



Présentation à l'OSSIR

14 Sept. 2010

Frederic Benichou,
Damien Chastrette,

directeur Europe du Sud
directeur technique

Agenda

- Zscaler: société
- Défis du filtrage Web
 - Réponse Cloud / mode SaaS
- Briques technologiques et Architecture Cloud Zscaler
 - Distribuée et Multi-tenant
- Fonctionnalités
 - Sécurité
 - Contrôle d'usage
 - DLP
 - Reporting et analyse de logs

Zscaler, la société

Focus Unique

- Fondée en 2007 dans la Silicon Valley. Equipe de très forte expérience
- Focus unique: Services de Sécurité “in-the-Cloud”

Services Intégrés

- Services intégrés web et email “security-as-a-service (SaaS)”
- Permet d’éliminer les produits ponctuels et de réduire les coûts

Technologies Revolutionnaire

- Conçu pour le SaaS – *pas une techno standard dans des data centers*
- Architecture *multi-tenant*; latence quasi-zero, support des nomades

Clients

- Protège plus d’1 million d’utilisateurs depuis 140 pays
- Plus de 300 entreprises, dont des noms prestigieux et Fortune 500
- Le plus grand client: 300,000 utilisateurs

Couverture Globale

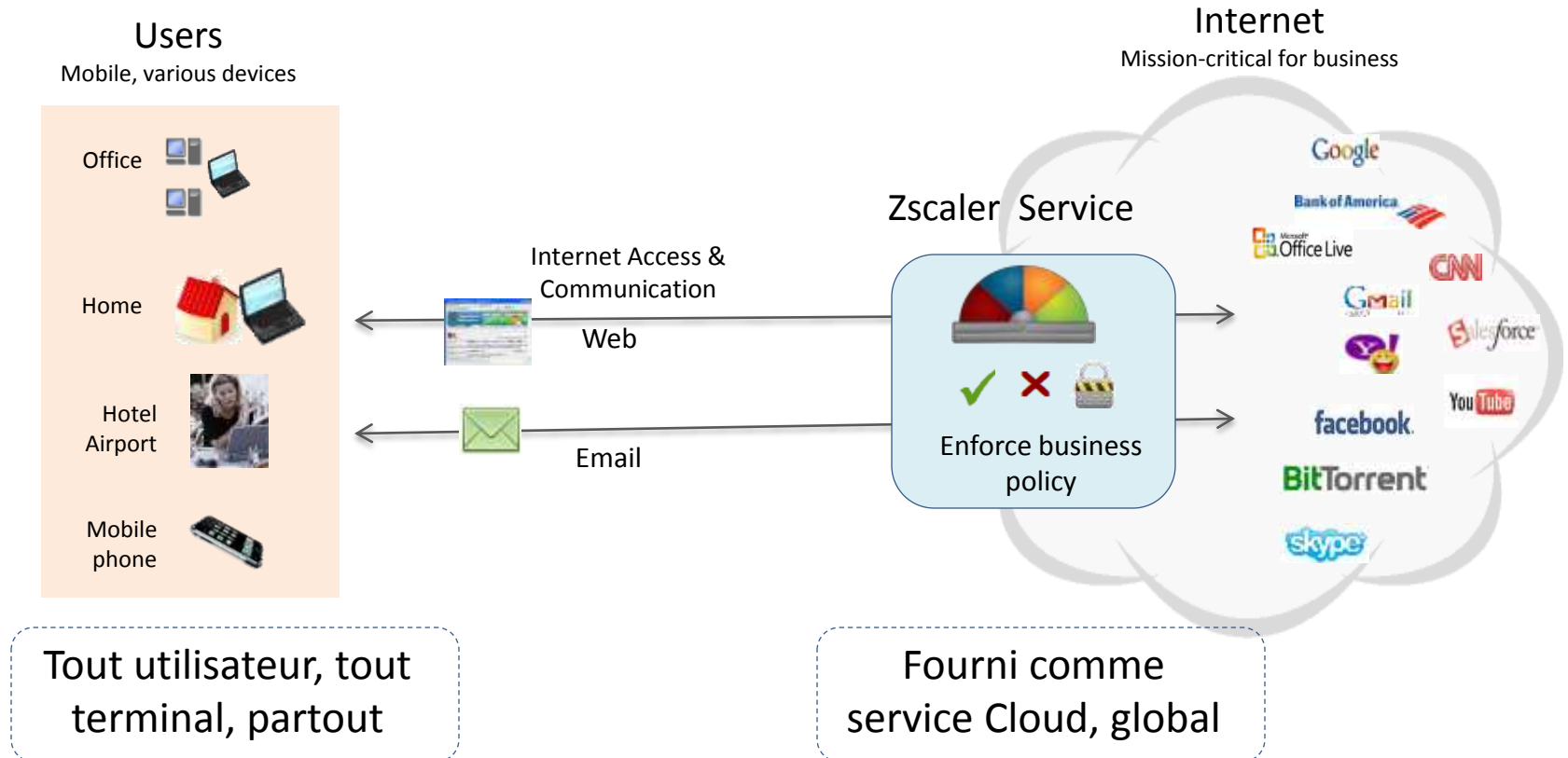
- Equipes commerciales et support dans 15 pays
- Réseau global – plus de 40 data centers dans le monde

Reconnaissance



Zscaler: Sécurité Cloud pour Web et Email

Permet d'imposer des politiques de sécurité et de contrôle d'usage pour l'accès à Internet (Web et Email)



Pas de hardware, pas de software! Pas d'investissement initial;
Déploiement facile

- Equipe de recherche en Sécurité
 - 9 personnes – en Californie et en Inde
 - Sous la direction de Michael Sutton, expert reconnu de l'industrie
- Voir blog de sécurité: <http://research.zscaler.com>
- Exemples de protection « zero-day »:
<http://www.zscaler.com/security-advisories.html>
- Partenariat avec une douzaine de sociétés de sécurité pour les feeds en temps réel et échange d'informations de vulnérabilité, notamment Microsoft (programme MAPPS)

Quelques références dans le monde

Trusted By The World's
Most Respected Companies



German Insurance



French Fashion



French Finance



US Beverages



UK/AU Media



Japanese Automotive



US Healthcare



Indian Services

Awarded & Recognized By The
World's Most Respected Analysts



Most Visionary



Zscaler dans l'analyse Magic Quadrant de Gartner

Zscaler: jugé comme le plus "Visionnaire" dans l'analyse MQ de Jan. 2010 sur les "SWG" ("Secure Web Gateways")

<http://www.gartner.com/technology/media-products/reprints/zscaler/172783.html>



"All reports are based on live data and allow drill down into detailed log."

"The policy manager is very easy to use follows roaming users, allows service at the nearest node."

"[Zscaler] offering already has the largest global footprint of data centers."

"Zscaler is a very strong choice for any organization interested in a Secure Web Gateway."

