



Today's security needs in networking

Besoins actuels de la sécurité réseau



European partner summit
Thursday, October 13, 2005

Hervé Schauer
<Herve.Schauer@hsc.fr>

- Firewalls
- Liability \Rightarrow Perimeter
- Users needs
 - Cost
 - Management
 - Nomadism
 - Filtering
 - HTTP/HTTPS
 - Voice over IP / IP Telephony
 - Outsourcing
- Conclusion

**Slides available at
www.hsc.fr**

Reminder : why firewalls ?

- Why did we need firewalls ?
 - Because the network where everyone talk to everyone has reached its limits with Internet : intrusions, malicious code, etc
 - To apply ingress access control to private networks
 - To enforce its security policy over a single or limited point of control
 - To avoid deployment of security solutions and patches everywhere
- Why not end-to-end security everywhere ?
 - We cannot trust endpoints, we can only trust our security device in between
 - We secure perimeters
 - Compromise and realism

Why perimeter ?

- Briefly you have :
- An area where an officer is responsible
 - His company or employer Information System
- An area where the same officer has no liabilities
 - The rest of the world
- Between his company information system and the rest of the world : the Information System **perimeter**
- We need to know where to start and where to end liability
- We need to protect the area where the officer is responsible

Liability ==> Perimeter ==> Firewalls

Why perimeter ?

- A security policy should apply to the whole Information System
- However :
 - Easiest way to globally enforce a security policy, is using first network access control
 - Network access control is efficient and realistic when first applied on the perimeter
 - Where are and will be the firewalls, and where will they be porous and circumvent
- "The threat comes from the inside", but anyway more from the outside
 - Bad employees use their inside knowledge to attempt attacks from the outside
 - Denial of service
 - ...

Where perimeter ?

- Users need to know where their liability area starts and stops
 - They will buy **firewalls** to build a security perimeter around their liability area
 - ⇒ Several perimeters and network segregation
- Despite the fact that the Information Security perimeter is hard to define
 - Joint-ventures, half-half subsidiaries, subcontractors, etc
 - Wireless networks
 - Removable stockage devices
 - Remote maintenance
 - Outsourcing
 - Nomadism

- Low cost
- Easy and smart firewall management
- Remote access with secured VPNs
- ⇒ **Unified Threats Management**
- Be able to apply filtering to all type of traffic
- ⇒ **HTTP firewall**
- Delegate and outsource when necessary
- ⇒ **Partners able to leverage both integration and outsourcing**
- Get a single person to talk to

- Multiple products often rise cost
 - Firewall, Antivirus, Antispyware, IDS, IPS, URL filtering, antispam, VPN
 - QoS, Wi-Fi, DHCP, DNS, ...
 - Multiple administration interfaces
 - Multiple logging interfaces
 - Multiple trainings for a single admin
 - Several deployment projects, one for each product
- ⇒ All capabilities in an all-in-one appliance
- Each appliance can still be used for a subset of capabilities
- ⇒ **Unified Threats Management**

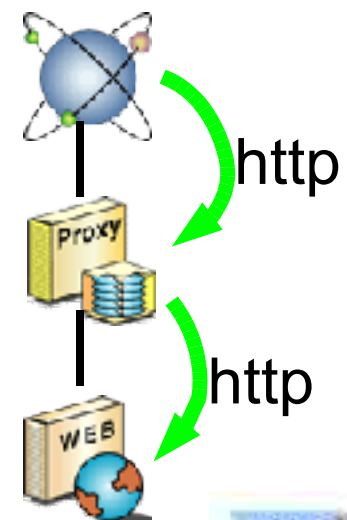
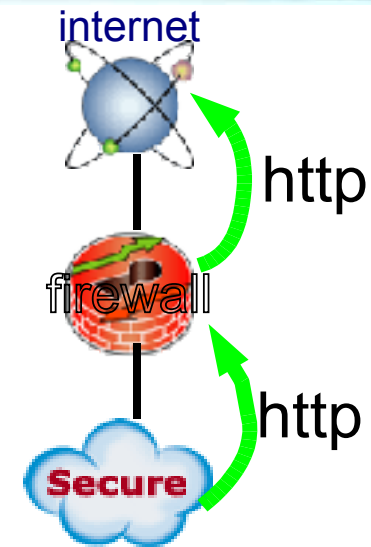
- Multiple interfaces made security unmanageable
- Multiple logging made logging just good for archiving
- ⇒ Same user interface for all capabilities
 - IP firewall, HTTP firewall, IDS, IPS, URL filtering, etc
 - IPsec and SSL VPNs
- ⇒ Same user interface for all devices to be managed
- ⇒ **Unified Threats Management**
 - Everything available in any box

