz P4 processor with 1MB Layer 2 cache	One 3.0 GHz dual-core Pentium D processor	Two 3.2 GHz Intel Pentium 4 Xeon processors with 1 MB Layer 2 cache
System Bus	-	-	800 MHz	800 MHz	800 MHz
Baseline SDRAM	512 MB	1 GB	· 1 GB · PC2700 ECC DDR1	· 2 GB · PC2700 ECC DDR2	· 4 GB · PC2700 ECC DDR2
Maximum SDRAM	512 MB	1 GB	· 2 GB (two 1 GB RDIMMs) · PC2700 ECC DDR2	· 4 GB (four 1 GB RDIMMs) · PC2700 ECC DDR2	· 4 GB (four 1 GB RDIMMs) · PC2700 ECC DDR2
Maximum Storage	80 GB	120 GB	Two 250-GB SATA hard drives	Two 300-GB SAS hard drive	Six 300-GB SCSI hard drives
Network Interfaces	One internal 10-/100/1000-Mbps Ethernet to router backplane	One internal 10-/100/1000-Mbps Ethernet to router backplane	Two 10/100/1000BASE-T	Two 10/100/1000BASE-T	Two 10/100/1000BASE-T
	One External 10-/100/1000-Mbps Ethernet Interface	One External 10-/100/1000-Mbps Ethernet Interface	Optional 4 ports card for on-line utilization	Optional 4 ports card for on-line utilization	Optional 4 ports card for on-line utilization
Flash Memory	64 MB	64 MB	128 MB	128 MB	128 MB
Fibre Channel Adapter (optional)	No	No	· Yes (support only with Cisco ACNS Software) · Bus type: fiber-optic media (short-wave 50 micron) · Bus transfer rate: 200 Mbps max at half duplex and 400 Mbps at full duplex	· Yes (support only with Cisco ACNS Software) · Bus type: fiber-optic media (short-wave 50 micron) · Bus transfer rate: 200 Mbps max at half duplex and 400 Mbps at full duplex	· Yes (support only with Cisco ACNS Software) · Bus type: fiber-optic media (short-wave 50 micron) · Bus transfer rate: 200 Mbps max at half duplex and 400 Mbps at full duplex

	NME-WAE-302	NME-WAE-502	Cisco WAE-512	Cisco WAE-612	Cisco WAE-7326
Power	-	-	One 350W AC	One 350W AC	Two 625W hot-swappable redundant AC
Rack Units	Network Module	Network Module	1 rack unit (RU)	1 RU	2 RU
External Connectors	-	-	1 serial port	· 1 serial port · One U320 SCSI port (dual-channel integrated controller)	· 1 serial port · One U320 SCSI port (dual-channel integrated controller)
Height	1.55 in. (39 mm)	1.55 in. (39 mm)	1.72 in. (43.7 mm)	1.72 in. (43.7 mm)	3.36 in. (85.4 mm)
Width	7.10 in. (180 mm)	7.10 in. (180 mm)	17.3 in. (440 mm)	17.3 in. (440 mm)	17.46 in. (443.5 mm)
Depth	7.20 in. (183 mm)	7.20 in. (183 mm)	20 in. (508 mm)	20 in. (508 mm)	27.48 in. (698.0 mm)
Maximum Weight	1.5 lb (0.7 kg)	1.5 lb (0.7 kg)	28 lb (12.7 kg)	28 lb (12.7 kg)	62 lb (28.1 kg)
Universal Input	-	-	Input voltage low range 100-127 VAC Input voltage high range 200-240 VAC	Input voltage low range 100-127 VAC Input voltage high range 200-240 VAC	Input voltage low range 100-127 VAC Input voltage high range 180-265 VAC
Maximum Power	-	-	300W (115 to 230 VAC)	300W (115 to 230 VAC)	625W (115 to 230 VAC)
OPERATING ENVIRONMENT					
Operational Temperature	41 to 104°F (5 to 40°C)	41 to 104°F (5 to 40°C)	50 to 95ºF (10 to 35ºC)	50 to 95ºF (10 to 35ºC)	50 to 95ºF (10 to 35ºC)
Nonoperational Temperature	-40 to 158°F (-40 to 70°C)	-40 to 158°F (-40 to 70°C)	-40 to 140ºF (-40 to 60ºC)	-40 to 140ºF (-40 to 60ºC)	-40 to 140ºF (-40 to 60ºC)
Humidity	5 to 85% noncondensing	5 to 85% noncondensing	Nonoperating: 8 to 80%	Nonoperating: 8 to 80%	Nonoperating: 8 to 80%
Altitude	-197 ft to 6,000 ft (-60 to 1,800 m)	-197 ft to 6,000 ft (-60 to 1,800 m)	Maximum altitude: 2133m (7000 ft)	Maximum altitude: 2133m (7000 ft)	Maximum altitude: 2133m (7000 ft)
Compliance		CE marking	CE marking	CE marking	CE marking
Safety	UL 60950-1, CSA 60950-1, IEC 60950-1, EN 60950-1	UL 60950-1, CSA 60950-1, IEC 60950-1, EN 60950-1	· UL 1950 · CSA-C22.2 No. 950 · EN 60950 · IEC 60950	· UL 1950 · CSA-C22.2 No. 950 · EN 60950 · IEC 60950	· UL 1950 · CSA-C22.2 No. 950 · EN 60950 · IEC 60950
EMC	FCC Part 15 Class A; EN55022 Class B; AS/NZS 3548 Class A; CISPR22 Class B; VCCI Class B; EN55024; EN61000-3-2; and EN61000-3-3	FCC Part 15 Class A; EN55022 Class B; AS/NZS 3548 Class A; CISPR22 Class B; VCCI Class B; EN55024; EN61000-3-2; and EN61000-3-3	· FCC Part 15 (CFR 47) Class A · ICES-003 Class A · EN 55022 Class A with UTP cables · CISPR22 Class A with UTP cables · ASNZ 3548 Class A with UTP cables · VCCI Class A with UTP cables · EN 55024 · EN 50082-1	· FCC Part 15 (CFR 47) Class A · ICES-003 Class A · EN 55022 Class A with UTP cables · CISPR22 Class A with UTP cables · ASNZ 3548 Class A with UTP cables · VCCI Class A with UTP cables · EN 55024 · EN 50082-1	· FCC Part 15 (CFR 47) Class A · ICES-003 Class A · EN 55022 Class A with UTP cables · CISPR22 Class A with UTP cables · ASNZ 3548 Class A with UTP cables · VCCI Class A with UTP cables · EN 55024 · EN 50082-1

Tableau récapitulatif de dimensionnement

Le tableau ci-dessous permet d'avoir une vue de synthèse des capacités des différents WAE, et de donner ainsi des éléments de dimensionnement :

Device*	Max Optimized TCP Conn	Max CIFS Sessions	Single Drive Capacity [GB]	Max Drives	RAM [GB]	Max recommanded WAN Link [Mbps]	Max Optimized Throughput [Mbps]	Max Edge peers **	Central Manager Scalability [Devices]
NME-WAE -302	200	NA	80	1	0.512	4	TBD	NA	NA
NME-WAE -502	500	500	120	1	1	4	TBD	2	NA
WAE-512-1	750	750	250	2	1	8	100	5	500
WAE-512-2	1500	1500	250	2	2	20	150	10	1000
WAE-612-2	2000	2000	300	2	2	45	250	20	2000
WAE-612-4	6000	2500	300	2	4	90	350	30	2500
WAE-7326	7500	2500	300	6	4	155	450	50	

* le chiffre de fin après le tiret indique le nombre de giga de RAM du WAE

** indique le nombre de Edge supporté si la fonction Core est utilisée sur ce type de WAE

FONCTIONNALITES ET PROTOCOLES SUPPORTES PAR CISCO WAAS

Le logiciel Cisco WAAS est basé sur un certain nombre de composants, chacun étant conçu dans l'objectif d'offrir un accès hautement performant aux données distantes, sans pour autant compromettre l'intégrité des données.

Toutes les fonctionnalités décrites ci-dessous sont activables ou non sous forme de politiques d'accélération. Ces politiques doivent être appliquées de manière homogène sur les appliances core et edge. Si la cohérence de configuration entre les sites de périphérie et le data center n'est pas respectée, certains types d'accélération ne seront pas effectifs (comme la compression DRE et l'optimisation TFO). Par contre, cela n'induit pas d'interruption de service pour l'utilisateur : les applications continuent de transiter même si elles ne sont pas optimisées.

Optimisation TCP

L'implémentation standard des stacks TCP au niveau des clients et des serveurs peut entraîner une perte de performance au niveau des applications. Plusieurs raisons peuvent exister :

- Impossibilité de remplir la ligne (mauvaise utilisation de la bande passante disponible)
- Mauvaise récupération lors de la perte de paquets, retransmissions,
- Consommation de toute la bande passante par de très nombreuses connexions courtes

La fonction WAAS **TFO** (**Transport Flow Optimization**) implémente des mécanismes standards sur le marché pour résoudre ces problèmes de performance liés à certaines implémentations de TCP.

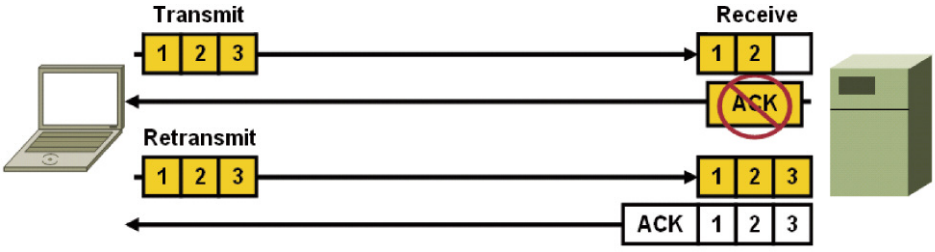
Fenêtrage TCP

La première fonction permettant d'améliorer les performances de TCP consiste à ajuster la valeur du fenêtrage de TCP. Après un certain nombre de paquets, TCP va attendre un acquittement de la part du destinataire. Sur une liaison WAN, apportant une latence importante, le temps perdu lors de ces phases d'acquittement entraîne un impact important sur les performances. Le fenêtrage classique de TCP (identifié sur un champ de 16 bits) limite celui-ci à 64 Ko. L'utilisation du RFC1323 permet d'augmenter la limite jusqu'à une valeur de 1 Go (correspondant à un champ de 30 bits).

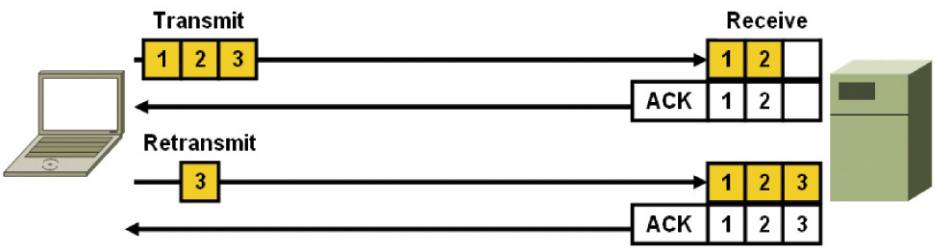
Ainsi le lien est utilisé de façon plus massive pour la transmission des données et les phases d'acquittements (impactés par la latence) sont proportionnellement moins importantes.

Acquittement sélectif (Sack)

Les implémentations TCP standard acquittent l'ensemble de la fenêtre de transmission. Ce qui veut dire que si sur 3 paquets seul le 3ème n'a pas été reçu, l'ensemble des 3 paquets est retransmis. Cela pose d'autant plus de problème que l'on a agrandi la fenêtre pour optimiser la performance de transmission.



L'acquittement sélectif permet de ne demander la réémission que du paquet manquant.

