

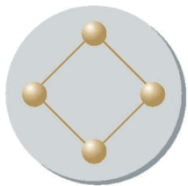
Les Critères Communs appliqués

Christophe BLAD
(OPPIDA)

- ■ Directeur technique du CESTI OPPIDA
- Évaluateur et certificateur CC depuis 1999
- **OPPIDA**
 - Cabinet d'expertise en SSI depuis 1998
 - Conseil, Audit et laboratoire de tests de produits de sécurité
 - Agréé CESTI par l'ANSSI depuis 2003 pour le domaine Systèmes et réseaux
 - 80 évaluations CC
 - 40 évaluations CSPN

Agenda

- 1. Organisation et déroulements des évaluations en France
- 2. Petit rappel sur les CC
Pas trop long, je le promets
- 3. Une évaluation en « live »



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION



Introduction des concepts



Assurance sécurité

Qualité

Caractéristiques subjectives
Non mesurables
Dépendantes des besoins

Sécurité

Expression des besoins



Exigences formalisées

Exigences fonctionnelles de sécurité [CC]

SFR: Security Functional Requirements

Assurance Sécurité

Éléments de confiance démontrant que la cible de l'évaluation implémente les exigences fonctionnelles de sécurité. [CC v3.1]

Assurance sécurité

■ Résultats d'une évaluation CC

CONFORME

« SUCCESS »

NON CONFORME

« FAIL »

■ Niveau d'assurance EAL1...EAL7

- Quantité d'information utilisée par l'évaluateur pour formuler ce verdict
- Plus la quantité information utilisée est élevée, plus le niveau de confiance dans le résultat est élevé

Le contexte réglementaire (civil) en France

Homologation de sécurité:

« le système peut traiter des informations sensibles »
Décision de l'Autorité Qualifiée pour le système

Qualification:

« le produit a les capacités de traiter des informations sensibles »
Référence : RGS
Par le bureau Réglementation de l'ANSSI

Certification:

« l'évaluation s'est déroulée dans les règles de l'art »
Référence : Décret 2002-535
Par le bureau Certification de l'ANSSI

Évaluation:

« le produit répond aux exigences mentionnées dans sa cible de sécurité »
Référence : critères CC ou CSPN
Par un laboratoire (CESTI) privé



L'évaluation réalisée par OPPIDA



Évaluation

- ■ Analyse des éléments d'Assurance Sécurité sur deux aspects
 - **conformité**: implémentation effective des « exigences de sécurité ».
 - **efficacité**: vulnérabilités de l'implémentation des exigences de sécurité (possibilité de désactiver les fonctions, de les contourner).
- Suivant une méthodologie reconnue
 - Au niveau national: les CSPN
 - Au niveau international : les Critères Communs

Déroulement de l'évaluation (1/2)

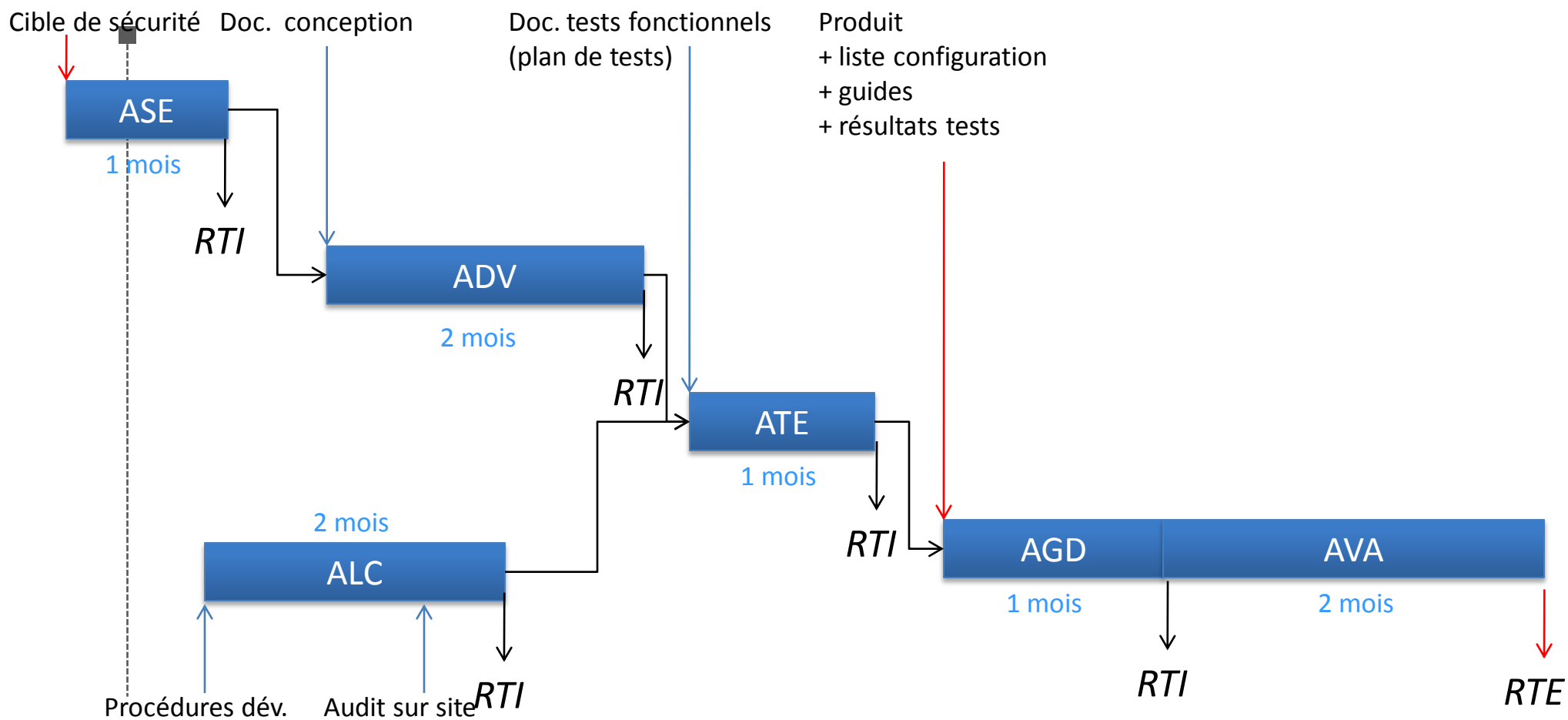
- 1. Fourniture du cahier des charges de l'évaluation: la Cible de Sécurité (Security Target: ST)
 - Liste des exigences fonctionnelles de sécurité (Security Functional Requirements: **SFR**) à évaluer
 - Liste des contrôles sur l'Assurance Sécurité (Security Assurance Requirements: **SAR**) à réaliser par l'évaluateur

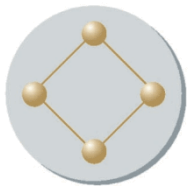
2. Livraison d'éléments de preuve (fournitures) par le développeur
 - Les procédures utilisées dans l'environnement de développement
 - Les documents de conception
 - Les guides
 - Les tests fonctionnels réalisés (plan de tests et résultats pour la version à évaluer)
 - Le produit

Déroulement de l'évaluation (2/2)

- Émission de Rapports Techniques Intermédiaires (RTI) tout au long de l'évaluation
- Émission d'un **Rapport Technique d'Évaluation** (RTE) à l'issue des travaux
- Pour chaque exigence d'Assurance, émission d'un verdict
 - **REUSSITE – SUCCESS**: l'exigence est satisfaite
 - **ECHEC – FAIL**: l'exigence n'est pas satisfaite
 - La tâche reste ouverte et doit nécessairement être terminée avant la fin de l'évaluation, sinon il y a échec global de l'évaluation
 - **A CONFIRMER – INCONCLUSIVE**: Les documents transmis ne permettent pas à l'évaluateur de statuer sur un verdict REUSSITE ou ECHEC
 - La tâche est suspendue, en attendant la livraison d'informations complémentaires

