Les firewalls ne sont pas morts

Protection des nouvelles frontières de l'entreprise

JSSI de l'OSSIR

10 mai 2005

Hervé Schauer

<Herve.Schauer@hsc.fr>

Plan

- Pourquoi les *firewalls* ?
- Du *firewall* au périmètre
- Pourquoi le périmètre
- En quoi consiste le périmètre ?
- En quoi consiste le contrôle d'accès ?
- HTTP/HTTPS
- HTTPS
- Télémaintenances
- Mobilité et nomadisme
- Internet et telecom
- Voix sur IP / Téléphonie sur IP
- Au delà du périmètre
- Firewall en plusieurs boîtes ou tout en un ?
- Conclusion
- Prochains rendez-vous

Les transparents sont disponibles sur `www.hsc.fr`

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Pourquoi les firewalls ?

- Pourquoi avons-nous eu besoin de firewalls ?
  - Parce que le réseau où tout le monde communique avec tout le monde a vite atteint ses limites avec Internet : intrusions, code malveillant, etc
  - Pour faire du contrôle d'accès en entrée de son réseau
  - Pour appliquer sa politique de sécurité sur ce point d'entrée
  - Pour ne faire de la sécurité que dans les firewalls en entrée de son réseau et pas trop ailleurs
- Pourquoi ne pouvait-on pas appliquer la sécurité partout ?
  - IPsec de bout en bout partout ? Car le bout je ne lui fait pas confiance, c'est le firewall entre les deux que je maîtrise
  - Compromis et réalisme

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Du *firewall* au périmètre

- A l'origine, le *firewall* est entre son réseau interne et l'internet
  - Sur ce qui s'est appellé le **périmètre**
- Actuellement il y a des firewalls partout
- S'il faut appliquer le concept du *firewall* sur chaque PC, est-ce que la notion de *firewall* est encore réaliste ?
- Est-ce que la notion de périmètre est dépassée ?
- Les réseaux sont tellement poreux et contournés que celà n'a plus de sens ?

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Pourquoi le périmètre ?

- Schématiquement il y a :
- Un espace dont le directeur est responsable :
  - Le système d'information (SI) de son organisme
- Un espace dont le directeur n'est plus responsable :
  - Le reste du monde
- Entre le système d'information de son organisme et le reste du monde : le **périmètre** du SI
- Il faut bien distinguer où s'arrête et où commence la responsabilité
- Il faut protéger l'espace sur lequel le directeur est responsable

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Pourquoi le périmètre ?

- La politique de sécurité s'applique sur l'ensemble du SI
- Cependant :
  - L'application la plus simple et globale d'une politique de sécurité est d'abord par du contrôle d'accès dans le réseau
  - Le contrôle d'accès dans le réseau est efficace et réaliste en étant appliqué en priorité sur le périmètre
    - Là où sont et seront les firewalls et là où ils sont poreux et contournés
- "La menace vient de l'intérieur", mais quand même surtout de l'extérieur
  - Les employés malveillants utilisent leur connaissent pour tenter leur actions de l'extérieur
  - Dénis de service
  - ...

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

En quoi consiste le périmètre

- Savoir où commence et où s'arrête son espace de responsabilité
  - Les responsables ne savent pas toujours qu'ils sont responsables
  - *Joint-venture*, GIE, structures à 50/50, sous-traitants, infrastructures infogérées, contrats inadaptés , etc
- Savoir où commence et où s'arrête son système d'information
  - Réseaux sans fil
  - Stockages amovibles
  - Télémaintenances
  - Infogérances
  - Nomades