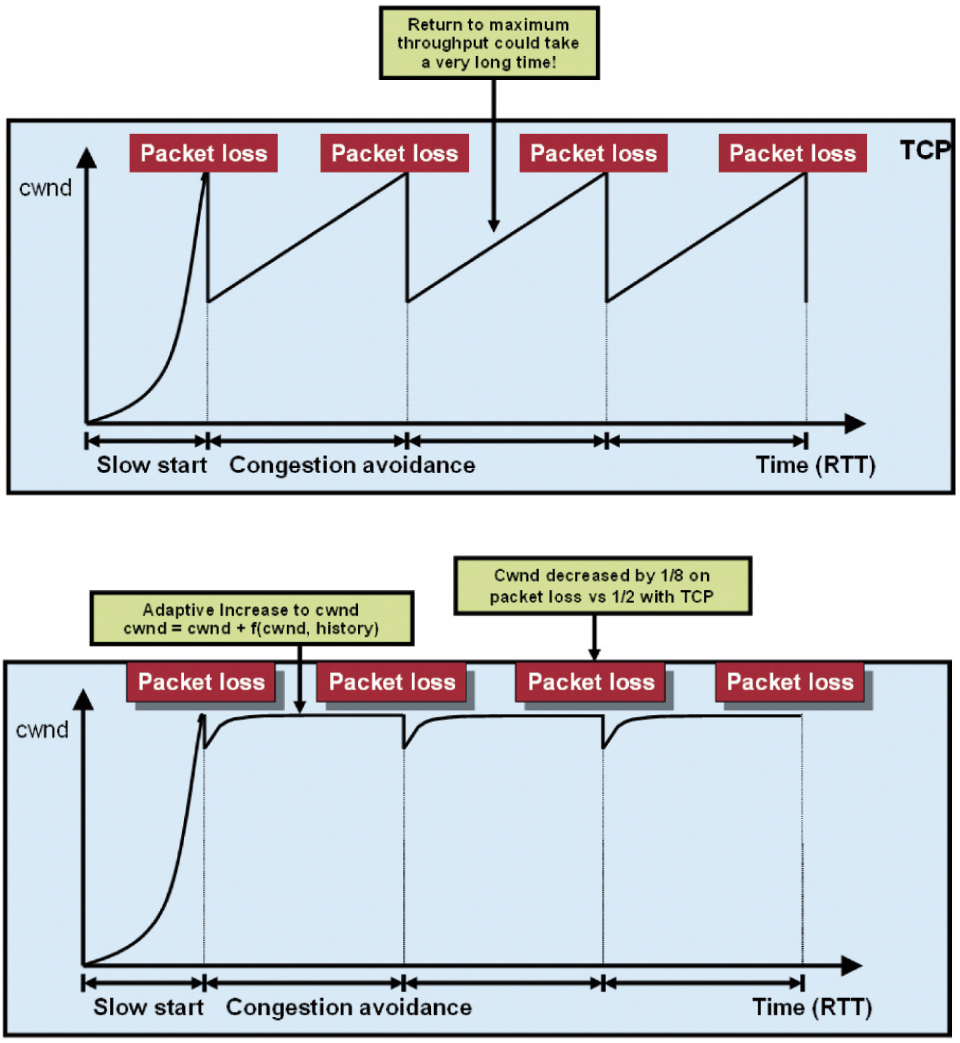


Adaptive Increase Window size

La fonction TFO va aussi réduire le temps de remontée de la fenêtre TCP, une fois le maximum atteint. L'objectif de cette fonction est de limiter l'effet « dent-de-scie » que l'on peut constater avec les flux TCP, lorsque ceux-ci arrivent à la limite de capacité du lien.

Les schémas ci-dessous illustrent ainsi le meilleur usage de la liaison :

Figure 5 : Action de «l'adaptive increase windows size»

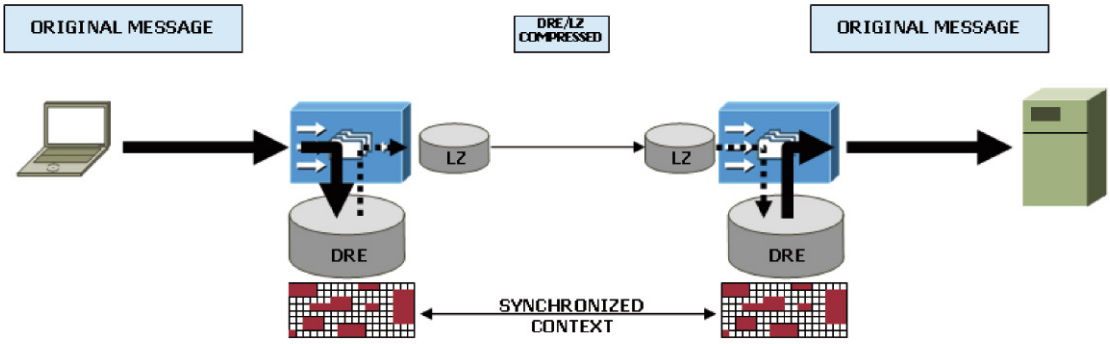


Compression DRE

Cisco WAAS 4.0 utilise deux mécanismes de compression avancés au niveau de la couche de transport (L4 – Throughput) :

- **La compression LZ (Lempel Zip) :** Compression standard réalisée en temps réel sur le flux
- **DRE (Data Redundancy Elimination) :** Mécanisme évolué permettant la suppression des données redondantes lors de la transmission.

Figure 6 : Représentation globale des mécanismes de compression



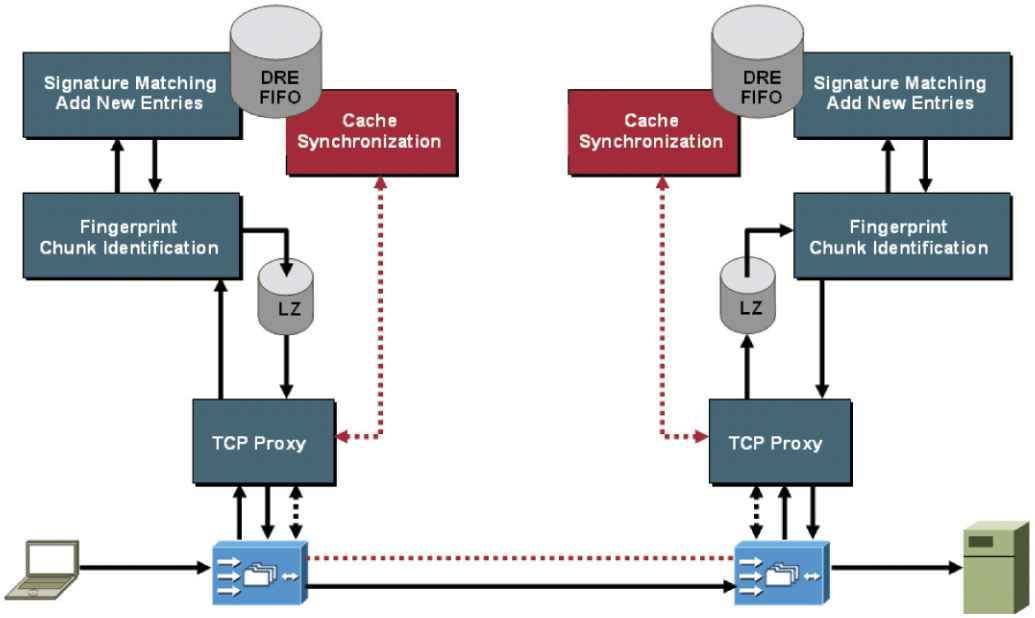
DRE utilise les ressemblances entre les données qui sont transmises sur le lien. Une fonction sophistiquée de reconnaissance par masques sur le contenu, identifie les blocs de données qui sont répétées (appelés «chunks»).

Ces blocs sont stockés et indexés dans un cache particulier de chaque côté de la liaison. Une fois qu'un bloc est stocké dans le cache, les émissions futures de ce même bloc ne demandent plus que la réémission d'un petit identifiant («signature» ou «label») au travers du lien WAN.

La compression LZ est appliquée lors de la première émission du bloc, ou lorsqu'un bloc de données ne correspond à aucun bloc mémorisé dans la zone de stockage.

Afin de maintenir une cohérence entre les cache de blocs des deux côté de la liaison, la fonction DRE utilise un mécanisme de synchronisation entre les caches.

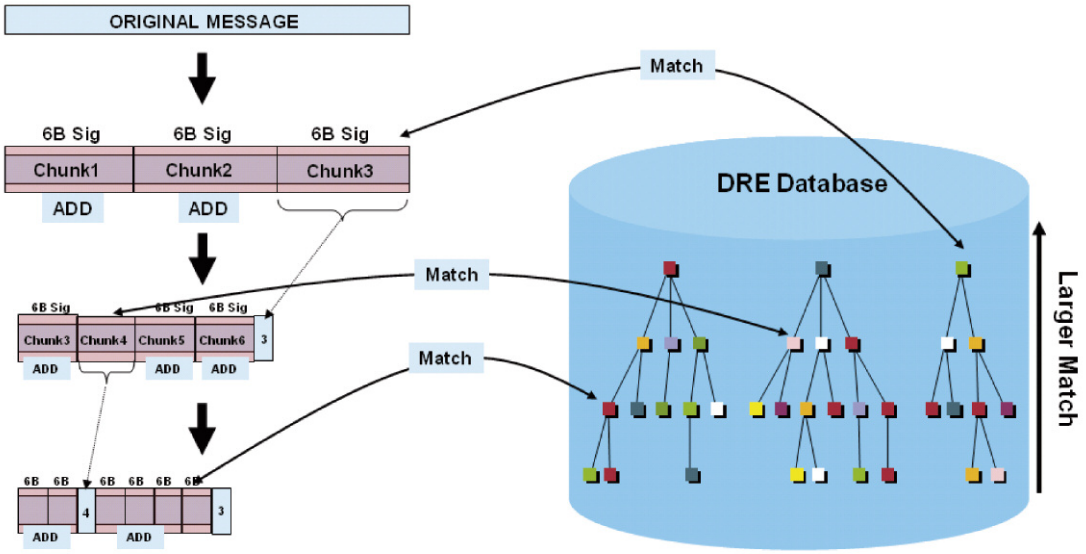
Le fonctionnement détaillé de la fonction DRE est détaillé ci-dessous :



1. La trame TCP est redirigée vers le WAE (par exemple par WCCP).
2. La trame est traitée par la fonction de TCP proxy de WAAS.
3. WAAS identifie les blocs dont une copie a déjà été mémorisée dans le cache.
4. Si le bloc n'a pas été trouvé, le mémorise dans le cache, créé un identifiant (signature) et envoie le bloc avec sa signature pour éduquer le cache se trouvant de l'autre côté.
5. Si le bloc existe, remplace le bloc par la signature correspondante.
6. Compresse les données par LZ.
7. Envoi la trame TCP résultante sur le lien WAN (à noter que les propriétés IP/TCP restent les mêmes, seul le payload a été compressé).
8. A la réception la trame est traitée par la fonction TCP proxy de WAAS.
9. Le payload est décompressé par LZ.
10. Les blocs non transmis sont identifiés par les signatures.
11. Les données sont recomposées.
12. La trame est envoyée au destinataire.

DRE va rechercher les blocs en utilisant un algorithme basé sur le parcours d'une fenêtre glissante le long des données. Il va chercher dans un premier temps à identifier les blocs redondants les plus grands, puis devenir plus granulaire. Il indexe alors les blocs dans son cache du plus grand au plus petit.

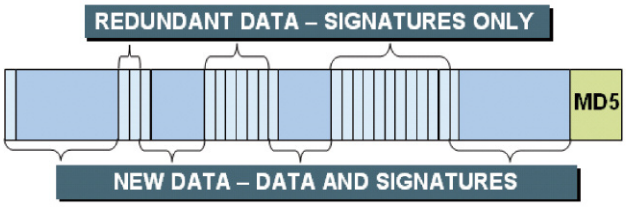
Figure 7 : Base de données DRE



Un payload passé au travers de DRE sera remplacé par un ensemble de signatures pour les blocs qui ont été remplacés, et un ensemble de blocs précédés par leur signature pour les nouveaux blocs indexés dans le cache. Le payload est terminé par une signature (hashing MD5) du paquet original, permettant de vérifier l'intégrité de la trame une fois recomposée à la réception.

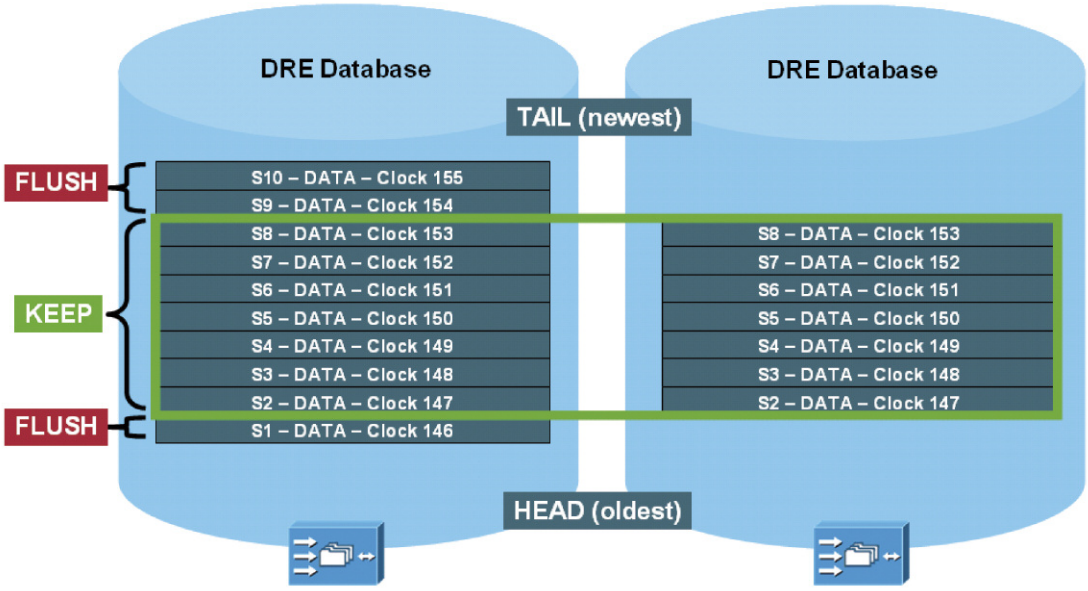
Il est important de noter que DRE est bidirectionnel et donc que les blocs supprimés dans un sens peuvent être utilisé de façon similaire pour le flux retour sans avoir besoin de faire un nouvel apprentissage pour ces mêmes blocs.

Figure 8 : Message compressé par DRE



Afin de conserver une cohérence entre les caches se trouvant des deux côté de la liaison WAN, un mécanisme de synchronisation existe entre les deux caches. Les caches s'échangent une information de contexte différente pour chaque liaison deux-à-deux. L'information de contexte est bidirectionnelle et va permettre de supprimer les blocs qui ne sont pas synchronisés avec le cache correspondant.