Un planning type (idéal) d'évaluation (CC EAL3+)





OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION



La certification par le Premier ministre



La Certification

- Objectifs

- Certifier que l'évaluation s'est déroulée dans les règles de l'art

L'évaluateur est compétent

L'évaluateur est indépendant

La méthodologie est respectée

} Agrément CESTI

La Certification

- ■ Encadrée par le schéma français de certification: décret 2002-535
 - Le **commanditaire** choisit un **centre d'évaluation (CESTI)** agréé par l'**ANSSI** pour mener l'évaluation du produit (Art. 3)
 - Un **commanditaire** demande la certification d'un produit ou d'un système à l'**ANSSI** (Art. 2)
 - L'**ANSSI** veille à la bonne exécution des travaux d'évaluation (Art. 5)
 - Au terme des travaux d'évaluation, le **CESTI** remet un rapport d'évaluation au **commanditaire** et à l'**ANSSI** (Art. 6)
 - L'**ANSSI** élabore un rapport de certification qui conclut soit à la délivrance d'un certificat, soit au refus de la certification (Art. 7)
 - Le certificat est délivré par le **Premier ministre** (Art. 8)

Reconnaissance internationale des certificats CC

Les certificats CC émis par l'ANSSI sont reconnus au niveau international

- Pays émetteurs de certificats

- France, Royaume Uni, Allemagne, Canada, États-Unis, Australie, Nouvelle Zélande, Japon, Pays-Bas, Norvège, Corée du Sud, Espagne, Suède, Italie, Malaisie, Turquie, Inde



- Pays reconnaissants les certificats

- Pays émetteurs + Autriche, République Tchèque, Danemark, Finlande, Grèce, Hongrie, Israël, Singapour, Pakistan

La Certification Sécurité Premier Niveau (CSPN)

- ■ Création du CSPN en mai 2008 suite au rapport du député Pierre Lasbordes (novembre 2005)
 - « Développer la politique de certification et de qualification par une augmentation des produits certifiés et qualifiés et une réduction des délais et des coûts de certification »
- Phase expérimentale 2008-2011, Officialisation de la démarche en mai 2011
- Charge imposée:
 - 25 hommes.jours pour les tests
 - 10 hommes.jours pour l'analyse de la crypto (si présente)

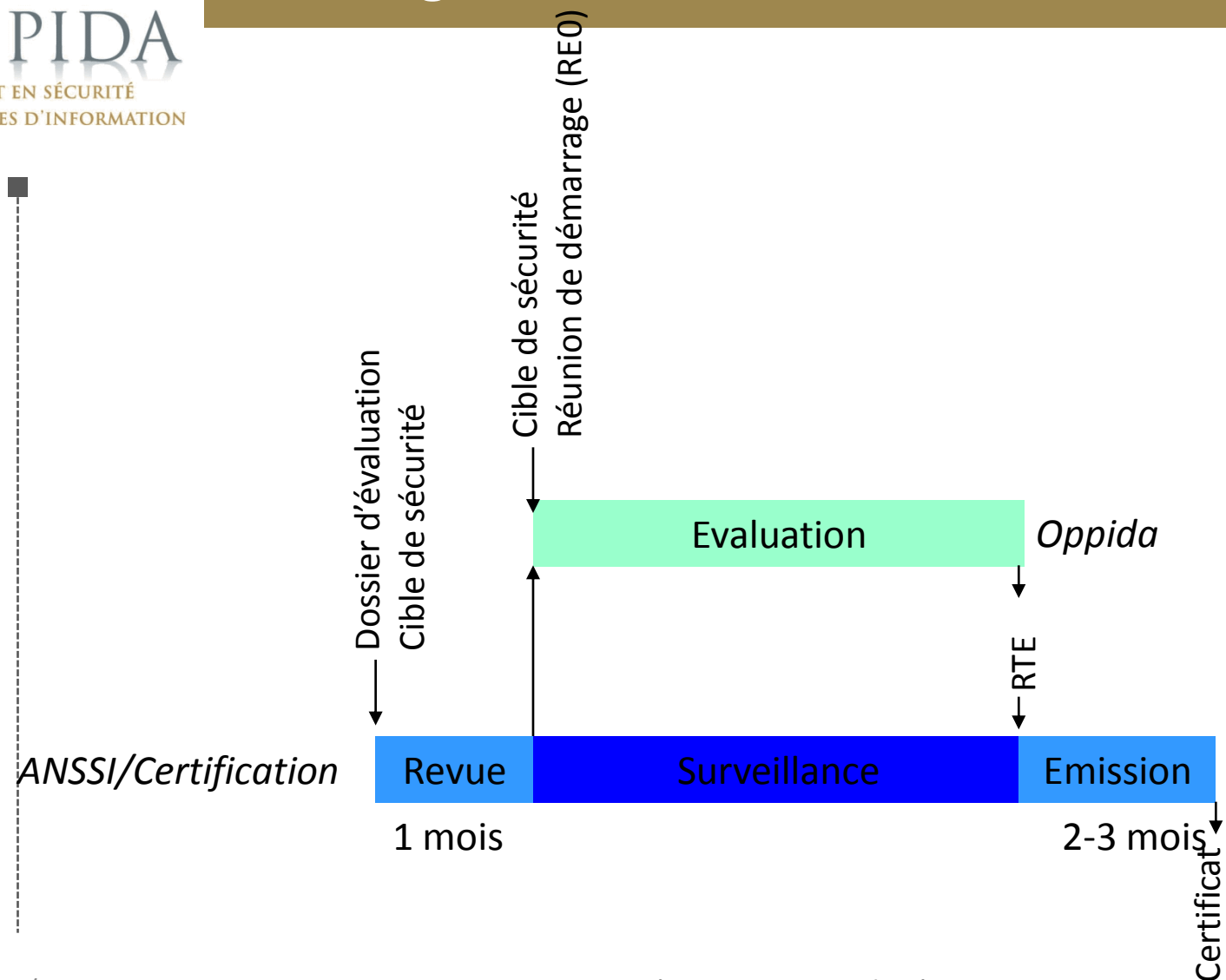
Différences CC - CSPN

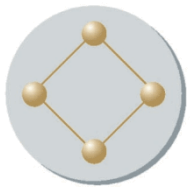
- | | | |
|--|---|--|
| <ul style="list-style-type: none"> ■ CC | <ul style="list-style-type: none"> ■ Cible de sécurité ■ Le CESTI émet des verdicts de conformité aux exigences des CC ■ RTE ■ Itérations documentaires et/ou du produit possibles ■ Reconnaissance internationale | <ul style="list-style-type: none"> ■ CSPN ■ Cible de sécurité ■ Le CESTI n'émet pas de verdict, seulement des constats ■ RTE ■ Aucune itération possible (car charge imposée) ■ Pas de reconnaissance internationale |
|--|---|--|

La maintenance du certificat

- ■ A produit constant: besoin de surveiller « l'érosion » de l'efficacité
 - La **surveillance**
 - Utile essentiellement pour le matériel
- Suite à une évolution du produit: besoin de contrôler à nouveau à la fois la conformité et l'efficacité
 - La **continuité de l'assurance**: décision de l'ANSSI sur la base d'une auto-déclaration du développeur (analyse d'impact)
 - Si pas d'impact sur fonctions de sécurité: validation de l'analyse d'impact par l'ANSSI
 - Si impact: réouverture de l'évaluation → implication du CESTI
 - Réalisation des travaux nécessaires (conformité et efficacité)
 - Nouveau RTE, nouveau certificat

Planning Certification





OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION



La Qualification de produits par l'ANSSI



La Qualification

■ Objectifs

Statuer sur l'éligibilité du produit à être intégré dans un système traitant des informations sensibles (mais non classifié de défense)

- Trois niveaux de qualification définis dans le RGS
 - **Élémentaire**: nécessite certificat CSPN
 - **Standard**: nécessite certificat CC EAL3+
 - **Renforcée**: nécessite certificat CC EAL4+

