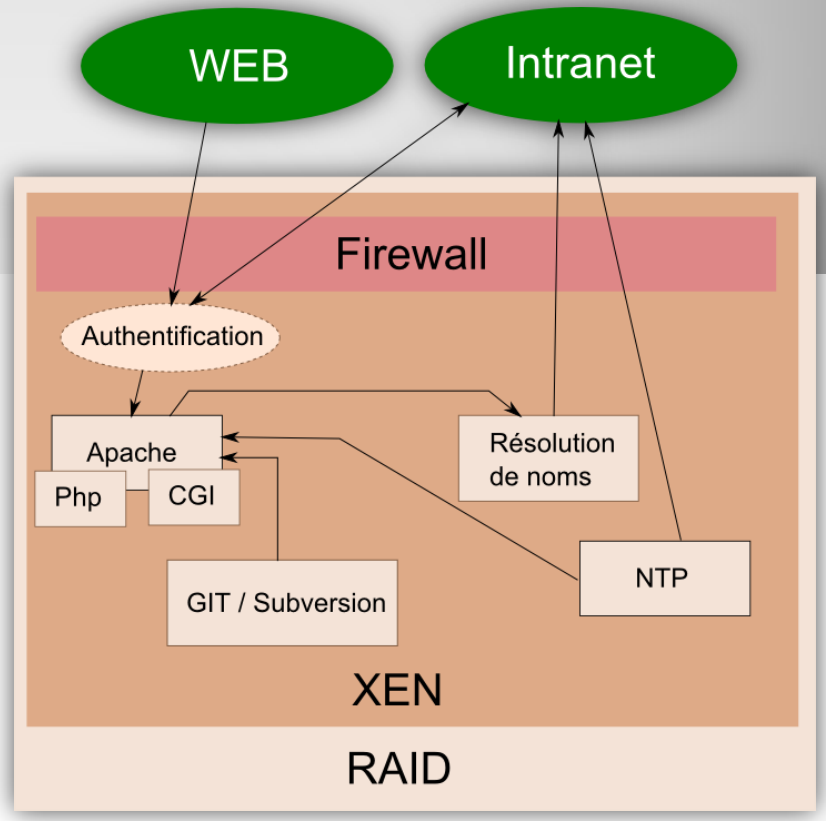
# SECURISATION de serveurs

1. Analyse de risques
2. Mesures de protection
3. Exemple
4. Conclusion

# Analyse de risques

1. **Analyse de risques**
2. Protection de serveurs
3. Exemple
4. Conclusion




- Inventaire par fonction*
- Analyse en terme de CID*
- Synoptique* + flux
- Etude solutions techniques
- Mise en œuvre

# Protection de serveurs

1. Analyse de risques
2. **Protection de serveurs**
3. Exemple
4. Conclusion

## « *BEST PRACTICES* »

*Objectifs de sécurité*

- Virtualisation?

***Disponibilité** accrue (Rsync)*
*Baisse de performances*
*Migration à chaud en iScsi, NetApp*
*PCA*

*<u>Logiciels</u> :*
*Xen, VMWare etc..*

# Protection de serveurs

1. Analyse de risques
2. **Protection de serveurs**
3. Exemple
4. Conclusion

## « *BEST PRACTICES* »

*Objectifs de sécurité*

- Virtualisation?
- Surveillance fichiers sensibles

*Logiciels :*
*Tripwire*

*Contrôle d'**intégrité** des binaires, fichiers de configuration…..*

# Protection de serveurs

1. Analyse de risques
2. **Protection de serveurs**
3. Exemple
4. Conclusion

## « *BEST PRACTICES* »

*Objectifs de sécurité*

- Virtualisation?
- Surveillance fichiers sensibles
- Firewall systématique

*A l'aide du synoptique et de l'analyse de risques , étudier les flux entrants et sortants et bloquer le reste*