Figure 9 : Synchronisation des contextes DRE



Application Traffic Policy Engine (ATP)

Cisco WAAS fournit aux administrateurs la flexibilité dont ils ont besoin pour définir la manière dont des types de trafic doivent être traités par le WAE. Ces définitions incluent l'optimisation (DRE, LZ compression, flow optimizations), le monitoring, et la fonction éventuelle de bypass. Par défaut, plus de 25 types d'applications sont identifiés et plus de 100 classificateurs d'application sont fournis, chacun étant mappés à un type d'optimisation spécifique pour fournir la meilleure amélioration possible pour cette application spécifique. Le tableau ci-dessous montre les différents types d'application existant dans la configuration par défaut :

Tableau 2 : Types d'application par défaut

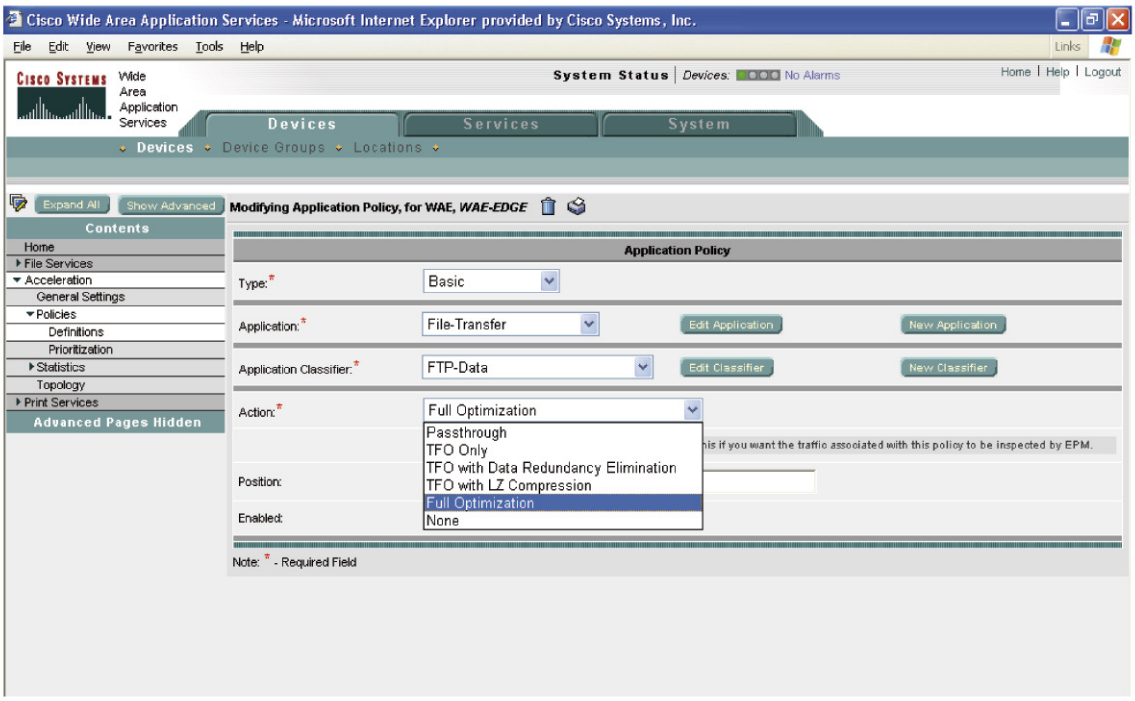
Common Application Types Optimized By Cisco Wide Area Application Services			
Authentication	Backup	Call Management	Conferencing
Console	Content Management	Directory Services	Enterprise Application
Enterprise Messaging	File Services	File Transfer	Instant Messaging
Name Services	Network Analysis	Printing	Remote Desktop
Replication Software	Database	Remote Access	Storage Protocols
Streaming	Systems Management	Version Management	Intranet/Internet

Les politiques de trafic permettent aux administrateurs de définir de façon granulaire les applications, les protocols, et les optimisations à appliquer en utilisant les composants suivants :

- Application name – un nom d'application est utilisé pour grouper de façon logique tous les identifiants qui identifent le traffic pour un type similaire d'application
- Application classifier – un classificateur est utilisé pour spécifier comment doit être identifié le trafic intéressant. Des classificateurs valides de trafic inclus des adresses IP source ou destination ou des subnet, des ports TCP, des intervalles de ports TCP, ou un identifiant spécifique RPC (UUID)
- Optimization map – Une correspondance est utilisée pour grouper un 'traffic classifier' avec une application spécifique et elle définit alors les types d'optimisation qui doivent être effectués si un tel trafic est trouvé.

La figure ci-dessous montre en exemple, l'écran de création ou de modification d'une politique d'application pour les flux de données FTP :

Figure 10 : écran de création d'une politique d'application



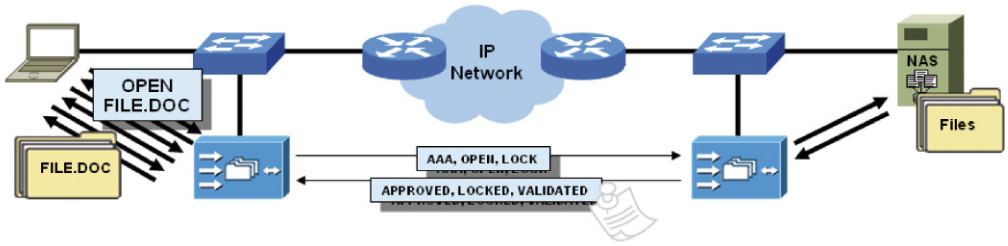
Wide Area Files Systems (WAFS)

Analyse de flux (flow parsing)

Le logiciel Cisco WAAS fournit une interface protocolaire serveur CIFS aux utilisateurs du site (sur les WAE edge) et présente une interface protocolaire cliente CIFS vers les serveurs de fichiers et les NAS du data center (sur les WAE core). Etant en lui-même une interface protocolaire avec des fonctions d'analyse de paquets avancées, le logiciel WAAS est capable de regarder dans chaque message de chaque flux. La fonction d'analyse de flux est responsable d'identifier les opérations au sein de chaque paquet pour déterminer la meilleure façon de les traiter.

Chaque flux qui impacte directement l'intégrité des données, l'authenticité de l'identité de l'utilisateur ou les niveaux d'accréditation est transmis de manière synchrone au serveur de fichier d'origine via un mécanisme de transport optimisé (décrit plus loin dans ce document).

Figure 11 : Gestion des opérations synchrones



Les opérations toujours traitées par le serveur d'origine sont notamment les suivantes :

- **Authentification des utilisateurs :** les opérations d'établissement et fermeture de session, authentification utilisateur incluse, sont toujours gérées par le serveur de fichier ou le NAS central. De ce fait, il n'est pas nécessaire de redéfinir les utilisateurs d'un site distant et la sécurité d'accès aux fichiers est toujours gérée par les mécanismes d'authentification en central (comme par exemple l'Active Directory).
- **Autorisation des utilisateurs :** les opérations de connexion et déconnexion à une ressource requièrent que l'utilisateur soit autorisé à y accéder. Toutes les demandes d'autorisation d'accès aux ressources sont aussi contrôlées par le serveur ou le NAS d'origine. De ce fait, de même que pour l'authentification, tous les mécanismes d'autorisation centralisés s'appliquent : permissions partagées, politique de groupe, permissions sur le système de fichiers, gestion des quotas,….
- **Vérouillage des fichiers (locking) :** pour garantir que les fichiers puissent être partagés par des utilisateurs situés sur de multiples sites, les demandes de verrouillage de fichier sont transmises au serveur ou NAS central dans le data center. En délégant la gestion du verrouillage au serveur central, tous les utilisateurs peuvent sans aucun problème travailler sur les même fichiers, en disposant toujours de la dernière version, et ce sans se soucier de l'intégrité des données. Le serveur de fichiers gère donc toutes les demandes de verrouillage mais aussi toutes les notifications de verrouillage, par exemple lorsqu'un fichier est déjà ouvert par un utilisateur d'un autre site. Contrairement aux architectures qui distribuent la gestion du verrouillage, il ne peut pas y avoir d'incohérence dans les données suite à une panne quelconque de l'infrastructure.
- **Ouverture et fermeture avec vidange des buffers :** les demandes d'ouverture et de fermeture de fichiers sont propagées de manière synchrone vers le serveur de fichiers ou NAS central pour garantir l'application des modes partagés et pour préserver les sémantiques protocolaires. De plus, la visibilité sur ces requêtes permet au logiciel WAAS de toujours connaître l'état d'un fichier sur les serveurs. L'opération de fermeture implique un transfert immédiat de toutes les données stockées dans les buffers avant de confirmer l'opération à l'utilisateur. Ce dernier est donc certain que son fichier est sauvegardé et présent intégralement à jour sur le NAS central lorsqu'il reçoit le message de confirmation.

Mécanismes de cache

Le logiciel WAAS utilise un cache de segments de fichiers (data cache) ainsi qu'un cache de métadonnées (metadata cache) qui sont utilisés pour maintenir des copies de fichiers et dossiers récemment consultés. De plus, un cache «write-back» permet de masquer les contraintes de performance lorsque l'on sauvegarde un fichier via le WAN.

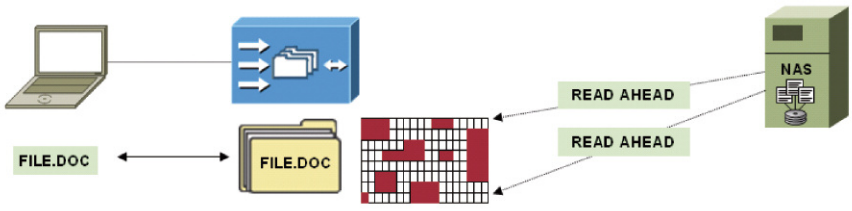
Le Data Cache : le data cache est un point de stockage des segments de fichiers qui ont été précédemment consultés ou volontairement pré-positionnés. Du fait que les protocoles d'accès aux fichiers fonctionnent en mode segment (les clients demandent en fait un certain nombre d'octets d'un fichier pour fournir les données nécessaires à l'environnement applicatif), l'usage d'un cache adapté permet de servir uniquement les segments disponibles et nécessaires, même si le fichier n'est pas intégralement présent. Lorsque l'utilisateur ouvre un fichier, un processus de validation («validate-on-open») est immédiatement déclenché pour comparer le contenu du cache avec celui du serveur central, afin que le logiciel WAAS ne délivre pas une version obsolète du fichier. Différents mécanismes sont utilisés pour cela comme une comparaison des métadonnées des fichiers demandés. Si la comparaison «validate-on-open» du fichier échoue, les segments concernés du fichier sont effacés du cache et remplacés par une nouvelle copie à jour des données du serveur central.

Le Metadata Cache : le cache des métadonnées offre un stockage des informations relatives aux structures des répertoires et fichiers du serveur central, ainsi que des fichiers présents dans le data cache. De nombreuses requêtes de métadonnées d'un utilisateur peuvent être servies directement depuis le metadata cache, cela comprend la navigation dans les répertoires ou encore les opérations de recherche. Contrairement aux données des fichiers qui sont validées à chaque accès, le metadata cache est contrôllé à intervalle de temps régulier et configurable (15 minutes par défaut).

Cache «write-back» asynchrone : le logiciel WAAS dispose d'un buffer «write-back» asynchrone qui masque les difficultés à écrire des données via le WAN. Il permet notamment de concaténer plusieurs opérations d'écriture pour maximiser l'usage de la bande passante et donc limiter l'impact de la latence (mécanisme connu sous le nom de «pipelining»). Les opérations d'écriture initiées par les utilisateurs sont examinées et classifiées comme supportant un traitement asynchrone ou non. Une opération supportant ce mode est par exemple une écriture pour laquelle le client n'attend pas de réponse immédiate. Cela ne remet en rien en cause l'intégrité des données. A contrario, l'opération de fermeture de fichier où l'utilisateur sauve son document et ferme l'application par exemple doit être traité de manière synchrone et ne bénéficie donc pas du cache «write-back». De la même manière, certaines opérations peuvent avoir été marquées comme synchrone par l'application et ne peuvent donc pas être cachées.

Lecture intelligente en avance de phase («read-ahead») : le logiciel WAAS suit également l'activité des utilisateurs et de leurs accès aux fichiers, ce qui lui permet de pronostiquer un certain nombre de lectures en avance de phase à réaliser. Il va ainsi charger de lui-même des segments de fichiers qui n'ont pas encore été consultés ni cachés, dans le souci d'améliorer les temps de réponse pendant que l'utilisateur continue à travailler sur le même fichier.

Figure 12 : Illustration du cache de segments et de la fonction "read-ahead" de WAAS



Proxies protocolaires

Le logiciel WAAS joue un rôle de proxy intelligent pour le protocole CIFS. De ce fait, il est capable de traiter un grand nombre de messages localement, libérant le WAN des multiples échanges qu'ils occasionnent et réduisant ainsi grandement les temps d'accès aux fichiers.

Le logiciel WAAS dispose donc du proxy protocolaire suivant :

- CIFS : ce proxy interprète l'intégralité des opérations CIFS. Il permet également d'insérer WAAS dans une architecture DFS en tant que point de réplication local des ressources. Dans un environnement Microsoft, WAAS peut donc être utilisé de 3 manières différentes :
    - En adressage directe CIFS : les utilisateurs indiquent l'UNC du WAAS pour accéder à leurs ressources
    - En l'intégrant dans un environnement DFS : les utilisateurs pointent sur le partage «root» et sont redirigés sur l'appliance du site.
    - En utilisant la redirection WCCP : le WAAS constate qu'un utilisateur tente d'accéder à une ressource centrale et insère ses fonctions d'optimisation de manière transparente.