Processus pour obtenir une qualification

■ ■ 3 étapes

- Approbation de la cible de sécurité par l'ANSSI
 - Le périmètre répond à un besoin de l'administration
 - Conformité à un profil de protection
- Estimation de la résistance des mécanismes cryptographiques
 - Cotation théorique des algorithmiques
 - Expertise de l'implémentation des mécanismes cryptographiques
- Évaluation CC

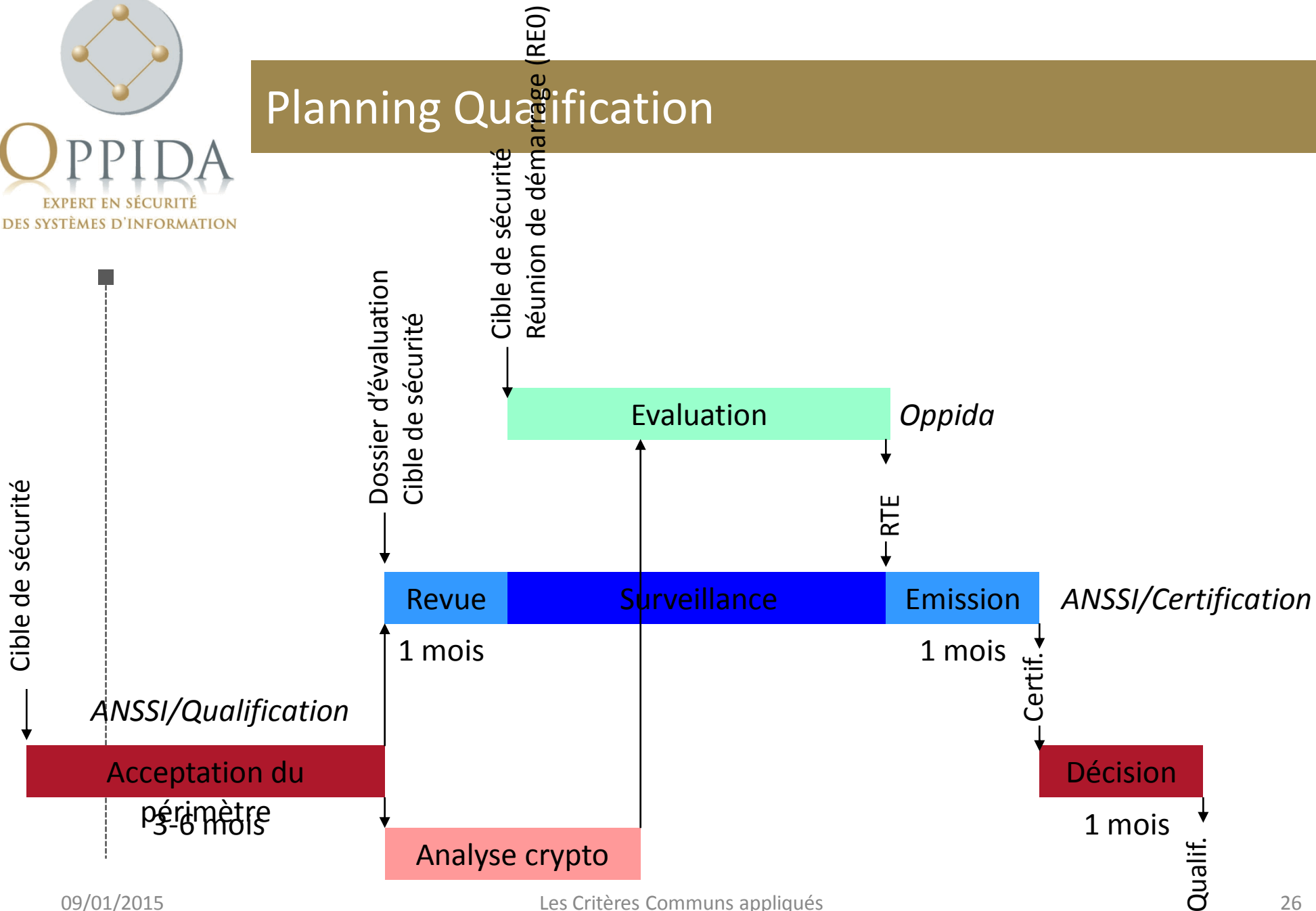
La cryptographie

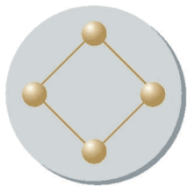
- ■ Estimation de la résistance des mécanismes cryptographiques
 - Le CESTI procède à l'étude théorique des mécanismes cryptographiques (« Cotation crypto »)
 - Vérification que les exigences du RGS (annexes B) sont respectées
 - Identification des vulnérabilités potentielles
 - Le CESTI contrôle l'implémentation effective des mécanismes cryptographiques (« Expertise de l'implémentation de la crypto »)
 - Fourniture du code source du produit complet, pour:
 - Vérifier la conformité du produit aux spécifications fournies
 - Vérifier si les attaques cryptographiques identifiées sont réellement exploitables

Evaluation CC pour la qualification standard

- EAL3 augmenté des composants ALC_FLR.3 et AVA_VAN.3
 - Evaluation de la Cible de Sécurité
 - Environnement de développement
 - Description du cycle de vie du produit (ALC_LCD.1)
 - Sécurité du site de développement (ALC_DVS.1)
 - Utilisation d'un système de gestion de configuration (ALC_CMC.3, ALC_CMS.3)
 - Procédures de livraison du produit (ALC_DEL.1)
 - Correction des anomalies (ALC_FLR.3)
 - Conception
 - Spécifications fonctionnelles (ADV_FSP.3)
 - Architecture du produit (ADV_ARC.1, ADV_TDS.2)
 - Guides
 - Guides d'installation (AGD_PRE.1)
 - Guides d'exploitation (AGD_OPE.1)
 - Tests fonctionnels
 - Plan de test fonctionnel (ATE_FUN.1)
 - Couverture des tests (ATE_COV.2, ATE_DPT.1)
 - Tests fonctionnels indépendants (ATE_IND.2)
 - Analyse des vulnérabilités
 - Résistance à un attaquant de niveau élémentaire (AVA_VAN.3)

Planning Qualification





OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION



Petit rappel sur les Critères Communs



Historique

- 1985 : TCSEC (« Orange Book ») - Etats-Unis
- 1991 : ITSEC – France, Allemagne, Royaume Uni, Pays-Bas
- 1994 : Critères Communs (CC) – Europe, Etats-Unis, Canada
- 1999 : ISO 15408:1999 (Common Criteria v2.1)
- 2005 : ISO 15408:2005 (Common Criteria v2.3)
- 2005: Common Criteria v3.0
- 2006: Common Criteria v3.1
- Aujourd'hui : Common Criteria v3.1 revision 4

Les CC

- 3 parties:

1. Introduction
2. Catalogue d'exigences fonctionnelles
3. Catalogue d'exigences d'assurance

- Des catalogues normalisés permettant

- La comparaison des fonctionnalités de sécurité d'un produit évalué (partie 2)
- La comparaison des travaux d'évaluation réalisés (partie 3)

- Sa méthodologie: la **CEM** (Common Evaluation Methodology)

- Pour chacun des composants de la partie 3: détail des contrôles à réaliser par le CESTI

Organisation des catalogues

- **Classes: Fxx, Axx**

- Familles: XXX_XXX

- Composants: XXX_XXX.X

- Exigences: XXX_XXX.X.yyy

- FXX_XXX.X.y : exigences fonctionnelles

- AXX_XXX.X.yD: exigences d'assurance pour le développeur (livrables)

- AXX_XXX.X.yC: exigences d'assurance de contenu (contenu des livrables)

- AXX_XXX.X.yE: exigences d'assurance pour l'évaluateur (tâches d'évaluation)