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

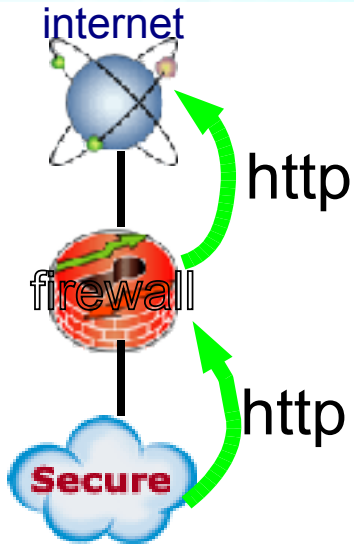
En quoi consiste le contrôle d'accès

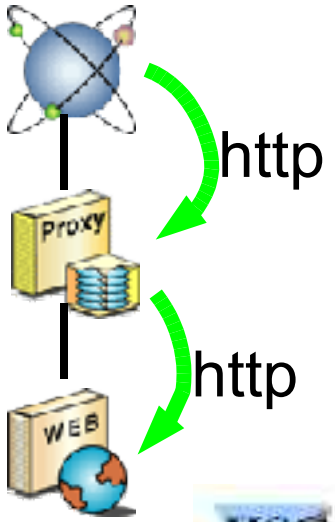
- Etre capable de dire sur chaque paquet qui entre ou qui sort s'il peut entrer ou sortir
- Ne pas permettre les codes malveillants
- Ne pas permettre les canaux cachés
  - Encapsulations dans HTTPS
- Faire la même chose sur tous les protocoles de transport
  - IP, HTTP, SIP, XML, SS7, etc

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

HTTP/HTTPS

- Laisser ouvert HTTPS sur Internet revient à connecter son réseau privé sur Internet sans *firewall*
- Il faut analyser le contenu de HTTP et d'HTTPS
- Rechercher les protocoles re-encapsulés interdits
- Analyser tous les contenus pour y détecter ceux qui sont malveillants ou ne répondent pas à sa politique de sécurité
- Appliquer le même filtrage dans HTTP que celui que nous réalisions sur TCP/IP dans les années 1990
  - Dans les deux sens

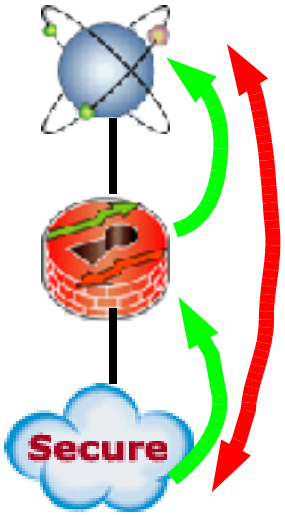




Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

HTTP/HTTPS

- Exemple de logiciels cherchant à contourner le contrôle d'accès du firewall :
  - Microsoft avec RPC over HTTPS, Outlook 2003, etc
  - VPN-SSL, ssltunnel, stunnel, http-tunnel, etc
  - Courrielweb (Webmail)
  - Logiciels d'EDI avec XML qui remettent du MIME et des protocoles de RPC dans HTTP/HTML,
  - Logiciels de messagerie instantanée
  - Logiciel de partage d'agenda et de messagerie
  - Logiciels basés sur les Web Services
  - Logiciels poste à poste (P2P:Peer-toPeer)



Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

HTTP/HTTPS

- Filtrer les logiciels de contournement de firewall institutionalisés
  - Messageries universelles qui renvoient la messagerie d'entreprise à l'extérieur sans serveur central dans votre SI
    - Ipracom, Blackberry
  - Logiciel de prise de contrôle à distance
    - WebEx
  - Téléphonie propriétaire
    - Skype
- Filtrer les logiciels malveillants qui sont passés à l'intérieur et qui recherchent la sortie vers l'extérieur
  - *Spywares*, *keyloggers*, etc

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

HTTP/HTTPS

- La majorité des logiciels pilotent Internet Explorer
  - Il faut à la fois un *firewall* HTTP/HTTPS sur le périmètre et un *firewall* personnel sur chaque poste qui sachent travailler de concert
- Journaliser le trafic
  - Y comprit le nombre d'octets transmis et les valeurs du champ `Content-Length`
- Détecter les anomalies et les valider / invalider
  - Beaucoup de trafic sortant
  - Site unique, URL unique
- HTTPS : autoriser les sites dans une liste blanche
  - Compromis à faire...

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

HTTP/HTTPS

- Exemple de requêtes HTTP POST et GET avec RTSP

```
POST /SmpDsBhgRl HTTP/1.0
Accept: application/x-rtsp-tunnelled, */*
Content-type: application/x-pncmd
Content-length: 32767
```

HTTP POST Request

```
3fe06463-55b0-448d-be04-120bd3cb7a1f
1BUSU9OUyBydHNwOi8vcm[...]
```

HTTP POST Request body : Base64 encoded RTSP Control channel

```
GET /SmpDsBhgRl3fe06463-55b0-448d-be04-120bd3cb7a1f HTTP/1.0
Accept: application/x-rtsp-tunnelled, */*
ClientID: WinNT_5.0_6.0.10.505_play32_RN9GPD_en-US_686_axembed
X-Actual-URL: rtsp://realserver.domain.tld/videos/20d05122002.rm
```