Si nécessaire, par exemple pour gérer des «home directories» locaux, il est possible de configurer WAAS pour gérer de la cohérence locale pour les accès aux fichiers et donc d'utiliser les mécanismes d'opportunistic Locking (OpLock) de CIFS.

Dans les deux cas, le système d'optimisation repose en grande partie sur un mécanisme nommé IMS (Intelligent Message Suppression). Un tunnel TCP permanent est établie entre un WAE edge et un WAE core du data center. Toutes les communications CIFS entre le site distant et le site central sont reformatées afin de les optimiser et de ne transmettre via le tunnel que les messages réellement nécessaires. Le WAE réceptionnant des instructions ou des données par le tunnel les retransforment en CIFS natif pour les transmettre au destinataire (utilisateur ou NAS).

IMS permet notamment de :

- traiter un maximum d'opérations en local et ainsi minimiser les échanges.
- grouper les commandes (notion de commandes composite)
- pronostiquer les futurs messages et pré-charger le data cache par anticipation

Pré-positionnement de fichiers

Le logiciel WAAS permet de pré-positionner ou «pousser» des fichiers sur les WAE edge de manière contrôlée à partir du Central Manager, et ceci de manière immédiate ou programmée.

Le choix des fichiers à distribuer peut se faire selon une sélection automatique par motif (ex : tous les fichiers commençant par xyz). Les recherches récursives de fichiers au sein d'une arborescence de répertoires sont également supportées.

Le choix des WAE edge de destination se font soit appliance par appliance, soit par groupe d'appliances, soit sur toutes les appliances.

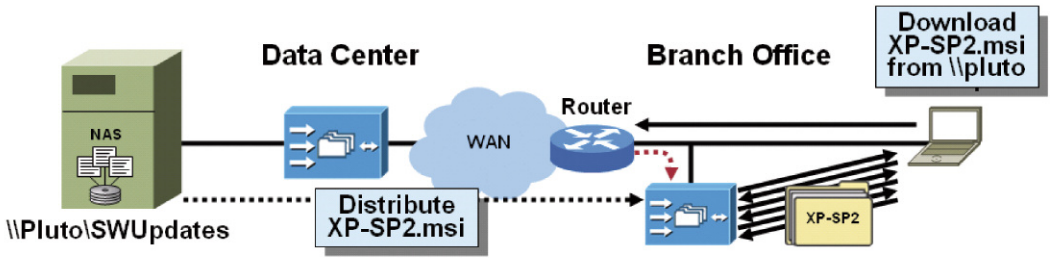
La fonction de pré-positionnement prend également certaines contraintes en compte avant de réaliser l'opération. Celles-ci sont configurables par l'administrateur qui programme la tâche. Elles peuvent être de natures suivantes :

- Plage horaire autorisée pour l'opération
- Espace de cache disponible sur les WAE cibles
- Taille maximale des fichiers distribuables
- Fréquence d'utilisation des fichiers (en fonction de la date de dernière modification)

Enfin, l'opération de pré-positionnement est optimisée, et ce de trois manières :

- Si le fichier existe déjà (en entier ou partiellement), seuls les segments manquants ou modifiés sont transférés
- Les fichiers complets sont distribués s'ils ne sont pas du tout présent dans le cache de l'appliance de destination
- La distribution tient compte de l'expiration potentielle des données du cache si celui-ci est déjà plein.

Figure 13 : Illustration du pré-positionnement de fichiers

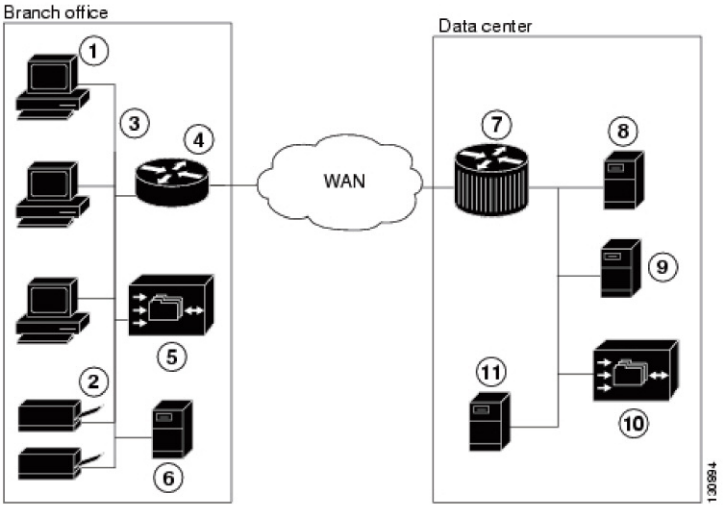


Services d'impression Windows

La solution WAAS Cisco inclue un serveur d'impression, qui permet de gérer les travaux d'impression directement au niveau du WAE edge, éliminant ainsi le besoin d'un serveur d'impression dédié dans les sites distants. Les services d'impression de WAAS sont comparables aux services d'impression Windows, et fonctionnent avec la grande majorité des imprimantes. Pour les utilisateurs, il est possible de downloader les drivers des imprimantes depuis le WAE edge (qui implémente la fonctionnalité Print Server), ce qui permet une intégration complète avec les wizards d'installation d'imprimantes de Windows. Les clients Windows peuvent alors automatiquement télécharger les drivers requis sur leur PC à partir du WAE edge. D'autre part, le service d'impression du WAE fournit aussi la gestion complète de la queue d'impression, incluant le monitoring du statut des travaux d'impression.

Topologie du service d'impression des sites distants

Une topologie typique d'un serveur d'impression dans un site distant est composée de stations clientes utilisant un seul serveur d'impression en proxy de plusieurs imprimantes. La configuration inclue aussi un domain controller et d'autres composants. En utilisant la solution WAAS pour le service d'impression, cette configuration inclue aussi le WAE. Le serveur de fichiers est par contre positionné sur le data center central.



1	Clients CIFS sur le site distant	7	Routeur Cisco dans le data center
2	Imprimantes réseaux sur le site distant	8	Serveur de fichiers dans le data center
3	Réseau local sur le site distant	9	Backup du serveur de fichiers dans le data center
4	Routeur Cisco sur le site distant	10	WAE servant de Core WAE dans le data center (Cisco WAE-512/ WAE-612/WAE-7326)
5	WAE servant de Edge WAE sur le site distant (Cisco WAE-512, Cisco WAE-612, Cisco WAE-7326)	11	Domain controller dans le data center
6	Domain controller sur le site distant		

A savoir, lorsque plusieurs domain controllers sont disponibles, il est préférable d'utiliser celui qui a la latence la plus faible avec le client, typiquement celui sur le site distant. Si le réseau est indisponible et que le Domain Controller est dans le data center, les services d'impressions peuvent être interrompus.

Dans cette configuration, le WAE du site distant fournit le service local d'impression aux clients de ce site. Les clients Microsoft utilisent le WAE Print Server exactement comme ils le feraient avec un serveur d'impression Microsoft :

- Les clients doivent ajouter ou retirer les queues d'impression sur leur PC personnel en utilisant les Wizard Windows, et en pointant sur le nom du WAE Print Server
- Les clients peuvent gérer les travaux d'impression sur le WAE Print Server
- Le serveur d'impression WAE communique avec les imprimantes pour leurs fonctions d'impression
- Les services d'impression de WAAS interopèrent avec le modèle de sécurité de Windows, nécessitant que les clients soient authentifiés à travers un Active Directory (NTLM v1 et v2 sont supportés).

La solution de services d'impression WAAS

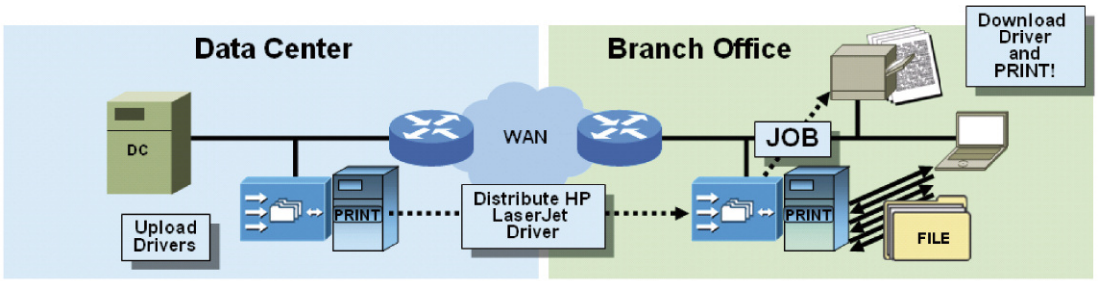
Les services d'impression de WAAS font partie intégrante de la configuration des WAE. Le serveur d'impression du WAE est une solution d'impression complète, consistant en deux composants majeurs :

- **Samba :** WAAS utilise Samba pour permettre aux clients Microsoft d'ajouter ou de retirer les queues d'impression, les drivers, de parcourir les queues d'impression, et de gérer les travaux sur le WAE. WINBIND, un composant de Samba, permet d'utiliser les mécanismes d'authentification et d'autorisation entre les clients Windows et le Domain Controller.
- **Common Unix Printing System (CUPS) :** WAFS utilise CUPS pour la gestion des queues d'impression et pour envoyer les travaux des clients Microsoft vers les imprimantes via TCP/IP.

Distribution des drivers

Le WAE central manager s'enregistre auprès de l'Active Directory. Cela fait, l'administrateur recopie les drivers sur ce serveur. Les WAE edge s'enregistrent aussi auprès de l'AD et fournissent les services d'impression en local, après avoir reçu les drivers directement par le central manager. Les drivers d'imprimante sont alors accessibles sur les sites distants avec le support de la fonctionnalité "Click-N-Print" (partage PRINT$).

Figure 14 : Distribution des drivers d'impression



INTERCEPTION TRANSPARENTE DES FLUX

Utilisation de la redirection avec WCCPv2

Qu'est-ce que WCCPv2 ?

WCCP, ou Web Cache Communication Protocol, est un mécanisme disponible sur les routeurs Cisco depuis 1997, ainsi que sur certaines gammes de commutateurs. Il assure la redirection du trafic en temps réel vers un groupe de caches. Cela n'interfère pas avec le fonctionnement normal des routeurs et des commutateurs.

WCCP permet de configurer des groupes de service, correspondant à des interceptions applicatives, auxquels viennent s'abonner tout équipement souhaitant recevoir ces flux. L'application à intercepter est caractérisée par son protocole de transport, UDP ou TCP, ainsi que par le numéro de port.

Les bénéfices apportés par WCCPv2 concernant le service WAAS sont les suivants :

- Equilibrage de charge sur l'ensemble des WAE Edge du site distant
- Tolérance aux pannes d'un WAE

Les versions logicielles minimum par plateforme pour supporter WCCPv2 sont les suivantes :

- Routeur : IOS 12.0(3)T (version 12.2 ou supérieure recommandée)
- Catalyst 6500 (redirection L2) : IOS 12.1(2)E
- Catalyst 6500 / Sup720 (toute redirection) : IOS 12.2(18)SXD4
- Catalyst 4500 : supporté depuis la version 12.2(31)SG
- Catalyst 3750/3560 : à venir en Q1 2007

Gestion des flux interceptés

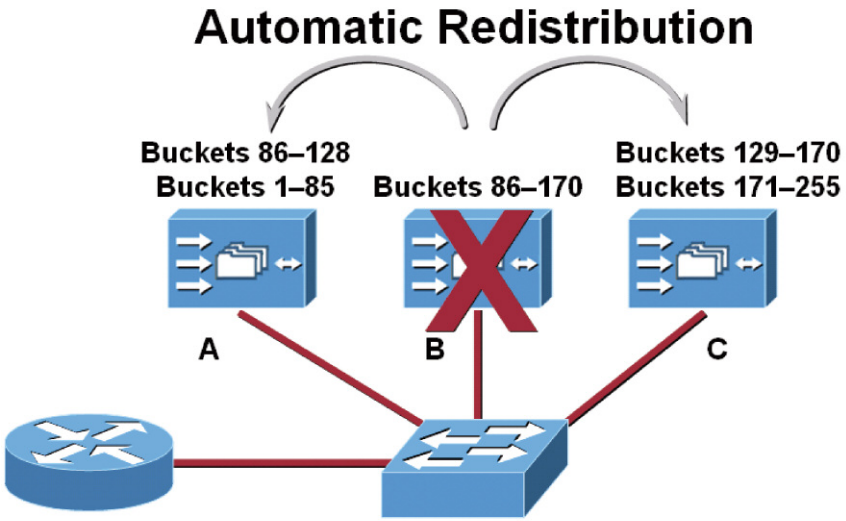
WCCP offre un mécanisme d'équilibrage de charge simple et performant en fonction de l'adresse IP source et / ou destination des flux interceptés. Ce partage de charge peut évoluer dynamiquement pour prendre en compte aussi bien l'introduction de nouvelles appliances pour ajouter de la capacité de traitement que la perte de toutes les appliances.