Hiérarchie entre les exigences

exigences AVA_VAN.1 < exigences AVA_VAN.2 < exigences AVA_VAN.3

Partie 2

■ Composants fonctionnels

- Structurés en 11 classes : [CC v3.1]

FAU Audit de sécurité

FCO Communication

FCS Support cryptographique

FDP Protection des données de l'utilisateur

FIA Identification et authentification

FMT Administration de la sécurité

FPR Protection de la vie privée

FPT Protection des fonctions de sécurité

FRU Utilisation des ressources

FTA Accès à la TOE

FTP Chemins et canaux de confiance

Partie 3

■ ■ Composants d'assurance

- Structurés en 5 classes : [CC v3.1]

ADVConception

AGD Guides

ALC Support du cycle de vie

ATE Tests

AVA Estimation des vulnérabilités

- Deux classes « spéciales »

APE Protection Profile Evaluation

ASE Security Target Evaluation

Le niveau d'évaluation

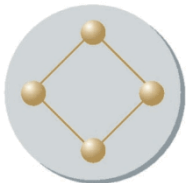
- Les Critères Communs définissent 7 paquets prédéfinis homogènes
 - EAL1 - testé fonctionnellement
 - EAL2 - testé structurellement
 - EAL3 - testé et vérifié méthodiquement
 - EAL4 - conçu, testé et revu méthodiquement
 - EAL5 - conçu à l'aide de méthodes semi-formelles et testé
 - EAL6 - conception vérifiée à l'aide de méthodes semi-formelles et testé
 - EAL7 - conception vérifiée à l'aide de méthodes formelles et testé
- Possibilité de définir son propre paquet à partir du catalogue
- Plus le niveau de confiance requis est élevé, plus les éléments de preuve demandés sont nombreux et détaillés

Les niveaux EAL

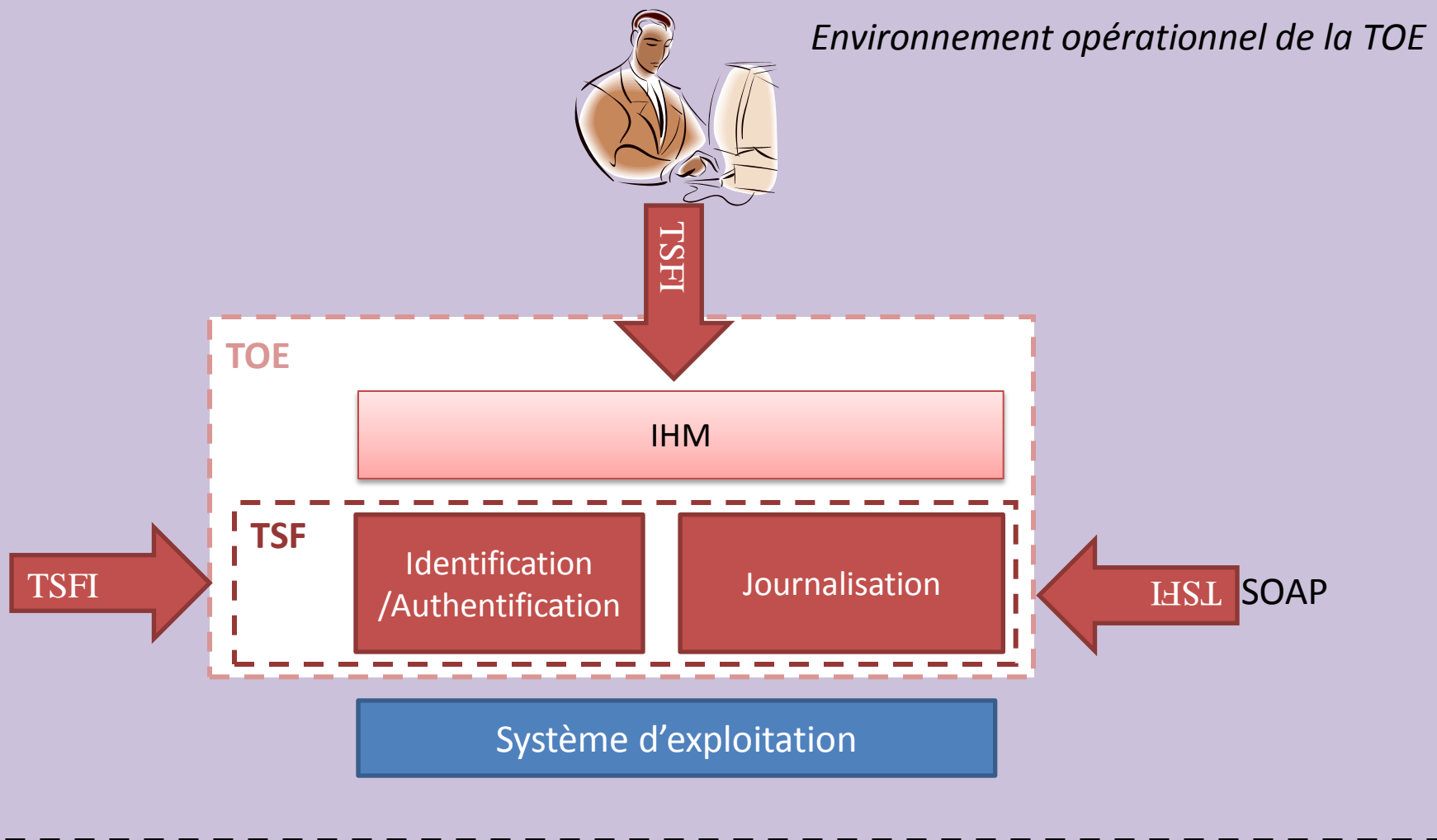
Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
Tests	ASE_TSS	1	1	1	1	1	1	1
	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
Vulnerability assessment	ATE_IND	1	2	2	2	2	2	3
	AVA_VAN	1	2	2	3	4	5	5

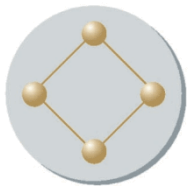
Concepts CC

- - La cible d'évaluation (TOE)
 - Le produit ou le système (technique) qui est l'objet de l'évaluation
 - **C'est l'objet produit et livré à l'issue du processus de « développement »**
 - Un Profil de protection (PP)
 - Cahier des charges générique décrivant les fonctionnalités de sécurité exigées et les travaux d'évaluation à réaliser pour un système ou un produit intégré dans un contexte opérationnel donné
 - Une Cible de sécurité (ST)
 - Profil de protection
 - +
 - Réponses spécifiques d'un produit aux exigences spécifiées dans le PP
 - La TSF (TOE Security Functions)
 - La partie du produit ou du système qui réalise les exigences fonctionnelles de sécurité
 - La TSFI (TSF Interfaces)
 - L'ensemble des interfaces permettant d'interagir avec la TSF