Source: Gartner

Défis des entreprises liés aux flux Web

Défis du Web 2.0: Sécurité, Contrôle, et Visibilité / reporting

Menaces de Sécurité



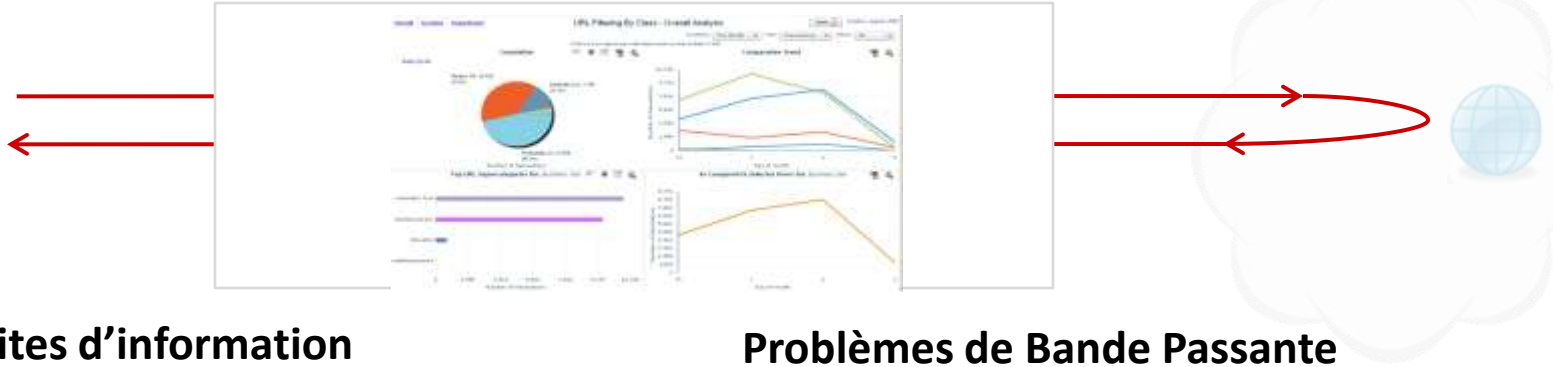
Anti-virus et catégorisation malware limités

Contrôle des usages / prévention des abus

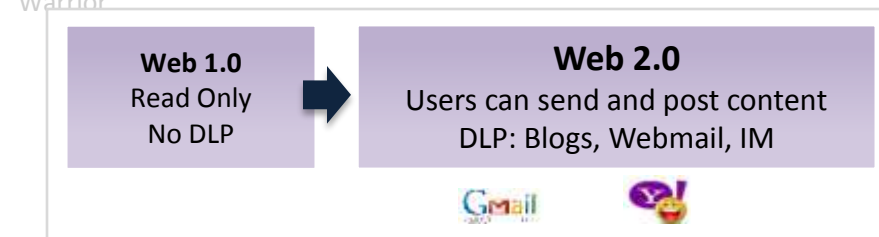


Filtrage d'URL traditionnel atteint ses limites avec le Web 2.0

Visibilité/ Reporting / Analyse consolidée des logs

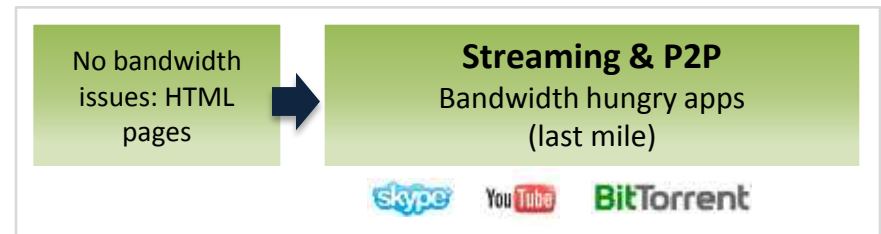


Fuites d'information



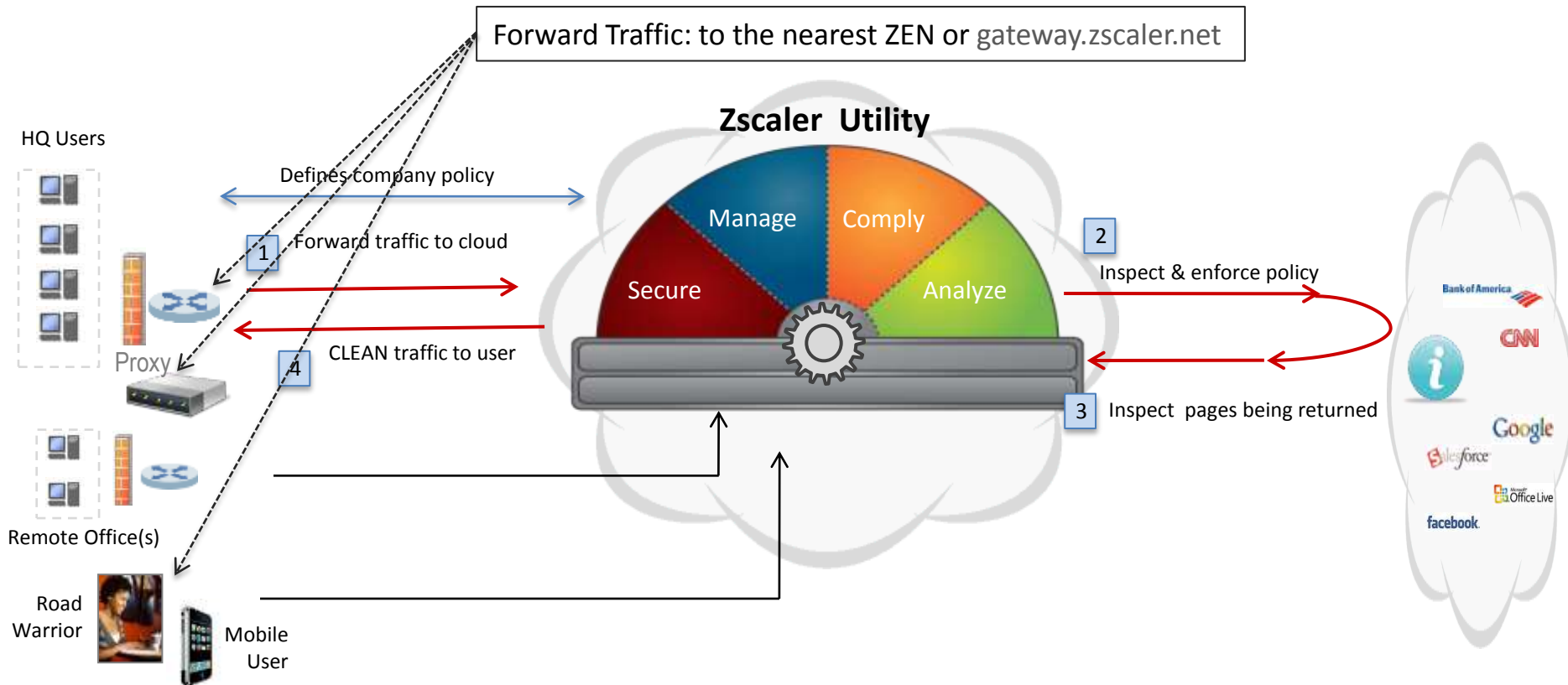
Un risque réel pour l'entreprise

Problèmes de Bande Passante



Besoin de prioriser les flux Web (ex. streaming vs. pro.)

