



Les pare-feu nuisent-ils à la sécurité ?

Quelques considérations autour du concept de
déprimétrisation

Cédric BLANCHER

`cedric.blancher@eads.net`
EADS Innovation Works
Computer Security Research Lab

`sid@rstack.org`
Rstack Team
<http://sid.rstack.org/>

Séminaire Aristote - La sécurité distribuée
École Polytechnique Palaiseau - 11 juin 2009



La dépérimétrisation en quelques mots...

Tendance à l'ouverture des réseaux

- Ouverture des périmètres
- Suppression (ou presque) des firewalls
- Concentration sur la sécurité des données

Discours volontairement polémique, mais néanmoins intéressante



Agenda

- 1 La déperimétrisation
- 2 Différents points de vue
- 3 Conclusion



Agenda

- 1 La déperimétrisation
- 2 Différents points de vue
- 3 Conclusion

Jericho Forum



THE *Open* GROUP
Making standards work®

HOME | SITE MAP | SEARCH

Sponsor an Event | Become a Member | Member Area

About | **Forums** | Certification | Services | Government | Events | Bookstore & Downloads | Newsroom | Contact

You are here: [Home](#) > [Forums](#)

Forums

- Architecture
- Enterprise Management
- Identity Management
- Platform
- Real-Time & Embedded Systems
- Security

Customer Council

What Forums are...

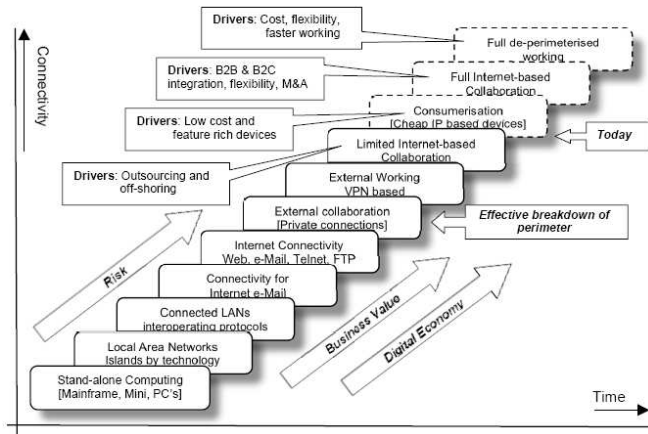
The Open Group is largely a federation of semi-autonomous forums that confront major barriers to enterprise integration, and enable their members to guide development and adoption of industry directives and standards. Covering a range of technical, business, legal and regulatory issues, each forum addresses a specific functional area, and provides a neutral platform to meet others with similar issues and work together on best practices. Each Forum is lead by a Forum Director, a specialist with thorough knowledge of their subject, and access to the vendor and user community.

Think Tank poussant la déperimétrisation

- Les 11 commandements
- Business Case for Deperimeterisation
- Nombreux White Papers
- Présentations et exemples



Arguments (1)



Arguments (2)

Grosso modo

- Les mécanismes de sécurité réseau sont obsolètes
- Ils ne protègent pas de la plupart des attaques
- Ils sont contre-productifs
- Ils encouragent des comportements "incidentogènes"

Arguments (2)

Grosso modo

- Les mécanismes de sécurité réseau sont obsolètes
- Ils ne protègent pas de la plupart des attaques
- Ils sont contre-productifs
- Ils encouragent des comportements "incidentogènes"

Solution

- Redonner au réseau son rôle de transport
- Rétablir la connectivité globale
- Remonter la sécurité vers les applications



Utopie ?

Une jolie collection de Yakafokons™© qui soulèvent plus de questions qu'ils n'apportent de réponses

- Faisabilité technique ?
- Ampleur des bénéfices ?
- Portée réelle du concept ?
- Applicabilité pratique ?
- Conditions, contraintes, limites, risques ?
- Etc.