Concepts CC





OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION



Fournitures

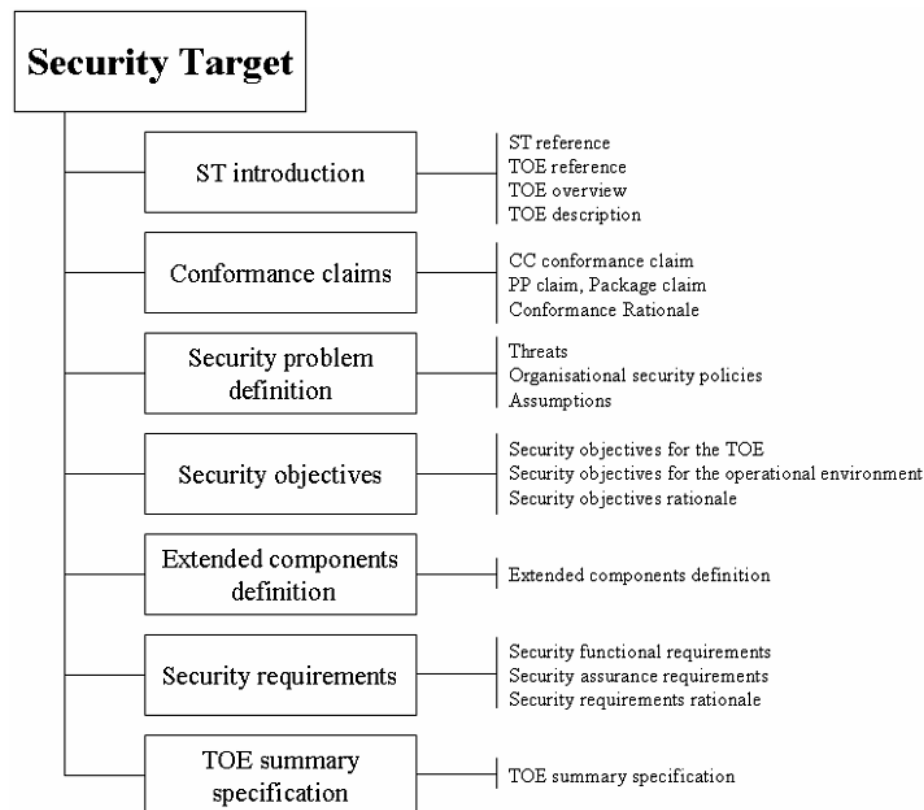


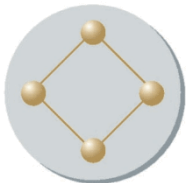
Les documents à livrer au CESTI

- ■ La Cible de sécurité
- La description de l'environnement de développement
 - à partir de EAL3 seulement
- La description de la conception du produit
 - le niveau de détail dépend du niveau
- La description des tests fonctionnels réalisés sur le produit
 - à partir de EAL2 seulement
- Le produit avec ses guides d'installation et d'utilisation

La Cible de sécurité

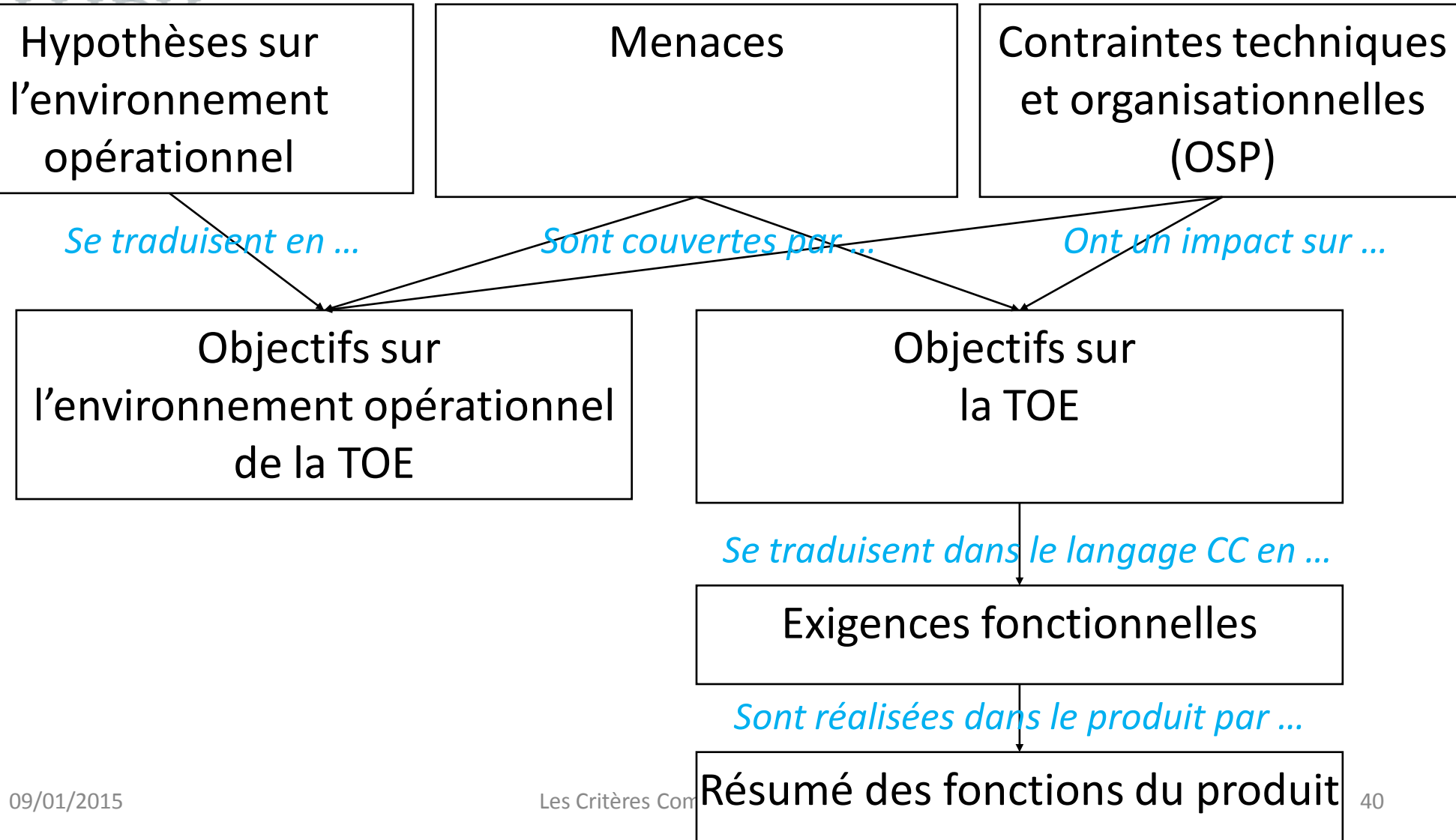
- Analyse de risques justifiant les fonctionnalités de sécurité exigées et les travaux d'évaluation à réaliser
+
- Présentation des fonctionnalités implémentées dans le produit à évaluer pour répondre à ces exigences
- Contenu décrit dans la Partie 1 des CC, Annexe A
- Exigences détaillées de contenus
 - Composant ASE: CC Partie 3





OPPIDA

Structure de la cible de sécurité



La Cible de sécurité

Objectifs du CESTI

Vérifier si le périmètre à évaluer est clair

Détecter les « trous » et les incohérences dans la justification des fonctions de sécurité

La description de l'environnement de développement (ALC)

- - À partir de EAL3 seulement
 - Le Plan de développement
 - Les Procédures de sécurité du site de développement
 - Sécurité physique
 - Sécurité informatique des serveurs contenant les sources et des postes de travail des développeurs
 - Le plan de gestion de configuration, la liste précise des composants gérés en configuration
 - La procédure de livraison du produit et de sa documentation
 - Les procédures du support logiciel

Objectifs du CESTI

Identifier les failles permettant de modifier le produit sans que personne ne s'en rende compte

La description de la conception du produit (ADV)

- - Les spécifications fonctionnelles
 - Dès EAL1
 - Un document d'architecture générale + un document de justification de l'architecture
 - Décomposition de la TOE en sous-systèmes
 - À partir de EAL2 seulement
 - Un document d'architecture détaillée
 - Décomposition des sous-systèmes en modules
 - À partir de EAL4 seulement
 - Le code source
 - Lien entre les modules et l'organisation des fichiers de code source
 - À partir de EAL4 seulement

Objectifs du CESTI

Être convaincu que les fonctions déclarées dans la cible de sécurité sont bien présentes dans le produit

La description des tests fonctionnels réalisés sur le produit (ATE)

- ■ À partir de EAL2 seulement
- Le plan de tests
- Des matrices de couverture des tests
 - Tests fonctionnels vs. Interfaces et fonctions de sécurité
 - Tests unitaires vs. Sous-systèmes (EAL3)
 - Tests unitaires vs. Modules (EAL5)
- Les résultats des tests pour la version de la TOE évaluée

Objectifs du CESTI

Vérifier que le fonctionnement des fonctions de sécurité déclarées dans la cible de sécurité a au moins été testé par le développeur