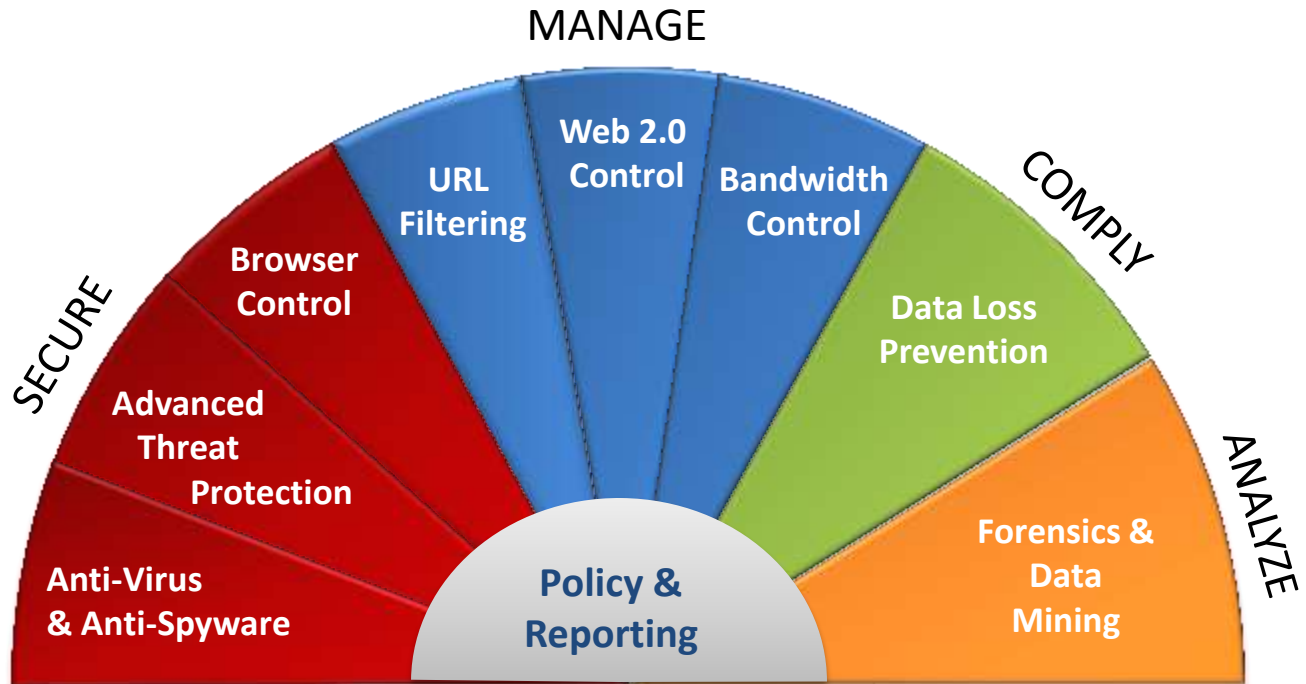
Comment le système Cloud Zscaler fonctionne







- 2 grands sujets techniques pour le déploiement:
 - Traffic Forwarding
 - Authentification des utilisateurs

Fonctionnalités Zscaler





Cloud Web Services



Technologies

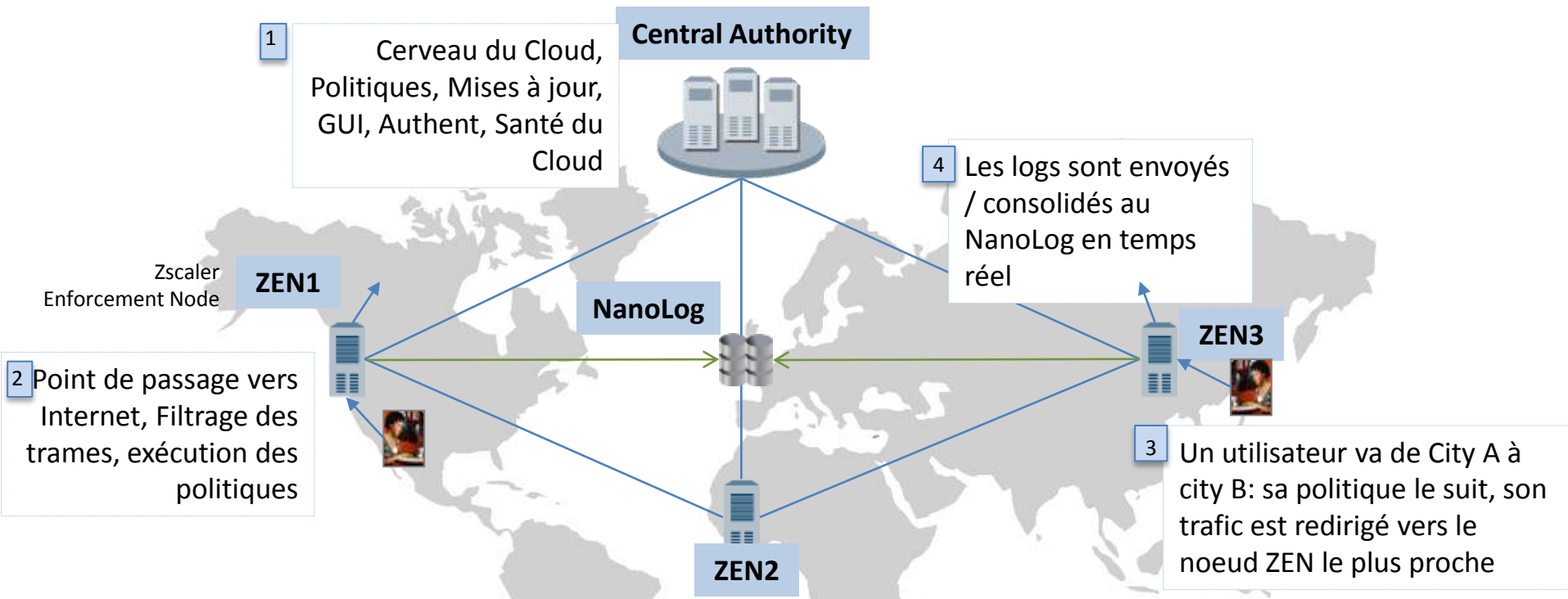
10 GBPS Proxy 	ShadowPolicy™ 	NanoLog™ 	Transparent Authentication 
--	--	---	---