Le routeur cherche en permanence à répartir un lot de 256 jetons de charge entre tous les WAE qui se sont abonnés à un service de redirection donné. S'ils sont au nombre de 3 et qu'aucune pondération particulière n'est paramétrée, le routeur attribuera 85 jetons à chacun d'entre eux : de 1 à 85 pour le premier, de 86 à 170 pour le second et de 171 à 255 pour le dernier.

L'appliance qui traitera un flux donné est simplement déterminé en passant l'adresse IP source et/ou destination dans une fonction de hachage qui retourne une valeur entre 1 et 256, correspondant à un numéro de jeton. Le WAE choisi par le routeur est celui à qui le jeton a été attribué. La fonction de hachage garanti qu'un même flux passera toujours par le même WAE (à moins d'un changement dans le nombre d'appliances disponibles).

Si l'un des 3 WAE de l'exemple précédent vient à être retirer de l'architecture, le routeur constate automatiquement sa disparition et répartit à nouveau les jetons entre les 2 appliances restantes.

Figure 15 : Algorithme de partage de charge WCCP



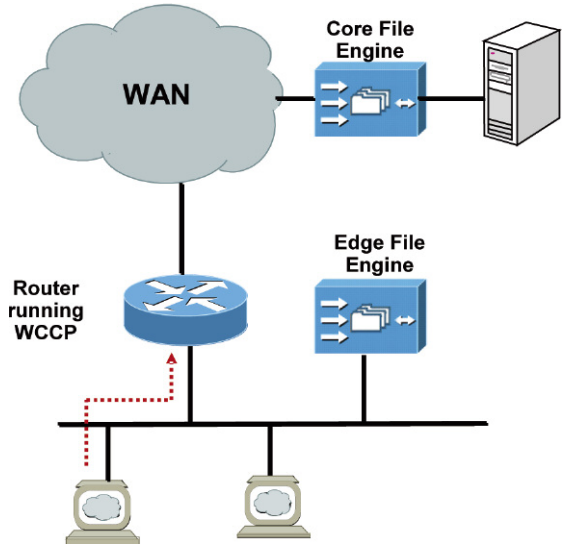
Lorsqu'aucun WAE n'est enregistré à un service donné, ou lorsque tous les WAE ont été retirés, le routeur arrête automatiquement l'interception et transmet le trafic directement au travers du WAN. **De cette manière, en cas de panne des appliances, le trafic n'est plus optimisé mais le service continue de fonctionner.**

Fonctionnement de l'interception WCCP

Lors de l'accès aux fichiers, les étapes sont les suivantes :

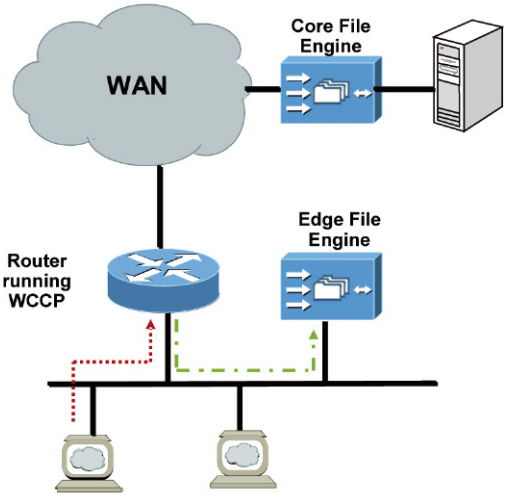
1) Le client initie la communication vers le serveur de fichiers.

Figure 16 : Requête initiale



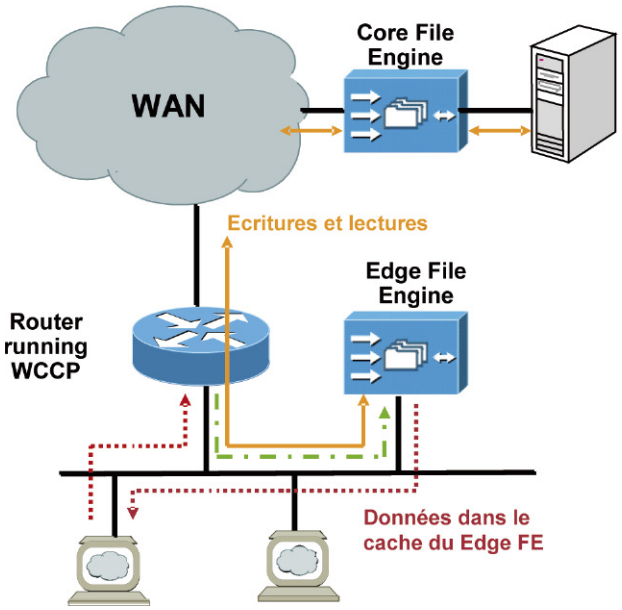
2) Le routeur intercepte le flux et le redirige vers le WAE Edge. Le paquet original est encapsulé dans une trame GRE à destination du WAE Core pour ne pas modifier l'adresse IP source. Les commutateurs tels que les Catalyst 6500 et Catalyst 4500 peuvent également faire de la redirection de niveau 2 sans altérer les adresses IP de la trame. Par contre, cette seconde solution nécessite une connexion directe des WAE sur le commutateur.

Figure 17 : Interception WCCP



3) Dans le cas où la donnée est présente dans le cache du Edge (cache hit), celle-ci est fournie directement par celui-ci. Sinon, la donnée est récupérée du serveur de fichier (cache miss).

Figure 18 : Propagation de la requêtes en central en cas de "cache miss"



Exemple de configuration WCCP

L'exemple ci-dessous indique comment configurer une redirection TCP générique sur les routeurs et les appliances WAE edge. Il utilise le service pré-défini « tcp-promiscuous » correspondant aux groupes WCCP 61 et 62.

Figure 19 : Points de redirection sur les routeurs pour le trafic entrant et sortant

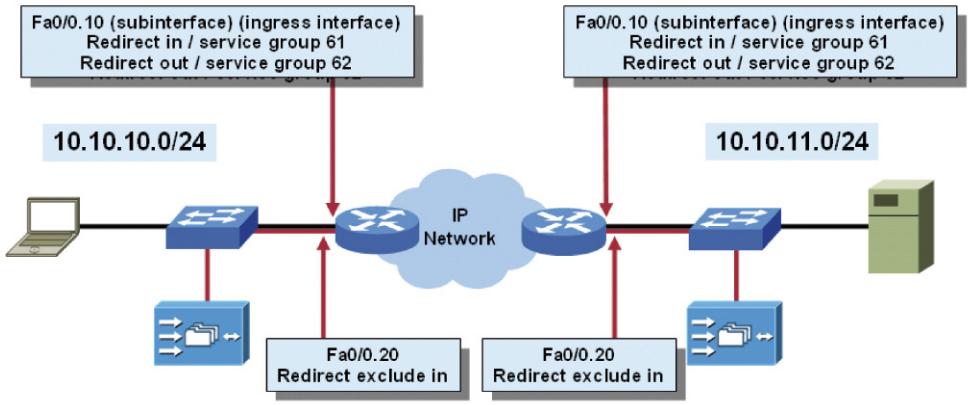


Tableau 3 : Configuration sur le WAE edge

Commande	Description
WAE(config)# wccp version 2	Enable WCCPv2
WAE(config)# wccp router-list 1 10.10.10.	Define router list, specify all applicable WCCPv2 routers
WAE(config)# wccp tcp-promiscuous router-list-num 1	Register with router-list 1 as a promiscuous TCP device (using service groups 61 and 62)

Tableau 4 : Configuration sur le routeur

Commande	Description
Rtr(config)# ip wccp version 2	Enable WCCPv2
Rtr(config)# ip wccp 61	Enable service group 61
Rtr(config)# ip wccp 62	Enable service group 62
Rtr(config)# int FastEthernet0/0.10	Enter subinterface configuration mode (LAN interface)
Rtr(config-if)# ip wccp 61 redirect in Rtr(config-if)# ip wccp 62 redirect out	Specify inbound redirection for service group 61 and outbound redirection for service group 62
Rtr(config-if)# int FastEthernet0/0.20	Enter subinterface configuration mode (where the WAE is attached)
Rtr(config-if)# ip wccp redirect exclude in	Specify that packets received on this interface should not be considered WCCPv2 redirection candidates on other interfaces

Utilisation du Policy Base Routing (PBR)

Policy-based Routing (PBR) permet aux administrateurs réseaux de configurer certains équipements (en particulier pour l'utilisation dans le cadre du WAAS, le dernier routeur ou switch avant le WAN) pour qu'ils appliquent un routage particulier pour un certain type de trafic que ces mêmes équipements vont classifier.

Le principe de configuration de PBR est de tout d'abord positionner une access-list qui va identifier le trafic considéré comme intéressant pour la redirection. Ensuite, une route-map est créée, associant une action à exécuter avec le trafic qui 'match' cette access-list. Finalement, on applique la policy route-map sur l'interface LAN du routeur. La CLI de cette configuration est très similaire à celui de la QOS.

La notion de haute disponibilité avec le PBR est obtenue par l'une des deux méthodes suivantes :

- **Option 1 –** Si le router ou le switch voit le WAE en tant que voisin CDP (Cisco Discovery Protocol), il peut alors vérifier que le WAE est bien vivant.

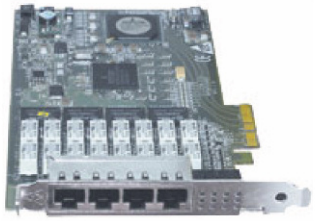
- **Option 2 –** Si le WAE n'est pas un voisin CDP, on peut utiliser IP SLAs pour suivre la disponibilité du WAE en utilisant soit les probes ICMP, soit une tentative de connexion TCP (nécessite un IOS 12.4 ou supérieur).

Il faut aussi configurer WCCP v2 sur les WAE afin qu'ils comprennent qu'il y a eu une redirection du trafic qu'ils sont en train de recevoir.

Positionnement du WAE en coupure

Une troisième méthode va consister à positionner le WAE en coupure entre le LAN et le routeur. Ainsi tous les flux vont passer à travers le WAE. Seuls les flux qui auront été définis pour être optimisés, seront traités par les algorithmes d'optimisation du WAE. Les autres traverseront tout simplement sans traitement du WAE. Un mécanisme de bypass physique permettra de gérer un disfonctionnement du WAE.

Cette solution de positionnement en coupure sera disponible en Q4 2006. Elle nécessitera l'ajout d'un module dans les WAE équipés de 4 ports RJ45, assurant un bypass physique en cas de dysfonctionnement du WAE :



DISPONIBILITE DU SERVICE WAAS

Associées avec WCCPv2, les appliances WAAS offrent une garantie de transparence lors de l'implémentation, mais aussi assurent la disponibilité du service d'optimisation des accès fichiers. Le déploiement de plusieurs appliance sur chaque site agence assure la tolérance aux pannes d'un boîtier par redirection WCCP sur le boîtier opérationnel.

Il est aussi recommandé de déployer un cluster au niveau des WAE Core afin d'assurer la tolérance aux pannes d'un boîtier sur le site central. Le mécanisme de clustering WAAS pour les WAE core offre à la fois résilience et partage de charge pour tous les WAE edge.

Dans le cas où tous les éléments WAAS seraient inopérants, la transparence de l'implémentation, grâce à WCCP v2, assure la continuité d'accès aux fichiers sans les bénéfices apportés par le service WAAS.

Dans un environnement Windows avec DFS, les boîtiers WAAS assurent le rôle de réplicas des données. Lors de la défaillance d'un élément, le serveur DFS assure l'accès aux données via le réplica le plus proche. La tolérance aux pannes est donc assurée nativement par DFS.

Le service WAAS assure la continuité de service dans le cas d'une déconnexion du réseau dont la durée est inférieure à 90 secondes. Les requêtes en cours sont mises en attente sur l'Edge. Si l'incident réseau dure moins de 90 secondes, la perte de connexion est transparente pour les utilisateurs. Dans le cas où la connexion n'est pas rétablie, les requêtes clients sont rejetées et l'Edge lance des tentatives de reconnexion régulièrement.

Le Central Manager est uniquement un outil de configuration globale de l'architecture. Une fois ce paramétrage poussé sur les appliances WAE core et edge, la perte temporaire de cette fonction n'a aucun impact sur le fonctionnement du système.

Disponibilité matérielle des appliances WAE

Les matériels proposés disposent des niveaux de redondance interne suivants :

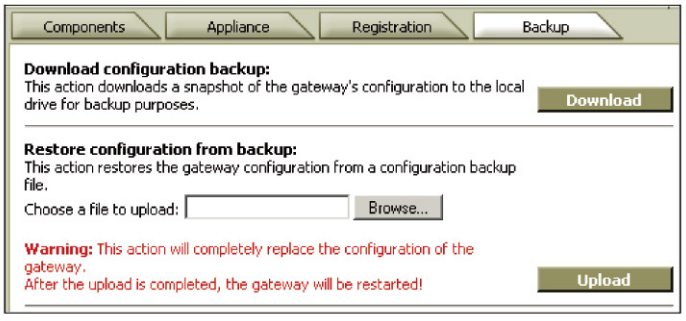
- WAE-512 : supporte deux disques SATA2 configurables en RAID mais qui ne sont pas échangeables à chaud. Pas d'alimentations redondantes.
- WAE-612 : supporte deux disques SCSI SAS configurables en RAID et échangeables à chaud. Pas d'alimentations redondantes.
- WAE-7326 : cette appliance dispose d'une double alimentation et de disques SCSI et ventilateurs échangeables à chaud.