Le produit avec ses guides d'installation et d'utilisation (AGD)

- ■ La TOE
 - Rappel: objet produit et livré à l'issue du processus de développement
- Son guide d'installation
- Ses guides d'utilisation et d'administration

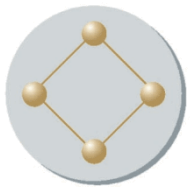
Objectifs du CESTI

Vérifier que la procédure de livraison est respectée

Installer le produit uniquement à partir des guides disponibles

Configurer puis utiliser le produit dans la configuration décrite dans la cible de sécurité

-> Tout cela permet de donner un avis sur la complétude et la clarté des guides



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION



Retour d'expérience d'un CESTI



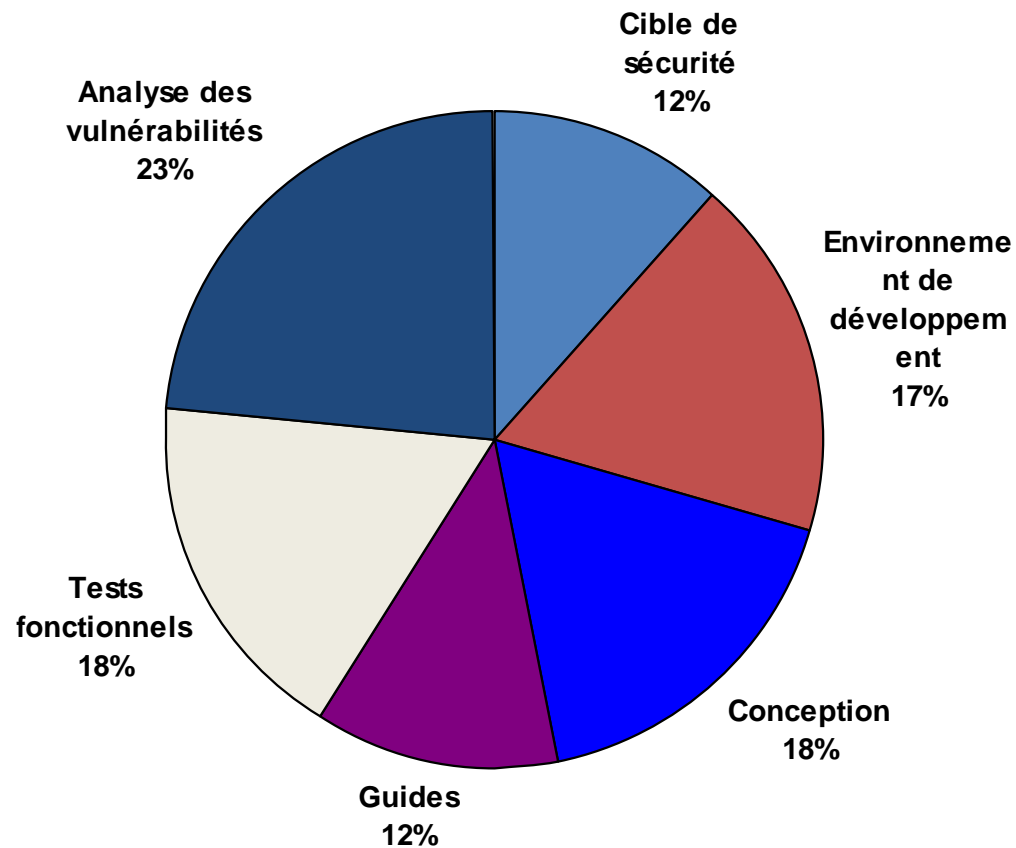
Difficultés d'une évaluation

- Coûts externes (contrat d'évaluation): 50%
 - Fortement liés à différents facteurs :
 - Niveau d'évaluation visé
 - Périmètre fonctionnel à évaluer
 - Taille du logiciel
- Coûts internes pour le développeur: 50%
 - Bilan documentaire du processus de développement
 - Formation au processus
 - Suivi de projet (relations développeur / CESTI / ANSSI)
 - Support technique à l'évaluateur
 - Maintenance des documents (reprises documentaires)

Coûts (externes) d'évaluation approximatifs

- CSPN (en vue d'une qualification élémentaire)
 - Equivalent à un audit « boîte noire »
 - Charge imposée par ANSSI : 25 + 10 h.j.
 - Délais imposé: 2 mois
- EAL3+ (en vue d'une qualification standard)
 - Equivalent à un audit « boîte grise » (+expertise crypto)
 - Charge : ~100 h.j.
 - Délais: 6 à 12 mois
- EAL4+ (en vue d'une qualification renforcée)
 - Equivalent à un audit « boîte blanche » (analyse du code source)
 - Charge : ~140 h.j.
 - Délais : 9 à 12 mois

Répartition des charges d'évaluation



EAL3+ (qualification standard)

Difficultés techniques rencontrées (1/2)

- Rédaction de la cible de sécurité

- ☞ Sous-traitance de la rédaction

- Spécification claire du périmètre

- Liste des personnes hostiles
 - Inclusion des librairies tierces, systèmes d'exploitation, des modules hardware

- Tous les éléments de la TOE doivent être intégrés dans la gestion de configuration

- ☞ Avoir les idées claires dès le début: qu'est ce qui est livré?

Difficultés techniques rencontrées (2/2)

- Homogénéité de la documentation de conception
 - – Doit permettre à l'évaluateur de « tracer » les mécanismes de sécurité implémentés :
 - dans les tests fonctionnels (cas d'erreur en particulier)
 - dans les guides (configuration en particulier)
 - 👉 Relire les documents avant de les envoyer
 - 👉 Si tous les documents existent déjà : procédure *Collection of evidence*
- Règles strictes sur les mécanismes cryptographiques
 - – Spécifications très précises
 - Le développeur doit maitriser tous les mécanismes utilisés
 - Nécessite une personne avec des compétences fortes dans le domaine
 - – Commentaires ont généralement un impact fort sur le produit
 - 👉 Envoyer les spécifications crypto le plus tôt possible

Avantages d'une évaluation

■ Impacts directs

- Obtention d'un certificat délivré par un organisme étatique: l'ANSSI
- Reconnaissance de ce certificat sur le plan international (seulement pour les CC)
- Publication sur la liste des produits évalués
<http://www.ssi.gouv.fr/>
- Possibilité de répondre à des appels d'offres exigeant un niveau d'évaluation minimum
- Si qualification, référencement/recommandation du produit par l'ANSSI auprès des ministères et autres administrations

Avantages d'une évaluation

- Impacts indirects

- - Amélioration du processus de développement logiciel
 - Gestion en configuration
 - Documentation
 - Sécurité du développement
 - Validation des méthodes de développement d'un produit
 - Traçabilité des fonctions de sécurité
 - Audit indépendant du code source
 - Analyse de la qualité de la cryptographie par un expert
 - Validation des méthodes de qualification d'un produit
 - Couverture et profondeur du plan de tests
 - Transfert de compétences sur les vulnérabilités et techniques d'attaque

Application pratique



Agenda

- ■ Rédiger la cible de sécurité
- Analyser le process de développement
- Analyser des spécifications fonctionnelles
- Analyser des documents de conception
- Analyser le code source
- Tests fonctionnels
- Tests de vulnérabilités