Infrastructure

40+ Data Centers Worldwide 	High Reliability and Availability 99.99% 	Near-Zero Latency < 10MS 	Privacy and Data Security 
--	--	--	---

Cloud Security Multi-tenant Architecture

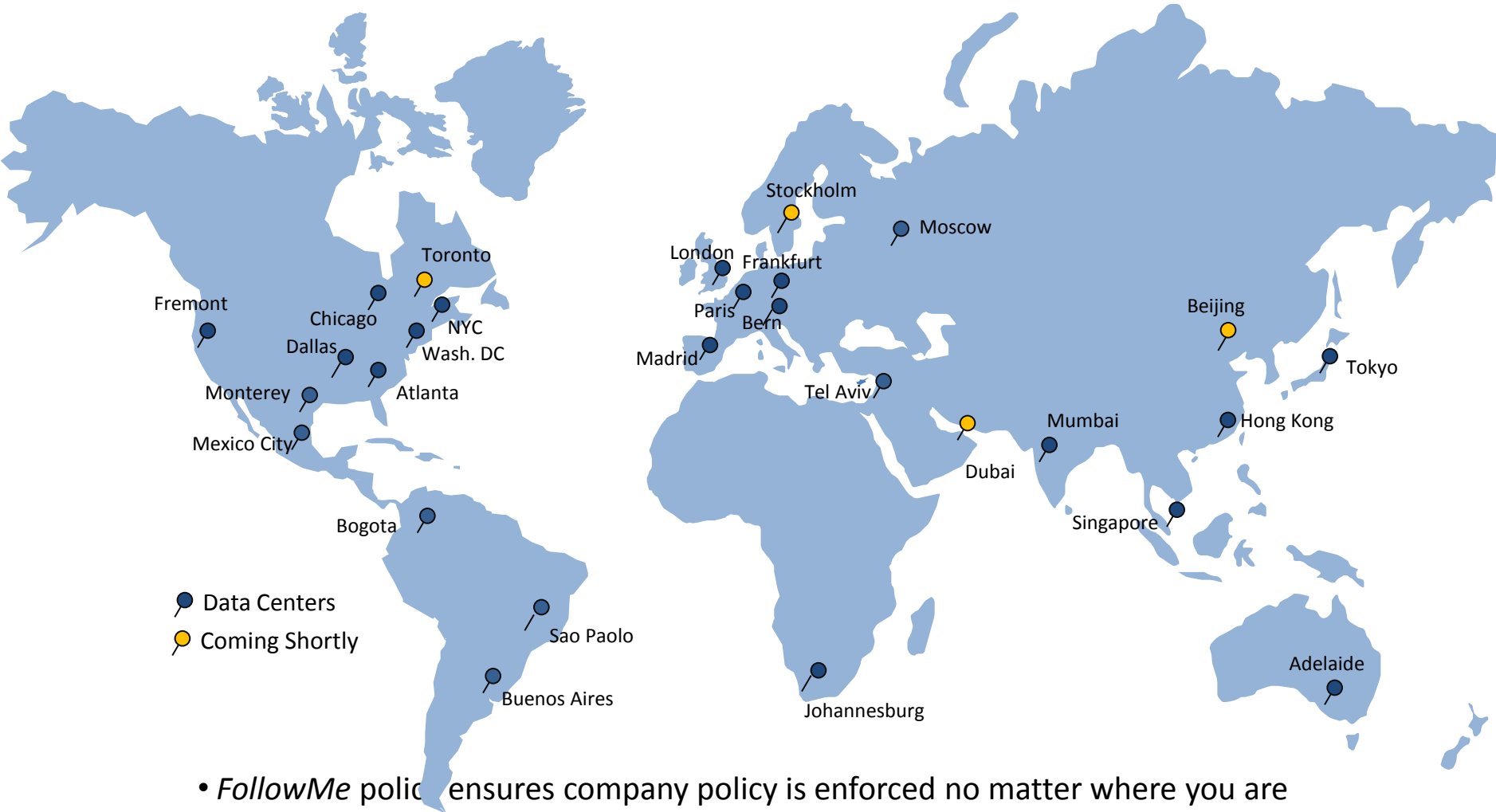
Zscaler Architecture: Multi-tenant, Distribuée



- Multi-tenant : les utilisateurs ne sont pas attachés à un data center en particulier
- Multiples bureaux, nomades et mobiles
- “*FollowMe Policy*”: la politique d’un utilisateur le suit et s’applique à lui partout et toujours
- Mise à jour immédiate de tous les ZENs face à une menace ou pour une politique.
- Technologie “NanoLog”: Logs consolidés et corrélés en temps réel, interrogeables en qq. Sec.