- Built-in nomadism management
 - Remote authentication
 - Encrypted VPNs
 - Specific firewalls rules for remote users
- ⇒ **Unified Threats Management**

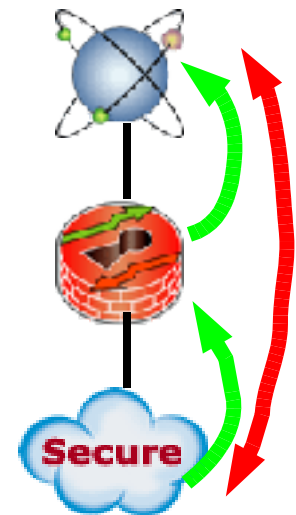
- Be able to apply filtering with all transport protocols
 - IP, HTTP, SIP (Voice over IP), XML, SS7, etc
- Do not allow hidden channels that circumvent the security policy
 - Like over HTTPS, DNS, ICMP
- Do not allow malicious code

⇒ HTTP firewall

- HTTP and HTTPS are carrying all sort of traffic
- Users do not want to let HTTP fully open
- Users would like to apply their security policy toward traffic encapsulated over HTTP
- Users need HTTP firewalls to be able to process content analysis to stop unwanted and malicious content
- Users need similar HTTP firewalling as what we used to have in IP firewalls since 10 years
 - In both ways



- Examples of traffic users would like to control
 - Microsoft : RPC over HTTPS, Outlook 2003, etc
 - VPN-SSL, ssltunnel, stunnel, http-tunnel, etc
 - Webmails
 - EDI software using XML, encapsulating MIME and RPC protocols over HTTP/HTML
 - Instant messaging
 - Groupware over internet
 - Software using Web Services
 - Peer-to-Peer software and others out of control technologies
 - Blackberry, Skype, WebEx, Interwise, MeetingOne, ...
 - Malicious software (spyware, keylogger) running on inside PC and trying to connect outside



- Voice over IP / IP telephony
 - Is not similar to regular telephony
 - Signalling/control and voice transport over the same IP network
 - Lost of geographical localisation of the caller
 - Do not enable application of existing security policies
 - Do not offer the security people are used to
 - Is not just a new application
 - Poor mutual authentication, no ciphering
 - Proprietary solutions are available from some vendors
 - Risks of interception and calls routed toward toll numbers
 - Forgery of number display messages sent back to the caller
 - Attacks attainable by any computer engineer and not limited to digital telephony experts

⇒ Each IP telephony project is an opportunity for security

- For the perimeter : a dedicated firewall
 - Remind your customers that a virtual IP PBX or IP Media Server is not a firewall and those who tried have been hacked
- For the private networks : a new architecture
 - Dedicated VLAN
 - Port / MAC address filtering
 - QoS
- For the management team
 - DNS and DHCP services are becoming **criticals**
 - Reminder : the phone is the first tool for emergency matters

- Customers are not always able to manage the firewalls they deployed
- Real opportunity for outsourced firewall management
 - Bring recurrent revenue
 - Enable long-term and close relationship with your customer
- User interface
 - Key factor of success
 - Prefer web-based
 - Real-time monitoring
 - Logging
 - Regular reports
 - Show explicitly what attacks have been blocked

- Users have always many "little" specific needs
 - Support of specific needs may cut down margin
 - Define your managed services from the beginning and stay with what you decided with a limited number of service agreement
 - Suggest in-house management when too specific
 - Customize via your own adds-on to the web-based interface

- Users need firewall appliances
- Good business opportunities
 - HTTP filtering and VoIP
 - Outsourcing

Questions ?

Herve.Schauer@hsc.fr

www.hsc.fr