Dans le cas où un matériel serait défectueux, son remplacement par un nouveau matériel est très rapide puisque le logiciel WAAS est pré-chargé sur les disques. Il suffit de restaurer la configuration pour que le boîtier soit opérationnel.

Sauvegarde / restauration des configurations des appliances

Depuis l'interface d'administration des boîtiers WAAS, il est possible de sauvegarder la configuration de l'appliance et donc de la restaurer rapidement sur une autre appliance.

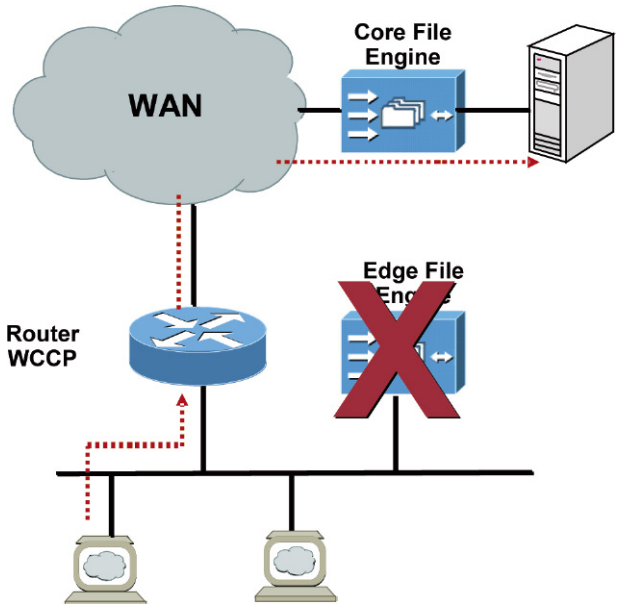
Figure 20 : Sauvegarde et restauration des appliances WAE



Disponibilité de l'architecture WAAS

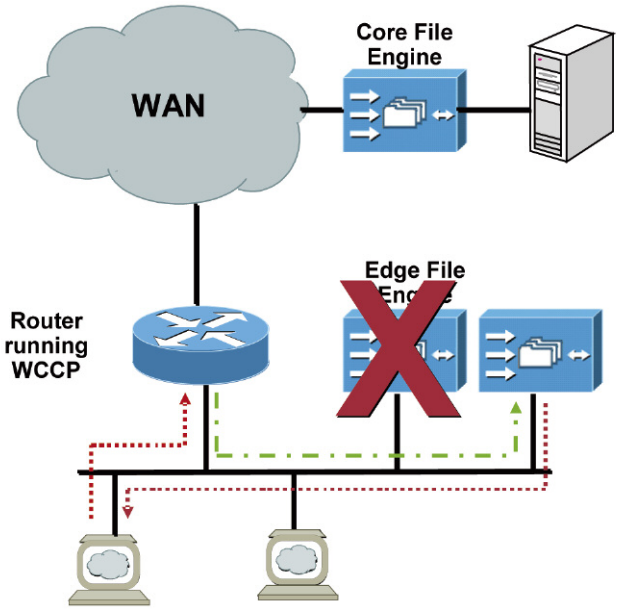
En fonctionnement avec WCCPv2 (recommandé), lors de la perte de l'appliance Edge du site distant, les flux ne sont redirigés par le routeur vers le WAE et ils sont donc envoyés à travers le WAN directement vers le serveur de fichiers. L'utilisateur accède toujours aux données, sans toutefois bénéficier des améliorations WAAS.

Figure 21 : Bypass WCCP en cas de défaillance des WAE



Si plusieurs appliances Edge sont déployées sur le site distant, le routeur redirige les flux vers l'appliance en fonctionnement.

Figure 22 : Redistribution de la charge en cas de défaillance d'un WAE



Dans le cadre d'une implémentation avec DFS, le serveur Root DFS redirige les flux vers un autre réplica de données local.

Intégrité des données

Les droits et autorisations du serveur de fichiers ne sont pas modifiés ni interceptés par le service WAAS. L'utilisateur doit disposer des accès sur la ressource et les fichiers auxquels il souhaite accéder.

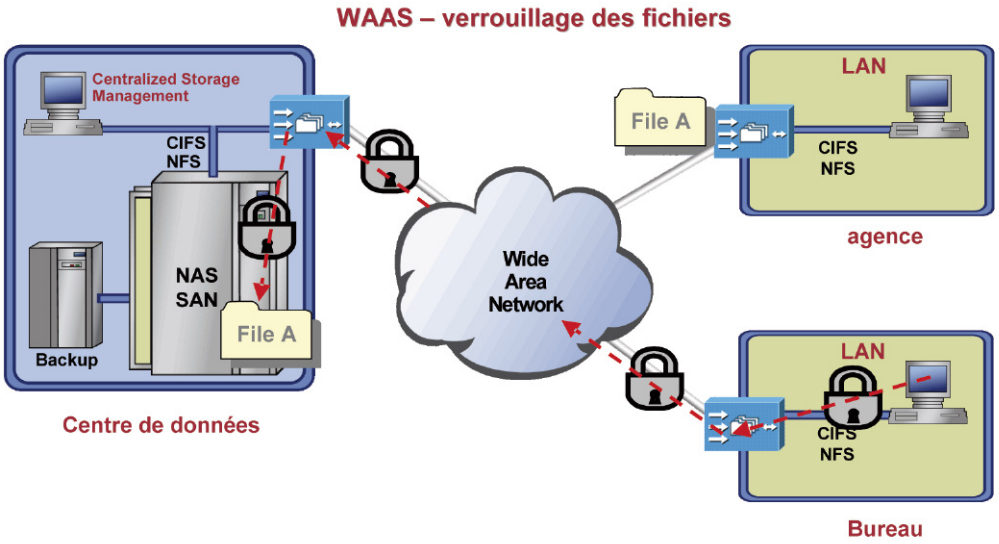
Accès à un fichier

Lors de l'ouverture d'un document par un utilisateur depuis un site distant, un lock est positionné sur le serveur de fichiers, garantissant que le fichier soit cohérant pour l'ensemble des utilisateurs du réseau.

Dans l'exemple ci-dessous, l'utilisateur depuis le site «bureau» a ouvert un fichier nommé «A» et positionne un verrou pour que les utilisateurs des autres sites ne puissent modifier le fichier.

Dans le cas où un utilisateur du site «agence» accède au fichier, il reçoit un message lui indiquant que le fichier est déjà ouvert par un autre utilisateur.

Figure 23 : Vérouillage des accès aux fichiers (locking)



Ecriture

Lors de l'écriture des données, les mises à jour effectuées depuis le site distant sont acquittées sur le serveur de fichier avant acquittement définitif de l'écriture au poste client. L'écriture est donc réalisée de manière synchrone, ce qui assure la cohérence des données dans le cas d'une perte d'accès au réseau ou lors d'un crash d'un élément de la chaîne.

ADMINISTRATION

L'ensemble des appliances WAAS déployées sur le réseau d'Entreprise est administré par le WAAS Central Manager.

WAAS Central Manager

WAAS Central Manager est installé sur une appliance de type WAE-512 dédiée. Lors de l'initialisation des boîtiers Core (site central) et Edge (site agence), l'adresse IP correspondant à l'appliance WAAS Central Manager est indiquée de manière à mettre en relation l'ensemble des boîtiers avec l'outil d'administration central.

L'interface d'administration est de type HTML et peut être accédée depuis n'importe quel point d'accès au réseau en HTTPS. Le Central Manager propose également une CLI évoluée de type IOS permettant de configurer la majorité des fonctions du système.

Authentification

Le Central Manager ainsi que les WAE arrivent par défaut avec un login administrateur.

Il est aussi possible d'ajouter deux types de comptes supplémentaires :

- Device-Based CLI account : ce type de compte fournit uniquement un accès CLI à un device (WAE) ou à un groupe de WAE.
- Roles-Based account : ce type de compte permet d'administrer et de configurer certaines fonctionnalités de WAAS (complètement paramétrables par l'administrateur principal) à travers l'interface graphique du Central Manager. En plus de la restriction au niveau fonctionnalité, on associe à ce compte un domaine qui peut être la totalité ou un sous-ensemble des WAE de l'architecture.

Pour les comptes Roles-Based, on peut aussi autoriser ou non ces comptes à accéder au CLI des WAE de son domaine.

Il existe aussi pour chaque type de compte 2 types de privilèges :

- Accès complet et modification des configurations
- Accès en visualisation uniquement

Directives de connectivité

Les directives de connectivité correspondent à la mise en relation d'un WAE Edge avec un WAE Core. Elles sont nécessaire à la publication des partages / points de montage du serveur de fichiers sur le WAE Edge.

Les paramètres à définir sont les suivants :

- Core WAE (ou cluster)
- Edge WAE (ou groupe)
- Définition de l'alias du serveur de fichiers (préfix / suffixe) si non WCCPv2
- Utilisation du WAN
    - Bande passante allouée maximum
    - Latence moyenne

Paramétrages WAAS

Les différents paramètres de communication entre les Core et les Edge sont effectués dans WAAS Central Manager :

- File Blocking : blocage de l'optimisation pour certains types de fichiers
- File prepositionning : mise à disposition des données dans le cache de l'Edge de manière planifiée pour optimiser les temps d'accès
- Policy distribution : tous les paramètres peuvent être transmis sur l'ensemble des WAE lors du déploiement de l'infrastructure

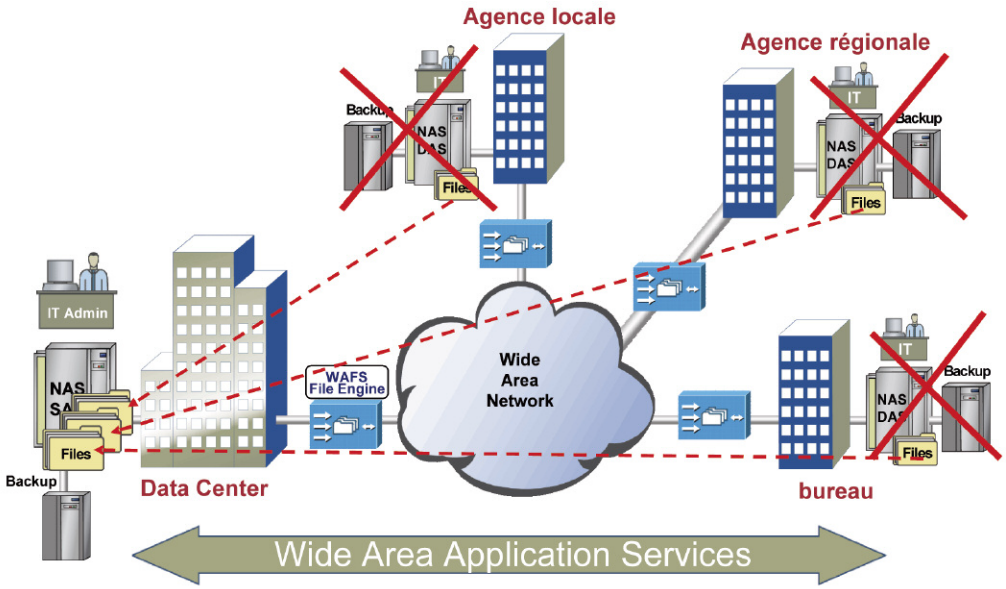
Déploiement

Le service WAAS est déployé hors du chemin de données. L'implémentation est donc transparente dans le cas où les routeurs disposent du service WCCPv2, ou de DFS en environnement Windows.

Le processus de déploiement est le suivant :

1) Les données et partages accédés précédemment en local dans les agences, sont déplacés vers le site central :

Figure 24 : Migration des NAS en architecture centralisée



2) Implémentation WAAS : WAAS Central Manager, Cores et Edges

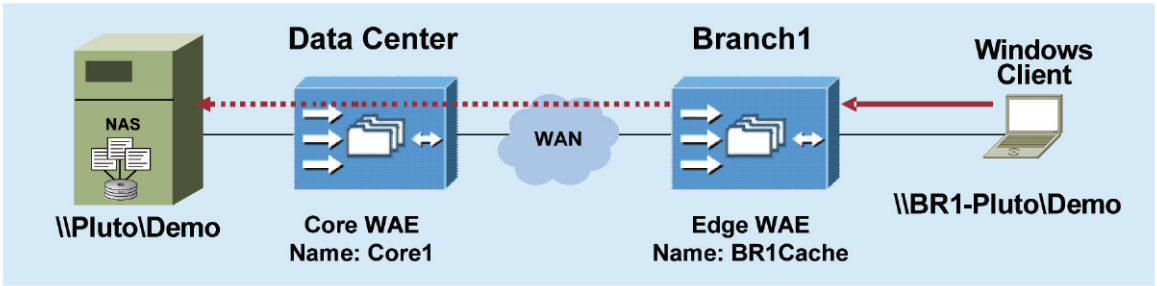
3) Paramétrage des clients pour accès aux données (si mode non transparent)

Le service WAAS repose sur la mise en relation entre un ou plusieurs WAE Core (cluster) et un ou plusieurs WAE Edge. Lors du paramétrage, les partages Windows à accélérer sont définis. Les requêtes des clients en agence relatives à ces partages et points de montage transitent alors via un tunnel entre l'Edge et le Core.

Environnement Windows en mode proxy

Après installation des appliances sur le réseau et définition des partages à accélérer, les clients doivent être configurés pour accéder aux ressources avec comme référence le nom de l'appliance Edge.