Temps de réponse rapides, et Haute Disponibilité

Le Cloud le plus global: environ 40 Data Centers

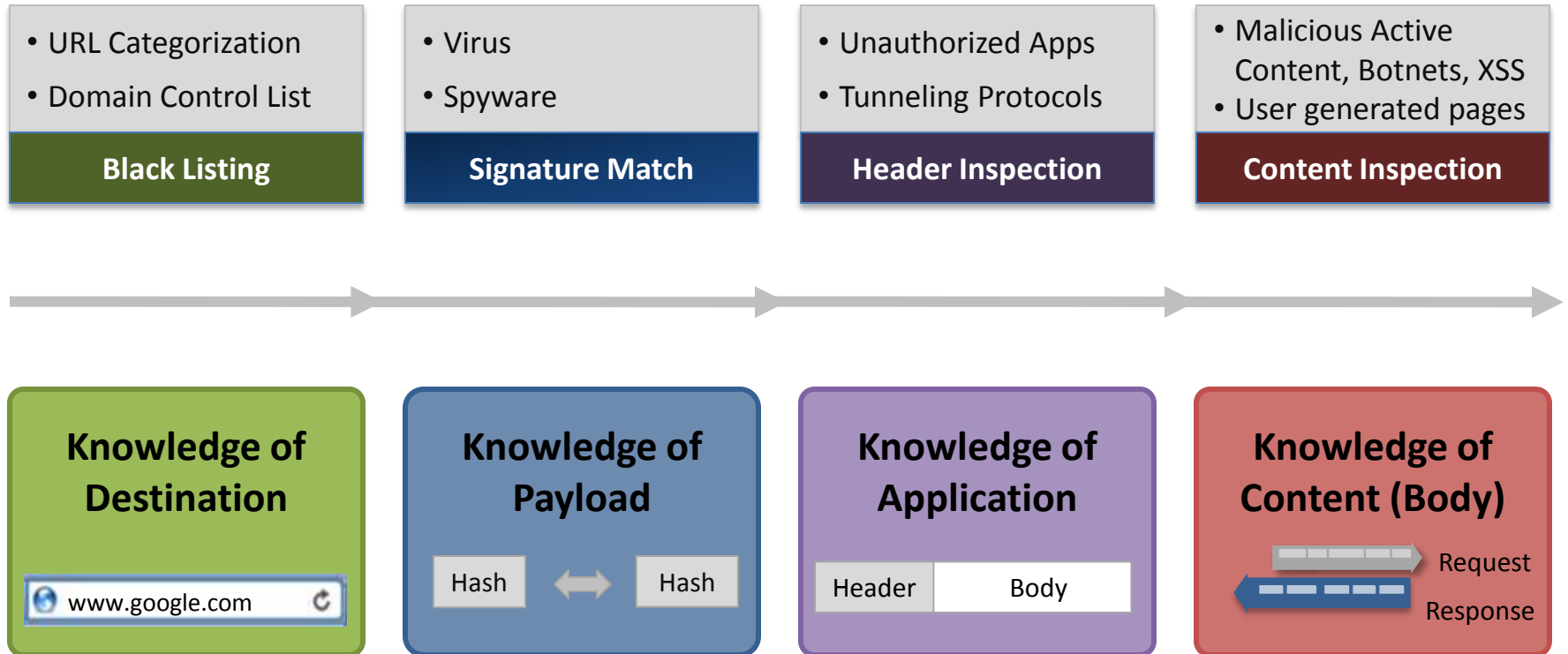


- *FollowMe* policy ensures company policy is enforced no matter where you are

Benefits: 1. Near-zero latency; 2. High reliability; 3. BW savings (no backhauling)

Fonctionnalités: Sécurité

Why Traditional Technologies No Longer Work



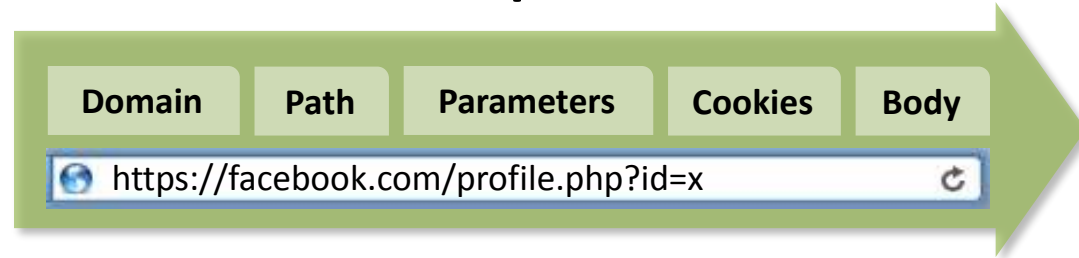
Full Content (page) inspection is required to detect today's threats

“AV signatures or URL filtering is obsolete for newer threats. High-speed scanning of content/pages is needed.” -- Gartner

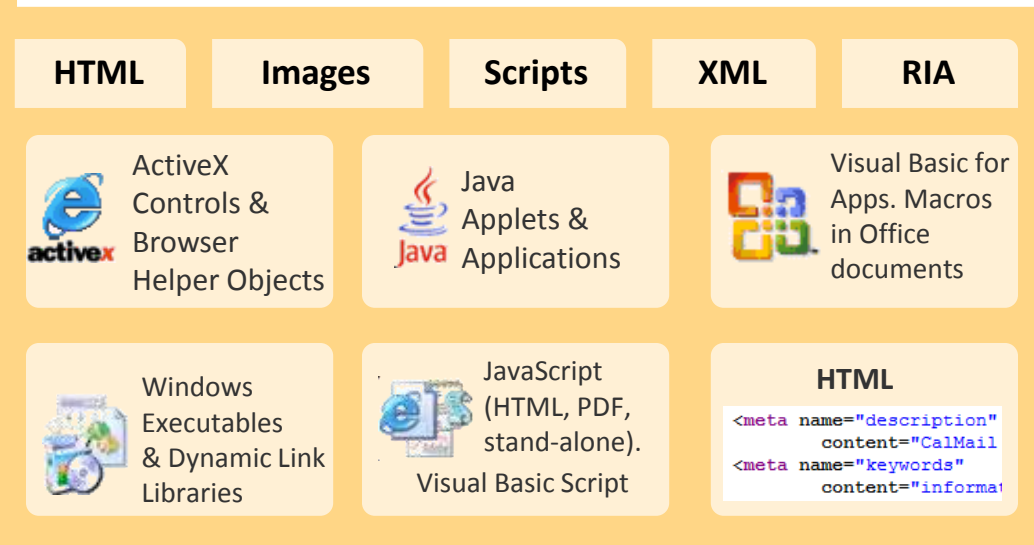
Zscaler Inspects Full Request & Response

- Most vendors analyze only domain and block based on a black list
- Domain represents < 5% of a total URL
- URL represents < 1% of a total page
- Most newer threats are hidden in the pages being served and require full page inspection