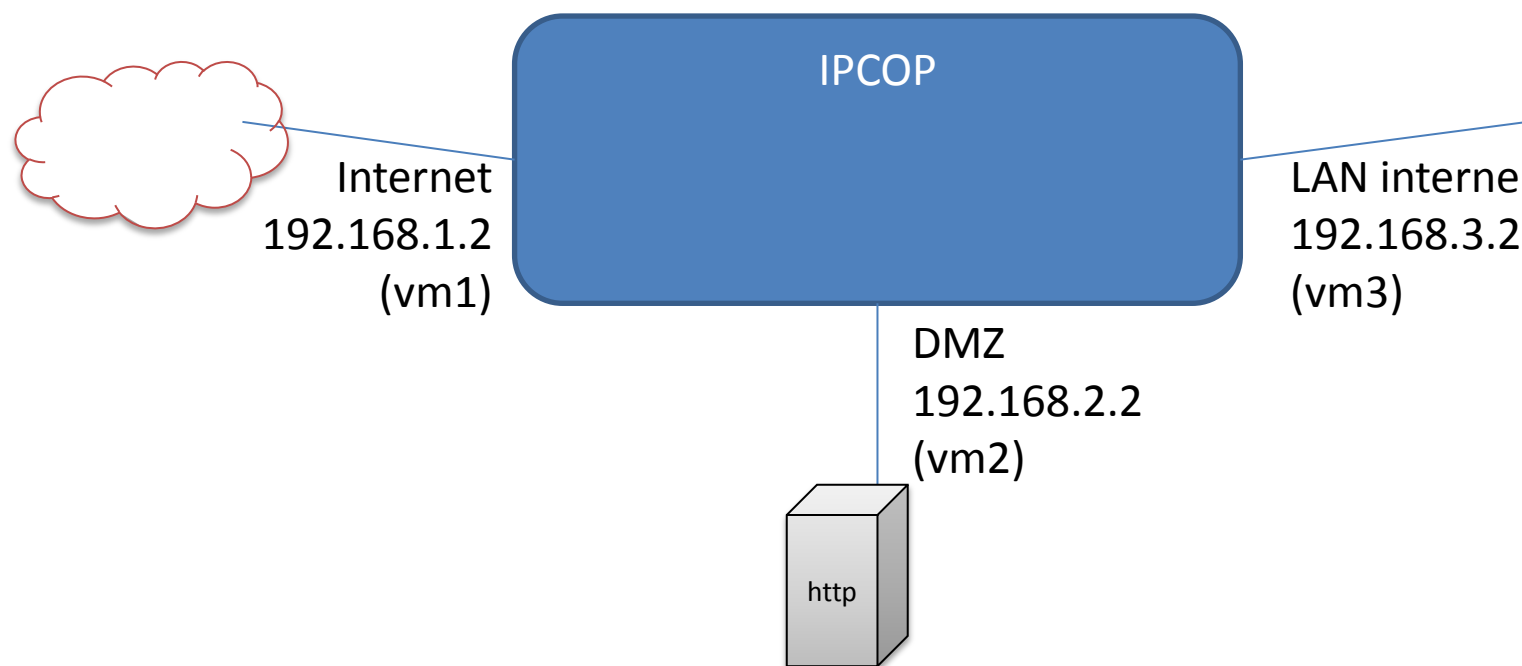
... sur un exemple concret

L'exemple concret

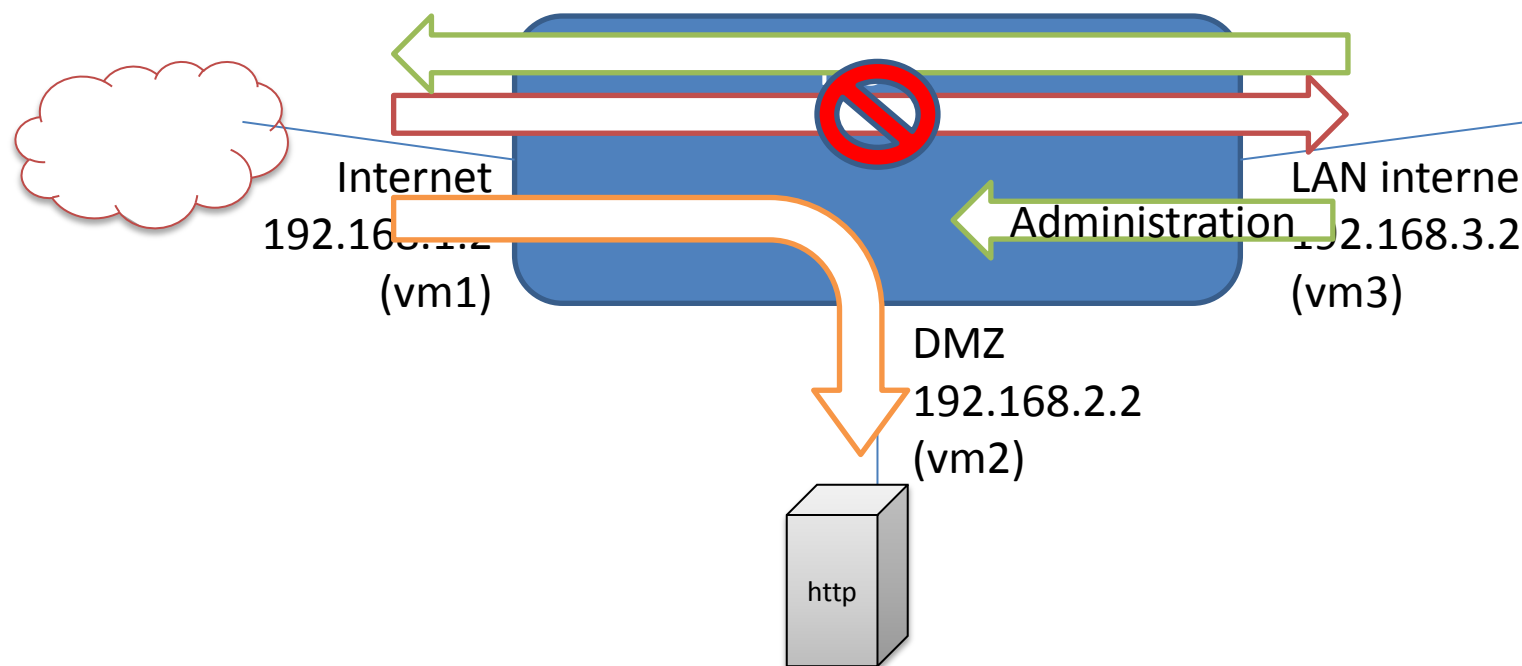
- ■ Firewall logiciel IPCOP v2.0.3
 - Sorti début 2012
- Open source (ipcop.org)
 - Code source disponible sur Sourceforge
- Jamais évalué CC à ce jour



L'exemple concret



Architecture classique DMZ



Agenda

- ■ Rédiger la cible de sécurité
 - Analyser le process de développement
 - Analyser des spécifications fonctionnelles
 - Analyser des documents de conception
 - Analyser le code source
 - Tests fonctionnels
 - Tests de vulnérabilités