HTTP GET Request

```
HTTP/1.0 200 OK
Server: RMServer 1.0
Content-type: audio/x-pn-realaudio
Content-length: 2147483000
```

```
RTSP/1.0 200 OK
CSeq: 1
Date: Mon, 06 Dec 1999 08:13:01 GMT
Server: RealServer Version 6.1.3.946 (sunos-5.6-sparc)
Public: OPTIONS, DESCRIBE, ANNOUNCE, SETUP, GET_PARAMETER, SET_PARAMETER, TEARDOWN
StatsMask: 3
[...]
```

HTTP Reply body : Base64 encoded RTSP/RTP Control/Data channel

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

HTTPS

- Une forme de firewall HTTPS en sortie est possible
- Le type de trafic même chiffré peut se distinguer entre un usage web normal en HTTPS et un tunnel VPN-SSL
  - Tunnel SSL = une session SSL et une connexion TCP
  - Accès web en HTTPS = une session SSL et plusieurs connexions TCP
  - Protocoles interactifs dans le tunnel SSL
  - Accès au web dans le tunnel SSL : trafic sans établissement et fermetures TCP
- TCPStatflow permet de mesurer le trafic dans chaque sens et l'uptime des sessions TCP et d'en tirer des alarmes
  - Voir la présentation "SSL VPN connection multiplexing techniques" pour plus de détails
    - **http://www.hsc.fr/ressources/presentations/upperside05-fw/**

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

HTTP/HTTPS

- Attention il n'y a pas que HTTP/HTTPS !
- DNS
  - Encapsulation ancienne mais popularisée depuis quelques années
  - Idem HTTP : filtrage, journalisation, détection
- SMTP

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Télémaintenances

- Minimiser les télémaintenances
  - Routeurs, PABX, SAN, Imprimantes, SAP, ...
- Intégrer sa politique de sécurité dès le départ dans tout processus d'infogérance et de télémaintenance
  - Contractuellement et systématiquement, ne serait-ce que pour savoir qu'il y a de la télémaintenance
- Créer un portail de contrôle d'accès
  - Indépendamment des moyens de connexion
  - Authentifier individuellement chaque télémainteneur
  - Journaliser les connexions
  - Recopier si possible la session complète des informations qui remontent à l'extérieur

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Mobilité et nomadisme

- Gérer et appliquer sa politique de sécurité sur tout ce dont se sert un employé
  - Ordinateur portable, assistant personnel, téléphone, ...
    - Une organisation, un service de support, des procédures d'alerte, un inventaire temps réel du parc connecté
    - Une authentification de l'employé et une connexion au SI par tunnel chiffré
    - Contrôle d'intégrité et mise en quarantaine avant la reconnexion au réseau d'entreprise
    - Gestion de parc centralisée exhaustive
  - Une politique de protection locale du mobile ou nomade lui-même
    - Firewall + anti-virus + anti-spyware + ... gérés de manière centralisée
    - Chiffrement des données (indispensable contre le vol)
    - Maintien à niveau des moyens de protection lorsque le nomade est à l'extérieur

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Internet et Telecom

- Les **télécommunications** et l'**Internet** ne font qu'**un**
  - Le PABX classique est un ordinateur Unix qui interroge l'annuaire d'entreprise
  - La télémaintenance par liaison téléphonique en PPP ne sert qu'à contourner le *firewall* sur les liaisons IP
    - SAN
    - Le photocopieur est un PC avec scanner/imprimante sur le réseau d'entreprise et télémaintenu par une ligne téléphonique
  - Les liaisons séries des immeubles intelligents passent aussi à IP
    - RS232 devient Telnet sans authentification
    - Les protocoles propriétaires (LonTalk, BACnet) sont ré-encapsulés sur IP
  - Voix sur IP / Téléphonie sur IP / GSM sur IP ...
    - Le PABX ou Centrex remplace toutes les strates de *firewalls* IP
- Manque d'offre de Firewalls IP et telecom

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Voix sur IP / Téléphonie sur IP