Request

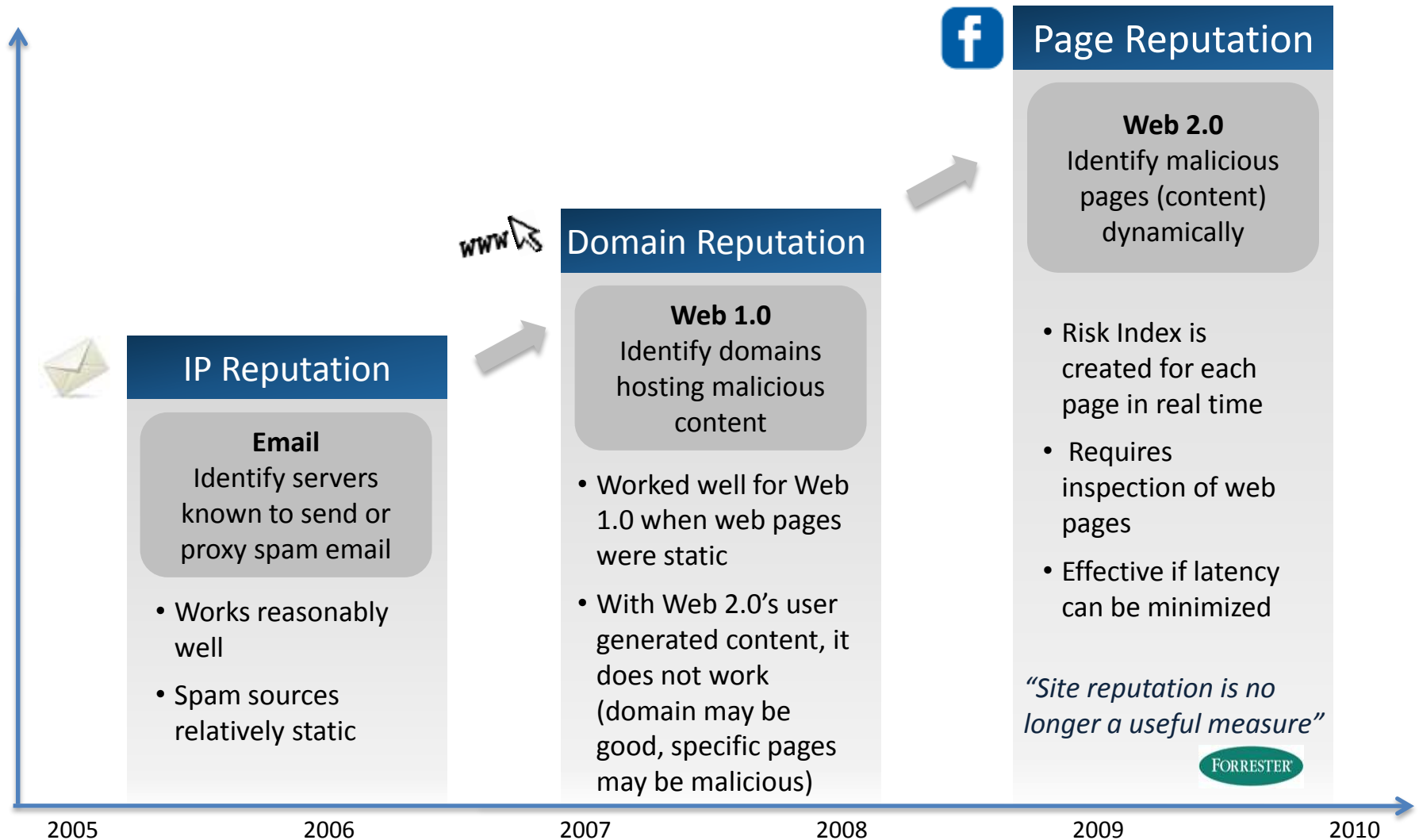


Response



Analysis of Request/Response is critical but can introduce latency

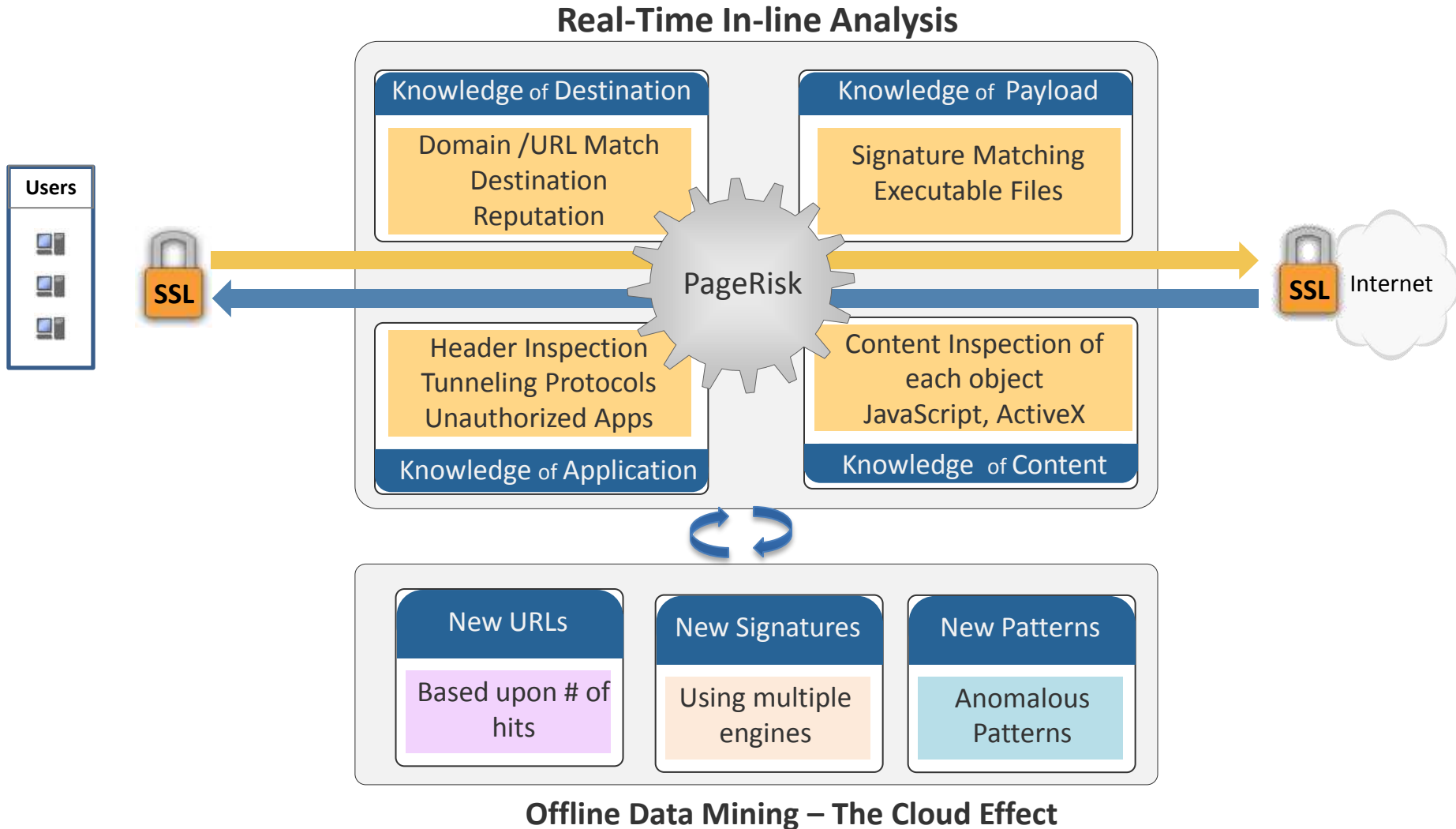
Traditional Reputation Score Ineffective for Web 2.0



Integrated & Comprehensive Threat Detection



Zscaler uses dynamic PageRisk to detect threats accurately



Zscaler: Comprehensive Detection Technologies

Zscaler Security Technologies

Data Mining

- Network effect
- Identify emerging threats

Offline Scans

- Multiple Engines
- Continual Scans
- URL DB updates

URL Database

- Continuously updated
- Proprietary

Pattern Match

- Custom signatures
- Real time
- High speed

Malicious Content

- Real time, in-line detection



Malicious URLs

- Feed #1
- Feed #2

Phishing

- Feed #3
- Feed #4

Botnets

- Feed #5
- Feed #6

AV Signatures

- Inline - Feed #7
- Offline - Feed 8 & 9

Vulnerabilities

- Feed #10
- Feed #11
- Feed #12

Third-Party Technologies

Combination of internal research & best external feeds results in the best threat detection

