



# Les limites des pare-feux

---

*Premier Maître Jean Baptiste FAVRE  
DCSIM / SDE / SIC / Audit SSI  
[jean-baptiste.favre@marine.defense.gouv.fr](mailto:jean-baptiste.favre@marine.defense.gouv.fr)*



# Les limites des pare-feux

- ➔ **Filtres de paquets**
  - « Pro »
  - « Perso »
- ➔ **Proxies**
- ➔ **IDS - IPS**
- ➔ **Anti-virus**
- ➔ **Protocoles**

# Filtres de paquets: les limites

## ➔ « Pro »

- Problème des nomades
  - Début de solution avec 802.1x

## ➔ « Perso »

- Dernier rempart avant les machines
- Pas toujours très fiables

## ➔ Combien de protocoles ?

- Pas toujours implémenté
- Souvent complexe
- RFC pas très claires

# IDS – IPS: les limites

- ➔ **Solution réactive**
- ➔ **Attention aux performances**
  - Paquets fragmentés de taille conséquente
- ➔ **Ne prends pas en compte le système ciblé**



# Anti-virus: les limites

- Solution réactive (mises à jour)
- Sensible aux défauts de l'OS
- Parfois porteur de vulnérabilités (implémentation)
- Attention aux discours marketing

# Protocoles: les limites

- ▶ Vieillissants ...
- ▶ ... et conçus à une époque où la sécurité n'existait pas.
  - Donc plus adaptés aux menaces actuelles

**Vivement IP V6 !!**



# Conclusion

**La sécurité absolue n'existe pas !!**

- Le filtrage est nécessaire ...
- ... mais pas suffisant
- Pensez à l'organisationnel ...
- ... et à la sensibilisation





# SOURCES:

- Magazine « MISC » n° 21, septembre 2005
- « Les virus informatiques: théorie, pratique et applications », Eric Filiol, éd. Springer, 2004
- A venir: SSTIC06 ( juin 2006 )
- Et Internet ;-)

## Questions ?