- La voix sur IP / téléphonie sur IP
  - N'est pas équivalente à la téléphonie classique
    - Signalisation/contrôle et transport de la voix sur le même réseau IP
    - Perte de la localisation géographique de l'appelant
  - Ne permet pas l'application de votre politique de sécurité
  - N'offre pas la sécurité à laquelle vous étiez habitué
  - N'est pas juste "une application en plus"
    - Faible authentification mutuelle, aucun chiffrement
      - Solutions propriétaires disponibles chez Avaya, Cisco, Ericsson
    - Risques d'interception et de routage des appels vers des numéros surfacturés
    - Falsification des messages d'affichage du numéro renvoyés à l'appelant
    - Attaques accessibles à tout informaticien et pas juste aux spécialistes de la téléphonie numérique

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Voix sur IP / Téléphonie sur IP

- Sur le périmètre : un nouveau *firewall*
  - Un PABX n'est pas un *firewall* et ceux qui ont testé pour vous ont étés victimes d'intrusions
  - Filtrage encore parfois complexe et sensible à la traduction d'adresse
- Sur le réseau privé : une architecture nouvelle
  - VLAN dédiés
  - Filtrage par adresses MAC par port
  - QoS
- Un coût d'exploitation
  - Les interfaces d'administration web des équipements de VoIP ont les failles habituelles des applications web
  - Les services comme le DNS et DHCP deviennent **critiques**
  - Rappel : le téléphone est le principal outil de sécurité des personnes

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Voix sur IP / Téléphonie sur IP

- Ne pas encore utiliser la téléphonie sur IP de manière généralisée sans sérieuse étude préalable intégrant la sécurité
  - **Il n'y a encore aucun calcul de retour sur investissement**
  - Sauf pour le vendeur
  - Attendre que la normalisation de la sécurité à l'IETF soit terminée
    - Protocole de gestion de clés VoIP pour SIP : MiKEY
  - Attendre que les terminaux aient les moyens de supporter des négociations de clés en cours de conversation et de chiffrer
- Un challenge de plus pour les *firewalls* et la protection périmétrique
  - Un *firewall* dans mon téléphone pour ne pas sonner quand une société de marketing téléphonique appelle le samedi matin

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Au delà du périmètre

- Cloisonner le réseau et intégrer la sécurité dans le réseau
  - Le réseau est le dénominateur commun du système d'information
  - Le réseau est le premier composant réellement sous le contrôle de l'entreprise
  - Séparer les réseaux bureautique, supervision, téléphonie, etc
  - Prévoir les commutateurs/*firewalls* et la prise en compte de l'espace hertzien
  - Prévoir et accepter la sécurité entre les VLAN
  - Authentifier équipements et utilisateurs
  - Gérer dans le réseau des zônes de confiances telles qu'elles existent dans l'entreprise
- Le cloisonnement permet de créer des lignes de défense qui appliqueront une défense en profondeur

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Firewall en plusieurs boîtes ou tout en un ?

- Tout-en-un :
  - Filtrage IP + vérification protocolaire + VPN + antivirus + IDS/IPS avec mises à jour automatiques
  - Adapté aux installations lointaines, petites de type PME ou site isolé
- Boitiers spécialisés
  - Un ou plusieurs boîtiers n'effectuant qu'une fonction
  - Adapté aux installations centrales, aux opérateurs
  - Devant permettre des mise à jour en production sans discontinuité de service
  - Permettant dprofité du meilleur chez chaque fournisseur
- Complémentaires

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Conclusion

- Poursuivre la progression globale des mesures de sécurité :
  - Inclure la sécurité périmètrique dans chaque PC avec un *firewall*
  - Analyser et journaliser le trafic HTTP et HTTPS, et autoriser les sites en HTTPS uniquement sur liste blanche
  - Etc, etc
- Nous n'en sommes qu'au début de l'ère des *firewalls*
  - Avant : un *firewall* pour tous
  - Maintenant : plusieurs *firewalls* par personne
  - Après ?

Questions ?

Herve.Schauer@hsc.fr
www.hsc.fr

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite

Prochains rendez-vous

- **Conférence 7799** le 24 mai
  - http://www.issafrance.org/premiere.htm
- **Convention Sécurité** les 15 et 16 juin
  - Exposition porte de Versailles
  - Deux jours de tutoriels et de **conférences gratuites**
  - Progr : http://www.hsc.fr/conferences/csm05_programme.html
  - Inscription en ligne : http://www.conventionsecurite.com/
- **Formations SecurityCertified**
  - Du 5 au 9 septembre et du 19 au 23 septembre
  - Permettant de passer la **certification** SCNP
  - http://www.hsc.fr/services/formations/

Copyright Hervé Schauer Consultants 2000-2005 - Reproduction Interdite