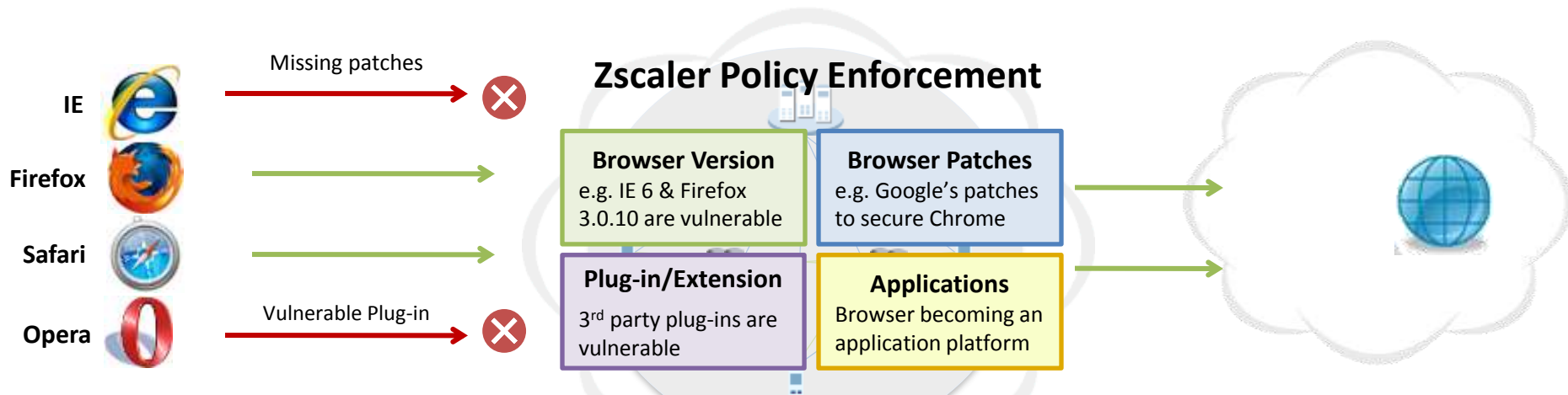
Browser Control



Challenge: Hackers are exploiting browsers to infect users' computer. Older and unpatched browsers are vulnerable.

“ There are more browser capabilities to be exploited, more potential for vulnerabilities. ” **Gartner**

Solution: Enforce browser policy: browser versions, patches, plug-ins & applications



- Configurable scans frequently (daily, weekly, monthly, etc)
- Warn if outdated or vulnerable
- No client-side software or download required

Benefit: Reduce security risk with least effort (centrally configured)

Fonctionnalités: Manage



Challenge:

“ URL Filtering is mostly reactionary. It has a fundamental flaw to be an effective security filter; it does not monitor threats in real time.

” **Gartner**

“ Internet bound traffic should be inspected for more than URL filtering. Web 2.0 applications require granular policies for control.

” **FORRESTER**

Solution: Granular control of Web 2.0 applications. Policies by location, user, group, location, time of day, quota

URL Filtering

- URL DB, multiple languages
- Enforcement by URL, not domain, Safe Search
- Real-time Dynamic Content Classification
- 6 classes, 30 super categories, 90 categories

Enforce traditional URL policies at low TCO

Web 2.0 Control

- Action-level control for Social sites, Streaming, Webmail & IM
- Allow viewing but block publishing
- Allow webmail but not file attachments

Enable use of Web 2.0 with right access to right users

Bandwidth Control

- 40 – 50% of BW is consumed by streaming
- Enforce policies by type of web application
- Ensure enough BW to mission critical apps

Tangible savings due to proper use of BW (last mile)

Right access to right resources to empower users and optimize resource use

Manage - Managed Access to Web 2.0



Challenge:

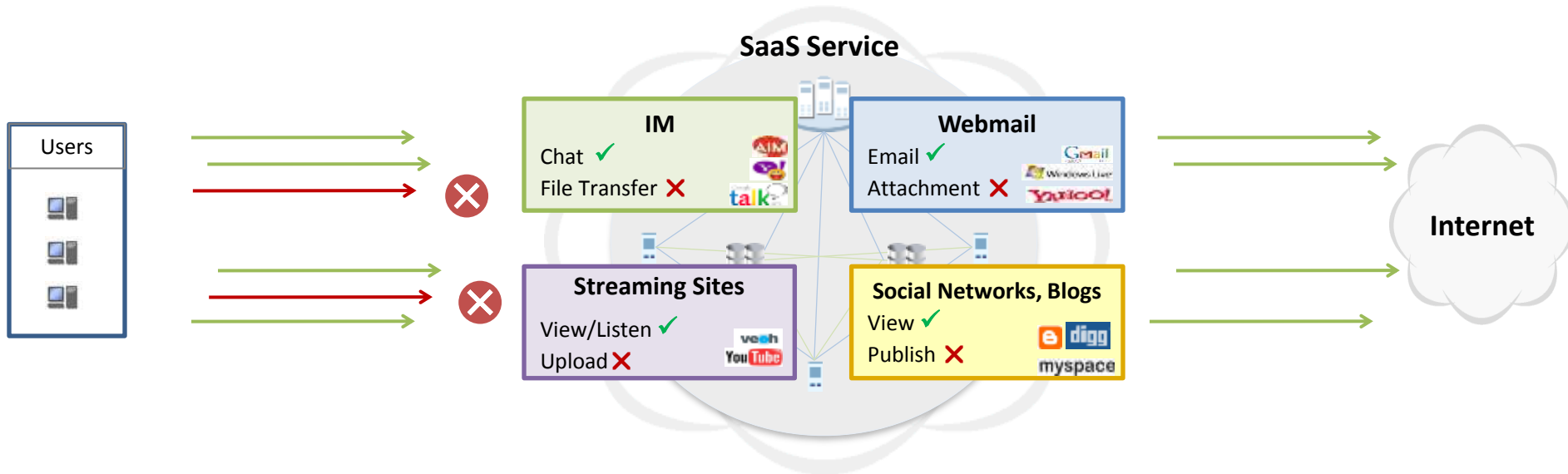
“ The advances in Web 2.0 technologies require a new generation of Web security tools that go well beyond traditional URL filtering. ”



“ Discerning one app from another is far from just a URL recognition game ”



Solution: Managed access - Granular policies by action, location, group, etc.