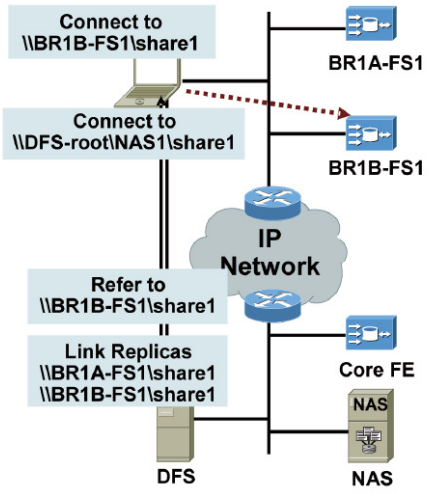
Figure 25 : Connexion d'un client CIFS en mode proxy



Environnement Windows en mode DFS

DFS fourni une arborescence unique pour l'ensemble des partages des serveurs du réseau. L'utilisateur se connecte à un volume sans connaître l'emplacement des données. Des réplicas sont définis sur le réseau pour donner l'accès aux données aux utilisateurs. Les appliances WAE font office de réplica et permettent de ne pas déployer de serveurs sur les sites agences. Les clients, lors de la demande d'accès aux fichiers, sont redirigés vers l'appliance WAE de proximité.

Figure 26 : Connexion d'un client CIF sur un partage DFS



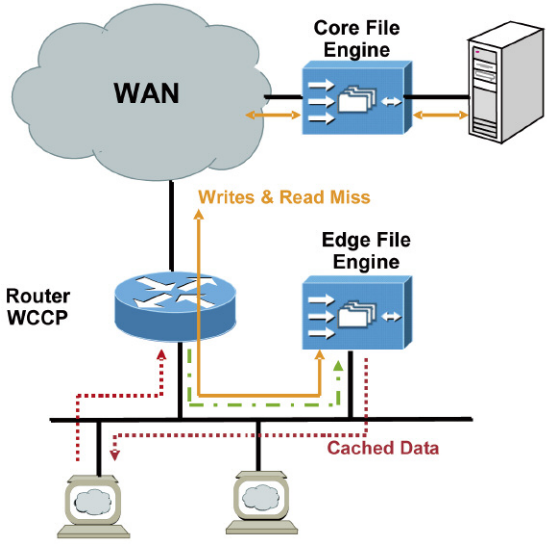
Dans le cadre d'une implémentation avec DFS, c'est le serveur DFS qui assure la disponibilité des accès aux données en affectant au client les boîtiers WAAS de proximité.

Environnement Windows en mode transparent

En mode transparent, WCCPv2 ou PBR, c'est le routeur qui redirige les flux des clients vers les boîtiers Edge du site agence.

Le client a comme référence le nom du serveur de fichiers et les partages publiés.

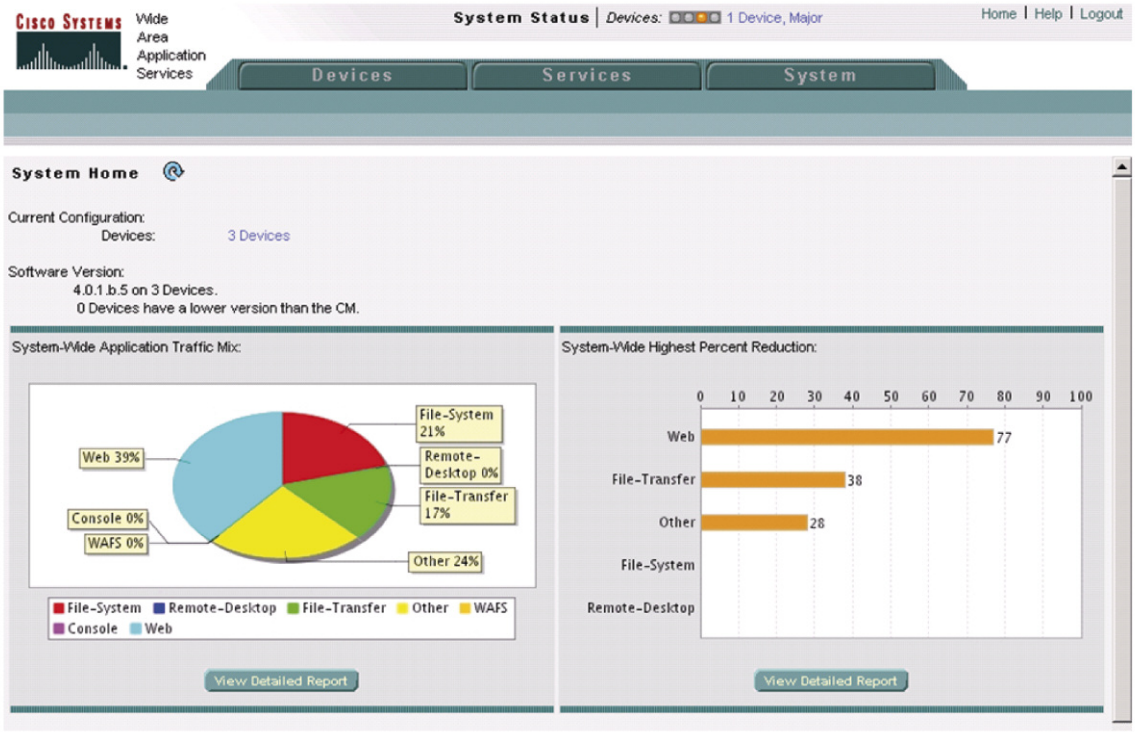
Figure 27 : Redirection transparente WCCP



Surveillance du système et des performances

Le logiciel WAAS offre nativement différents écrans de monitoring et de reporting sur l'activité de la solution, accessibles directement depuis le Central Manager. Dès que l'administrateur se connecte sur le système, la page d'accueil lui donne un tableau de bord synthétique et temps réel des principaux critères de performance de son système. Cela inclus notamment le nombre d'appliances WAE enregistrées, le résumé des versions logicielles déployées ainsi que les 10 principales applications reconnues sur le réseau. Pour celles-ci, des graphes simples et lisibles indiquent leur part d'occupation de la bande passante, ainsi qu'un classement des applications les plus optimisées.

Figure 28 : Tableau de bord de la page d'accueil du Central Manager



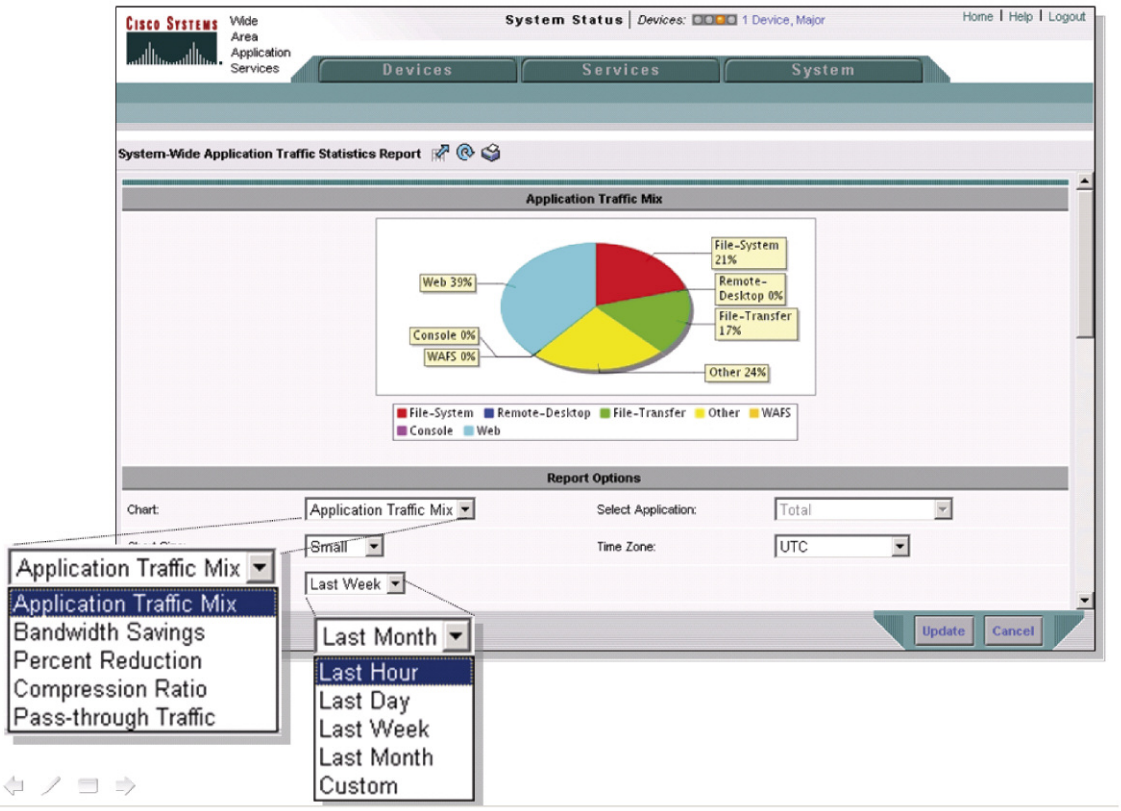
Ce tableau de bord offre également un lien direct vers l'outil de reporting détaillé de l'architecture WAAS. Celui-ci permet d'exploiter les informations historisées par le Central Manager afin d'en extraire l'un des rapports suivants :

- l'ensemble des applications traitées et reconnues
- les gains de bande passante réalisés
- le pourcentage de réduction des informations
- le taux de compression
- la quantité de trafic non optimisé.

L'administrateur peut choisir la période de temps désirée pour l'extraction des données tels que l'heure, le jour, la semaine ou le mois en cours, ou bien tout simplement indiquer la période exacte souhaitée (date de début, date de fin).

Les rapports peuvent également être affinés pour analyser plus précisément le comportement de certaines applications données. Pour cela WAAS distingue les applications suivantes : sauvegarde, distribution de contenu, services d'annuaire, email et messagerie, applications d'entreprise, système de fichiers, transferts de fichiers, peer-to-peer, impressions, « remote-desktop », réplications, SQL, flux de stockage, streaming vidéo, Web, flux d'administration de la solution (échanges système, gestion de version logicielle, flux de contrôle),…

Figure 29 : Outil de reporting détaillé sur l'architecture WAAS

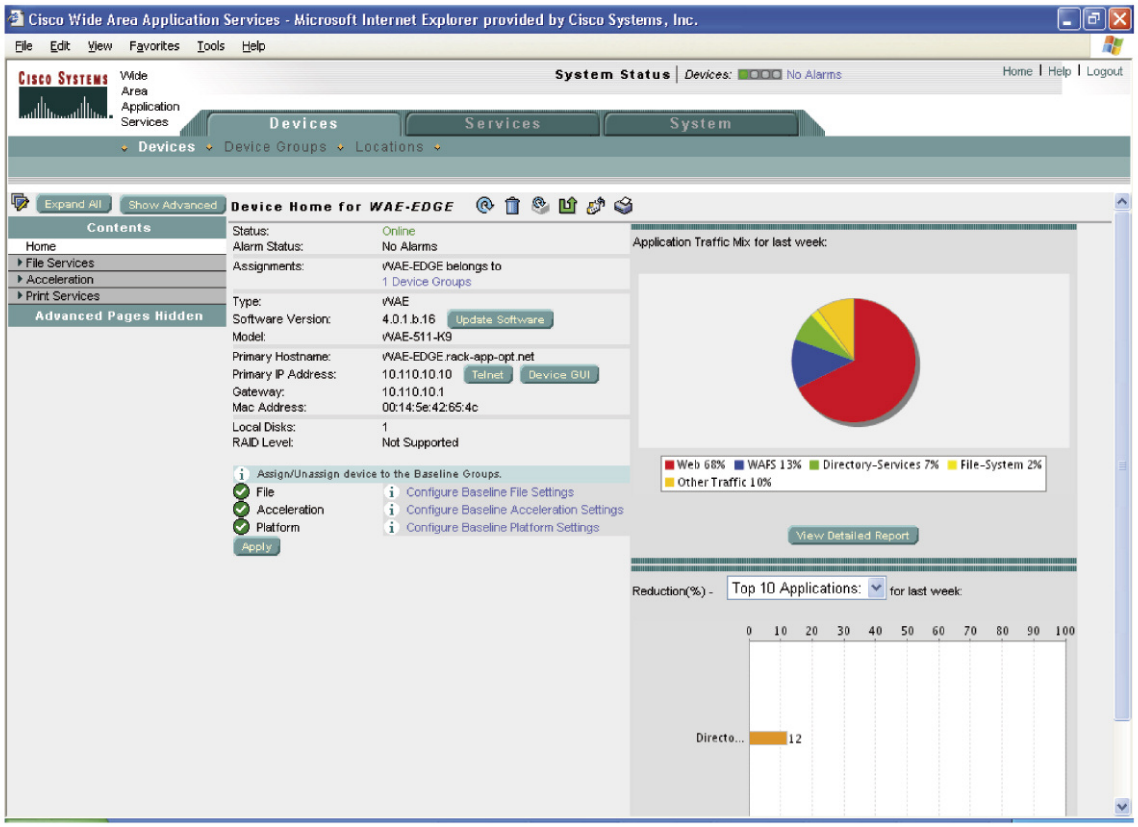


Le Central Manager dispose également de fonctions de surveillance de toutes les appliances WAE de l'architecture. Outre les remontées d'alarmes visibles très distinctement depuis le tableau de bord de la page d'accueil, chaque appliance dispose d'une page de supervision qui lui est propre. Les informations disponibles sur les appliances sont les suivantes :

- Etat de l'appliance (active, en erreur, inactive)
- Le nombre d'alarmes actives et le niveau de sévérité de la plus grave d'entre elles
- L'appartenance à un groupe
- Son type et son model précis
- Sa version logicielle
- Ses paramètres réseau (nom de machine, adresse IP, passerelle par défaut, adresse MAC)
- Les paramètres disque (nombre de disques, niveau RAID).