*Logiciels :*
*Iptables, Symantec..*

# Protection de serveurs

1. Analyse de risques
2. **Protection de serveurs**
3. Exemple
4. Conclusion

## « *BEST PRACTICES* »

*Objectifs de sécurité*

- Virtualisation?
- Surveillance fichiers sensibles
- Firewall systématique
- Filtre autoban pour toute authentification + chiffrement

*Logiciels :*
*Fail2ban, OpenSSL*

*Empêcher les attaques par « bruteforce » et « MitM », **confidentialité** des échanges*

# Protection de serveurs

1. Analyse de risques
2. **Protection de serveurs**
3. Exemple
4. Conclusion

## « *BEST PRACTICES* »

*Objectifs de sécurité*

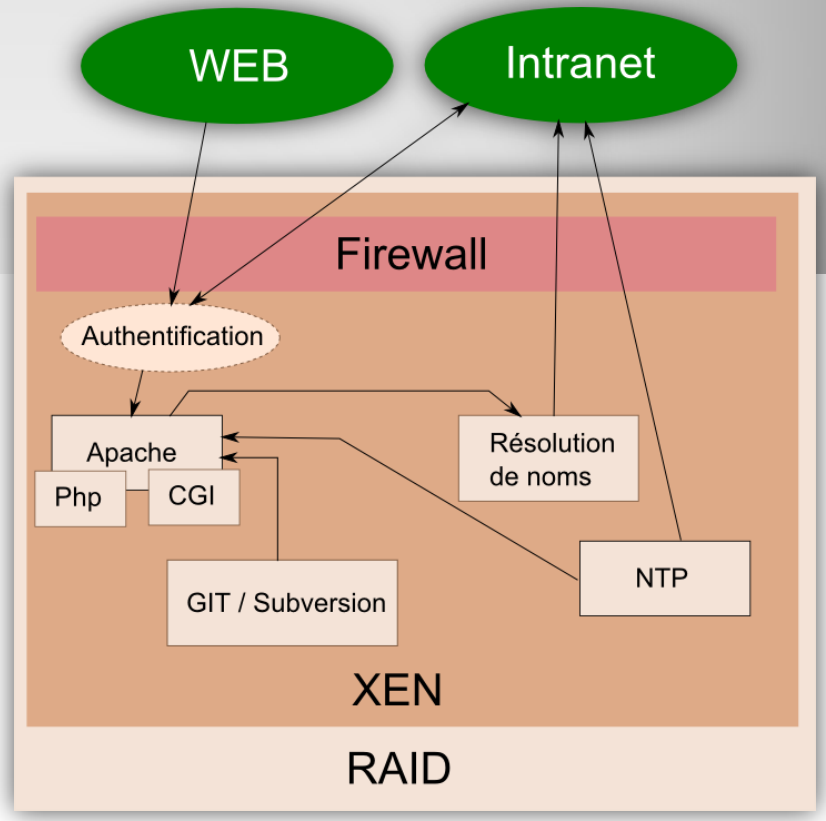
- Virtualisation?
- Surveillance fichiers sensibles
- Firewall systématique
- Filtre autoban pour toute authentification + chiffrement
- Monitoring des ressources et des journaux

*Logiciels :*
*Nagios, rsyslogNG etc…*

*Avoir une meilleure réactivité sur la* ***disponibilité*** *et améliorer la* ***traçabilité***

# Protection de serveurs

1. Analyse de risques
2. Protection de serveurs
3. **Exemple**
4. Conclusion




<u>Développement collaboratif</u> :

- Subversion
- GIT

# Protection de serveurs

1. Analyse de risques
2. Protection de serveurs
3. Exemple
4. **Conclusion**

Aller plus loin vers le PCA : backup, mises à jour, snapshots VM, dépendances de services, restauration de services…

Retour sur expérience : l'analyse de risques met en évidence les besoins en sécurité d'où l'intérêt de « best practices »