Agenda

- 1 La déperimétrisation
- 2 Différents points de vue
- 3 Conclusion



Point de vue du réseau (1)

Migration vers un réseau plus plat

- Moins de firewalls
- Plus de connectivité (cf. modèle IPv6)
- Sécurité de bout en bout



Point de vue du réseau (1)

Migration vers un réseau plus plat

- Moins de firewalls
- Plus de connectivité (cf. modèle IPv6)
- Sécurité de bout en bout

Principe

- Chiffrement des flux applicatifs (SSL/TLS)
- Recentrage de la sécurité sur les données



Point de vue du réseau (2)

La segmentation du réseau est un problème

- Problèmes de NAT
- Configuration des pare-feu
- Mécanismes compliqués (cf. P2P)

Point de vue du réseau (2)

La segmentation du réseau est un problème

- Problèmes de NAT
- Configuration des pare-feu
- Mécanismes compliqués (cf. P2P)

Apports de la connectivité globale

- Véritable sécurité de bout en bout
- Intégration de la mobilité
- Constitution d'overlays
- Etc.

Repérimétrisation

On ne supprime pas le périmètre, on le reconstruit...

- Périmètre plus ouvert physiquement
- Mais construction de domaines logiques
- Communication au sein de ces nouveaux périmètres

La dépérimétrisation transforme le périmètre physique en périmètre logique par la mise en place d'overlays



Point de vue système...

Axée connectivité, la déperimétrisation apporte peu au système...

- Mêmes moyens de sécurité
- Menaces client-side exacerbées
- Problématiques de confinement

Point de vue système...

Axée connectivité, la déperimétrisation apporte peu au système...

- Mêmes moyens de sécurité
- Menaces client-side exacerbées
- Problématiques de confinement

Questions...

- Gestion de l'exposition des systèmes ?
- Assurance de la résilience ?
- Confinement par rapport au reste du périmètre ?



L'accès aux données

Problématique strictement identique

- Mêmes services
- Mêmes données
- Mêmes accès



L'accès aux données

Problématique strictement identique

- Mêmes services
- Mêmes données
- Mêmes accès

Problèmes

- Exposition accrue des clients
- Adaptation des applications



La dépérimétrisation pour tous ?

L'éclatement du périmètre ne veut pas dire mort du firewall

- Concept poussé par les besoins de mobilité
- Aucun intérêt pour les ressources fixes



La dépérimétrisation pour tous ?

L'éclatement du périmètre ne veut pas dire mort du firewall

- Concept poussé par les besoins de mobilité
- Aucun intérêt pour les ressources fixes

Mais aussi...

Votre dépérimétrisation profitera d'abord aux autres !



Agenda

- 1 La déperimétrisation
- 2 Différents points de vue
- 3 Conclusion**



L'accès aux données

Le fond du problème réside dans la gestion des données

- La valeur réside dans les données
- Comment protéger efficacement les données ?

L'accès aux données

Le fond du problème réside dans la gestion des données

- La valeur réside dans les données
- Comment protéger efficacement les données ?

Problématiques

- De nombreuses données ne transitent pas sur le réseau !
- Distribution des données (e.g. Cloud Computing)



Une solution ?

La déperimétrisation c'est peut-être sexy, mais...

- Comment gérer l'explosion des clients avec des moyens dépassés
- Comment gérer la protection des données dans ces conditions
- Quelle est la résilience d'un tel réseau face à un hôte compromis ?
- Impact des moyens de crypto sur l'infrastructure (charge, monitoring)



Une solution ?

La déperimétrisation c'est peut-être sexy, mais...

- Comment gérer l'explosion des clients avec des moyens dépassés
- Comment gérer la protection des données dans ces conditions
- Quelle est la résilience d'un tel réseau face à un hôte compromis ?
- Impact des moyens de crypto sur l'infrastructure (charge, monitoring)

Oui mais...

- Probablement la solution à l'expansion du Net
- Beaucoup de travail en perspective



That's all folks !

Merci pour votre patience...

Questions ?