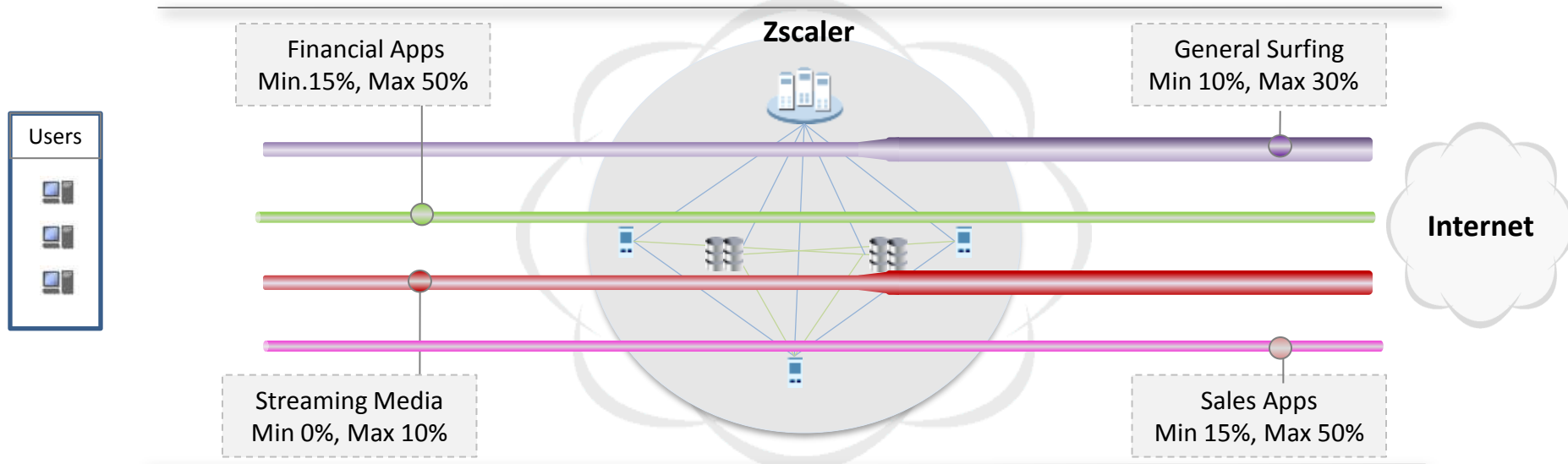
Benefits: Provide right access to right users

Manage - Policy-based Bandwidth Control



Challenge: 40% - 50% of bandwidth is consumed by streaming applications

Solution: Bandwidth allocation by application type



Benefits: Right applications get the right bandwidth; cost saving



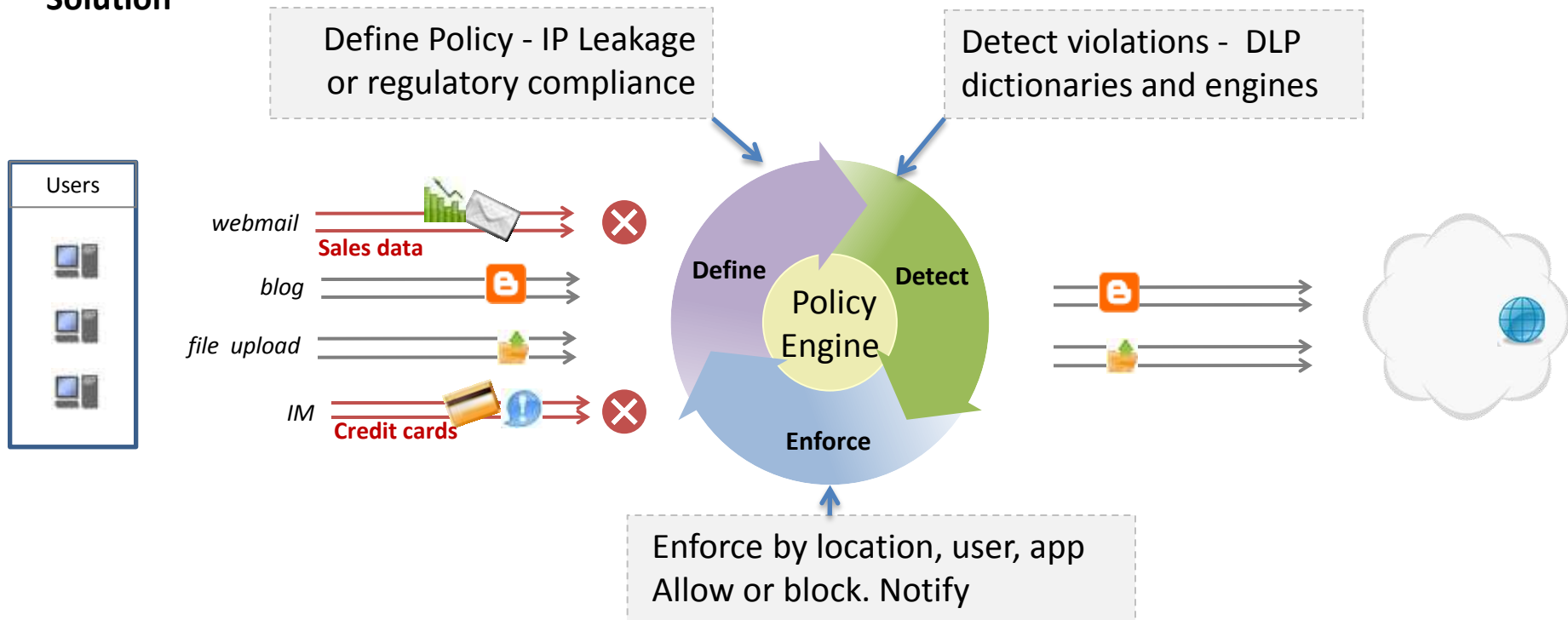
Fonctionnalités: Data Leakage Prevention

Comply - Data Leakage Prevention (DLP)

Challenge

Social networks, Blogs, Webmail/IM are easily accessible from any browser and are dangerous backdoors. May lead to accidental or intentional leakage of proprietary and private information.

Solution



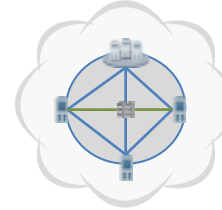
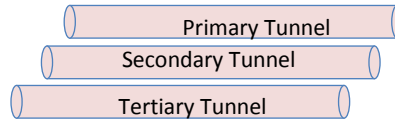
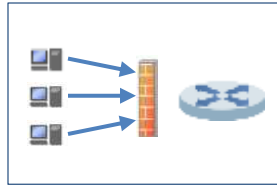
Benefits

Rapid deployment. Highly accurate, Ultra-low latency, Complete inline inspection (not a tap node)

Fonctionnalités: Reporting & log analysis

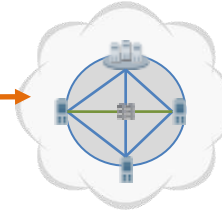
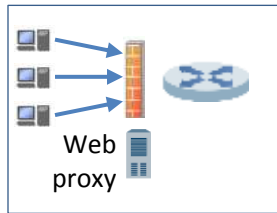
Multiple and Easy Traffic Forwarding Options

GRE Tunneling



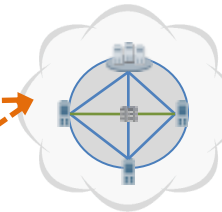
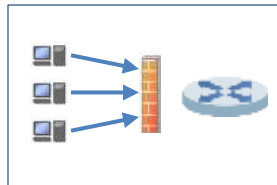
Create a GRE tunnel to forward Port 80/443 traffic our SaaS Service

Forward Proxy Chaining



Forward port 80/443 traffic from Squid, ISA, Bluecoat, etc.

Proxy / PAC File



PAC File/Explicit Browser to SaaS Service
Browser based PAC file or explicit proxy setting support Road Warriors

No device needed on customer premise, no software to deploy.
Simply forward the traffic from each location to Zscaler

Questions / Réponses

damien@zscaler.com
fbenichou@zscaler.com