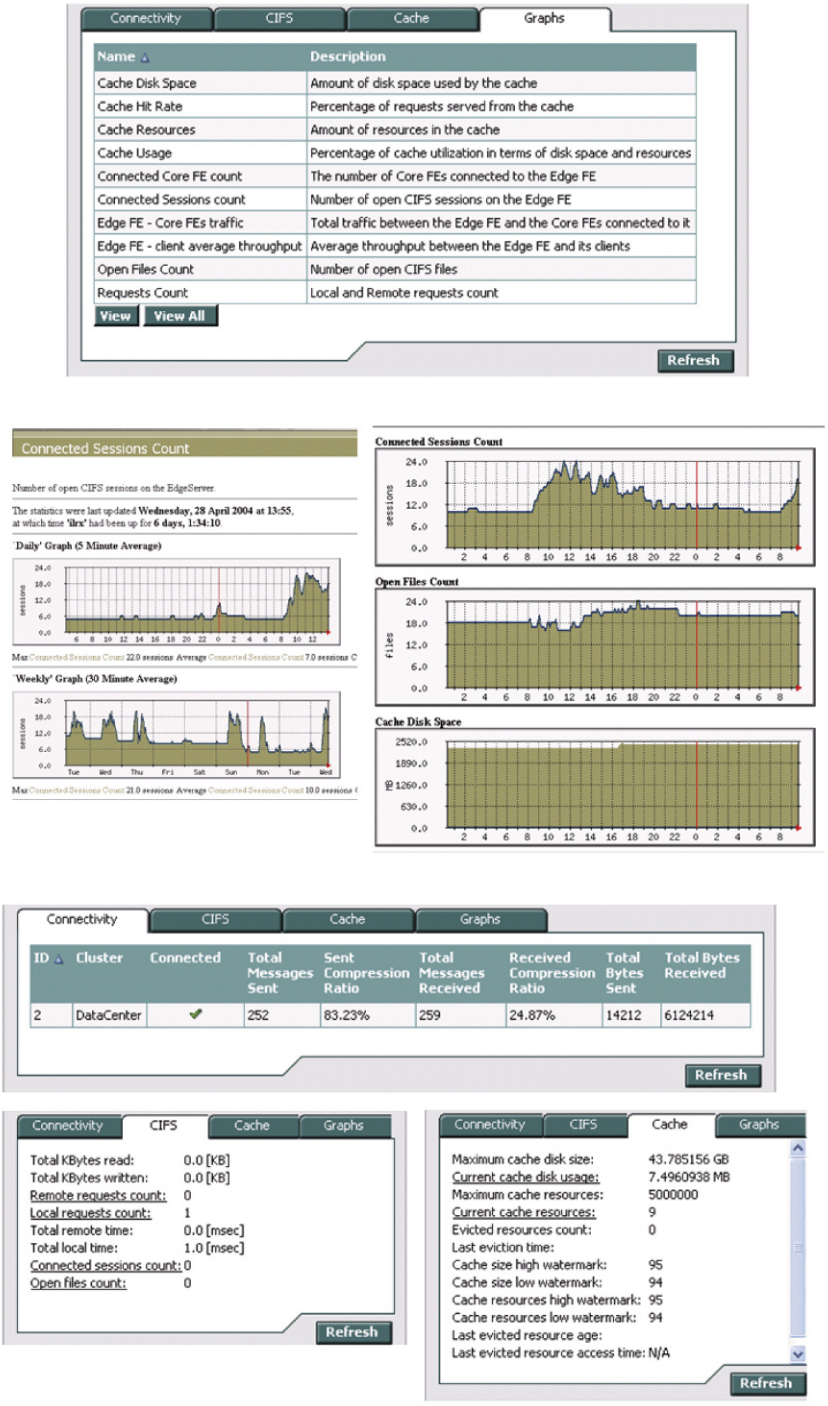
Tout comme pour le tableau de bord principal, il offre des rapports d'activité détaillés tirant profit de l'historisation faite pour chaque appliance. Ceux-ci donnent d'excellentes indications sur les applications utilisées sur chaque site et leur niveau d'optimisation.

Figure 30 : Tableau de bord des appliances



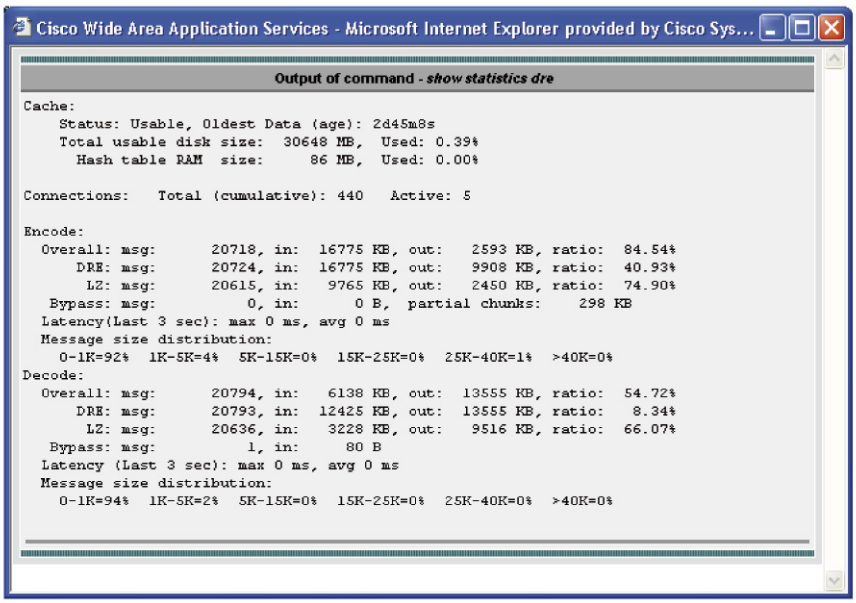
Enfin, il est également possible de récupérer des rapports et graphes pré-formatés sur l'usage des ressources internes de l'appliance WAE, ainsi que du volume de données qu'elle traite.

Figure 31 : Options de reporting par appliance WAE



Il est de plus possible d'accéder à des statistiques détaillées sur les différents mécanismes d'optimisation comme DRE, LZ et TFO, par un ensemble de « show command » accessibles directement à travers le CLI ou à travers le lancement de ces « show command » par le Central Manager :

Figure 32 : accès aux commandes Show à travers le CM



Gestion des évolutions

Evolutions logicielles

L'ensemble des appliances déployées sur le réseau d'Entreprise est géré depuis WAAS Central Manager. Les évolutions logicielles sont administrées depuis cette interface. Après téléchargement du nouveau code, celui-ci est déployé sur chaque Appliance sélectionnée.

Evolutions matérielles

Les sites agences peuvent évoluer en termes de nombre d'utilisateur, volumétrie des fichiers partagés et nombre d'imprimantes.

WAAS autorise les évolutions de plates-formes et les ajouts de composants mémoires et disques sur le matériel existant, suivant les limites matérielles de chaque élément.

Dans le cadre d'une implémentation transparente avec WCCPv2 associée avec la redondance des équipements, l'évolution est réalisée très rapidement et sans impact sur la production.

Supervision

Monitoring interne

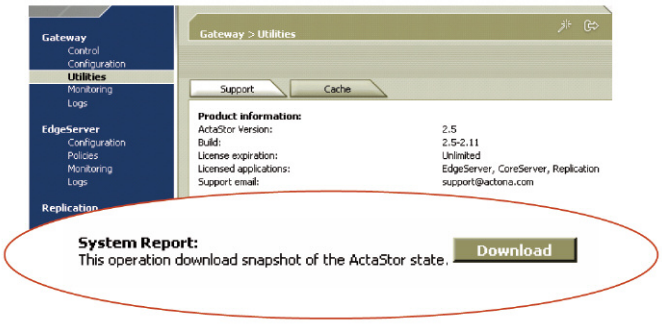
Chaque élément dispose de fichiers de LOG qui permettent une analyse rapide en cas d'incident :

- Admin Log,
- Internal Log : informations détaillées des événements
- Monitoring Log.

Les informations fournies sont de types INFO, WARNING, ERROR et FATAL.

Un outil est disponible sur chaque élément, le «system report», qui donne l'état de la configuration et les Logs pour le système et pour le service WAAS.

Figure 33 : Récupération des fichiers de log



Un mode «debug» est disponible depuis l'interface d'administration expert du boîtier. Le mode expert est réservé au support ou aux utilisateurs ayant une très bonne connaissance du service WAAS.

Analyse d'incidents

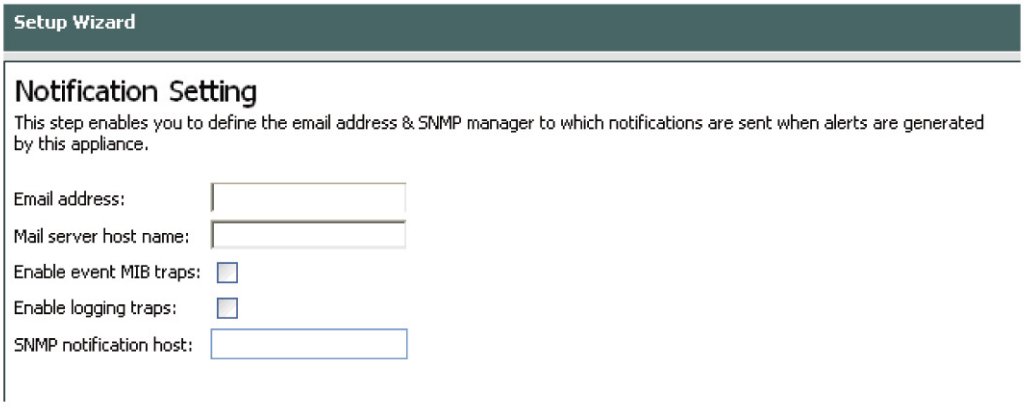
Il est possible de s'appuyer sur les outils des serveurs pour analyser les incidents. En règle générale, le réseau est souvent en cause. Il est donc important de connaître l'emplacement exact du problème.

- Outils réseau : NET, NBTSTAT, NSLOOKUP, PING, TRACERT, IPCONFIG, NETSH
- Outils spécifiques à l'environnement Windows : DFSUTIL, BROWSTAT, DCDIAG, NETDIAG, PERFMON

Intégration avec un superviseur

Chaque module Core et Edge dispose de mécanisme d'envoie de traps SNMP. Lors de l'initialisation du module, il suffit de renseigner la communauté et les paramètres relatifs à la console de supervision pour l'émission des traps.

Figure 34 : Programmation de notifications



Les MIBs Cisco sont accessibles via le collecteur SNMP de la manière suivante :

1) Le superviseur lance une requête au WAE
2) Le device agent qui tourne sur le WAE inspecte la MIB
3) Lorsque le device agent a trouvé l'information demandée, celle-ci est envoyée via SNMP au superviseur.

WAAS supporte les versions SNMP suivantes :

- Version 1 (SNMPv1)
- Version 2 (SNMPv2c)
- Version 3 (SNMPv3)

Les informations suivantes sont disponibles via SNMP :

- Statut du système pour chaque File Engine (CPU, Disk, Memory)
- Statut du service WAAS (Uptime, Version, License Status)
- Sur le WAE Edge :
    - Etat de la connexion avec le(s) WAE Core et statistiques de connexions
    - Statut du cache
    - Statistiques relatives au service CIFS
- Sur le WAE Core
    - Etat de la connexion avec le(s) WAE Edge et statistiques de connexions
    - Etat des connexions aux serveurs de fichiers CIFS et NFS

Les MIBS suivantes sont supportées sur les équipements WAAS v4 :

- ACTONA-ACTASTOR-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-CONTENT-ENGINE-MIB
- CISCO-ENTITY-ASSET-MIB
- ENTITY-MIB
- EVENT-MIB
- HOST-RESOURCES-MIB
- MIB-II

Elles sont téléchargeables sur ftp://ftp.cisco.com/pub/mibs/v2

Siège social Mondial
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France
Cisco Systems France
11 rue Camilles Desmoulins
92782 Issy Les Moulineaux
Cédex 9
France
www.cisco.fr
Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912
www.cisco.com
Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :

www.cisco.com/go/offices

Afrique du Sud • Allemagne • Arabie saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Colombie • Corée Costa Rica • Croatie • Danemark • Dubaï, Emirats arabes unis • Ecosse • Espagne • Etats-Unis • Finlande • France • Grèce • Hong Kong SAR Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie • Mexique • Nouvelle Zélande • Norvège • Pays-Bas Pérou • Philippines •Pologne • Portugal • Porto Rico • République tchèque • Roumanie • Royaume-Uni • République populaire de Chine Russie • Singapour • Slovaquie •Slovénie • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe

01/07