La cible d'évaluation

- ■ TOE: Target of Evaluation

IPCOP v2.0.3

- Type de TOE: firewall
- Description de la TOE: cf. site web

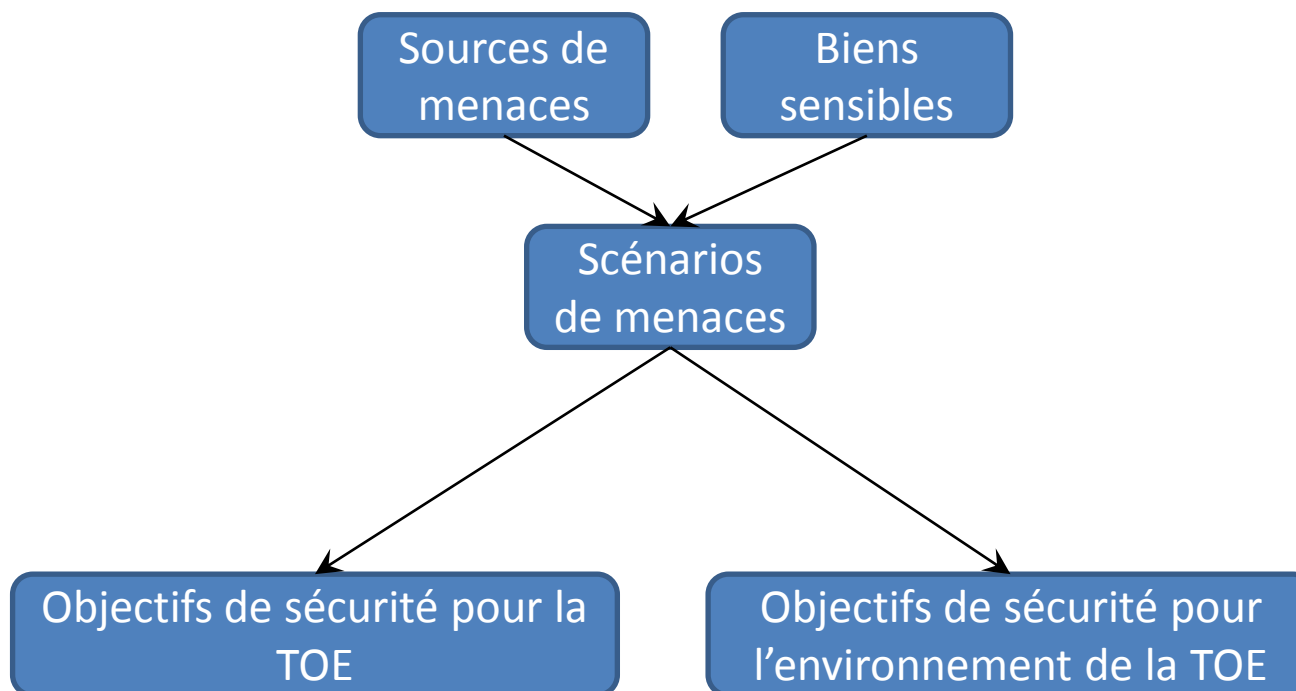
Les utilisateurs de la TOE

- Les utilisateurs/machines connectés aux réseaux interconnectés (WAN, DMZ, LAN)
- Les administrateurs du firewall

Sujets / Opérations / Objets

- ■ Sujet / Verbe / Complément
- La [TOE] [filtre] les [trames IP]
- L'[Administrateur] [configure] les [règles de filtrage]

L'analyse de risque



Sources de menaces (accident et/ou attaque)

- Les utilisateurs légitimes

- Utilisateurs des réseaux
 - Administrateurs

- Les personnes ayant accès à la TOE

- Accès physique

- Technicien ayant accès à la salle serveur

- Accès réseau

- Machine sur le WAN (utilisateurs du WAN)

- Machine sur la DMZ (utilisateurs de la DMZ)

- Machine sur le LAN interne (utilisateurs du LAN)

C'est le moment de faire des choix

- Les sources de menaces sont-elles retenues pour l'évaluation?
- Si non -> hypothèses

Administrateurs	NON	<i>Il est fait l'hypothèse que les administrateurs sont de confiance et bien formés</i>
Technicien ayant accès à la salle serveur	NON	<i>Il est fait l'hypothèse que l'accès physique à la TOE est limité à des personnes de confiance</i>
Machine sur le WAN	OUI	
Machine sur la DMZ	OUI	
Machine sur le LAN	OUI	

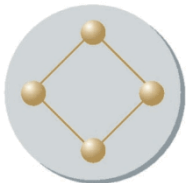
Les biens sensibles

- ■ Les données protégées par la TOE (*User-data*)
 - La DMZ
 - Le réseau interne

- Les données de la TOE elle-même (*TSF-data*)
 - Les règles de filtrage

Scénarios de menaces

	La DMZ	Le réseau interne	Les règles de filtrage
Machine sur le WAN	Intrusion DMZ	Intrusion réseau interne	Intrusion TOE
Machine sur la DMZ	à partir WAN	à partir WAN	à partir WAN
	Hors périmètre	Intrusion réseau interne	Intrusion TOE
Machine sur le LAN		à partir DMZ	à partir DMZ
	Non retenu	Hors périmètre	Intrusion TOE
			Attaque du compte administrateur



Objectifs de sécurité

	Objectifs pour la TOE	Objectifs pour l'environnement de la TOE
Intrusion DMZ à partir WAN	Filtrage trames traversantes Journalisation	
Intrusion réseau interne à partir WAN	Filtrage trames traversantes Journalisation	
Intrusion TOE à partir WAN	Filtrage trames entrantes Journalisation	
Intrusion réseau interne à partir DMZ	Filtrage trames traversantes Journalisation	
Intrusion TOE à partir DMZ	Filtrage trames entrantes Journalisation	
Intrusion TOE à partir LAN	Filtrage trames entrantes Journalisation	
Attaque compte administrateur	Authentification administrateur	Administrateur ne doit pas communiquer son mot de passe
		Procédures d'habilitation et de formation des administrateurs
Administrateurs de confiance	Les Critères Communs appliqués	TOE doit être installée dans une salle à accès contrôlé

C'est là que ca pique ...

- Traduction des objectifs sur la TOE dans le langage CC
- Langage naturel -> Exigences communes extraites de la partie 2

	Exigences CC Part 2
Filtrage trames traversantes	FDP_IFC.1, FDP_IFF.1 / trames traversantes
Filtrage trames entrantes	FDP_IFC.1, FDP_IFF.1 / trames entrantes
Journalisation	FAU_GEN.1
Authentification administrateur	FIA_UAU.1

Juste un exemple: Politique de contrôle de flux traversants

- FDP_IFC.1

- FDP_IFC.1.1 The TSF shall enforce the [*Politique filtrage flux traversants*] on [*Trames IP*].

- FDP_IFF.1

- FDP_IFF.1.1 The TSF shall enforce the [*Politique filtrage flux traversants*] based on the following types of subject and information security attributes: [*Trames IP : adresse/port source, adresse/port destination*].
- FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
[*Trames IP : adresse/port source, adresse/port destination autorisées par les Règles de filtrage*].

Juste un exemple: Politique de contrôle de flux traversants

- FDP_IFC.1

- FDP_IFC.1.1 La TSF doit appliquer la [*Politique filtrage flux traversants*] aux [*Trames IP*].

- FDP_IFF.1

- FDP_IFF.1.1 La TSF doit appliquer la [*Politique filtrage flux traversants*] en fonction des types suivants de sujets et d'attributs de sécurité :
[*Trames IP : adresse/port source, adresse/port destination*]
- FDP_IFF.1.2 La TSF doit autoriser un flux d'information entre un sujet et des informations par l'intermédiaire d'une opération contrôlée si les règles suivantes s'appliquent:
[*Trames IP : adresse/port source, adresse/port destination autorisées par les Règles de filtrage*].

Politique de contrôle de flux traversants

1. ALLOW + LOG

source_IP = 192.168.1.*, (wan)

source_port = *,

destination_IP = 192.168.2.127, (serveur web)

Destination_port = tcp 80 (http)

2. ALLOW + LOG

source_IP = 192.168.3.*, (lan)

source_port = *,

destination_IP = 192.168.1.*, (wan)

Destination_port = *

3. DENY ALL

Politique de contrôle de flux entrants

- 1. ALLOW + LOG
 - source_IP = 192.168.3.*, (lan)
 - source_port = *,
 - destination_IP = 192.168.3.2, (TOE)
 - Destination_port = tcp 8443 (https)

- 2. DENY ALL

Traduction des objectifs de sécurité en SFR

- ■ Je vous épargne la suite ...

Résumé des spécifications fonctionnelles

SFR	Fonctions présentes dans la TOE
FDP_IFC.1, FDP_IFF.1 / trames traversantes	Filtrage à l'aide du programme iptables (règles FORWARD)
FDP_IFC.1, FDP_IFF.1 / trames entrantes	Filtrage à l'aide du programme iptables (règles INPUT)
FAU_GEN.1	Journalisation syslog
FIA_UAU.1	Authentification par login / mot de passe

Agenda

- Rédiger la cible de sécurité
- **Analyser le process de développement**
- Analyser des spécifications fonctionnelles
- Analyser des documents de conception
- Analyser le code source
- Tests fonctionnels
- Tests de vulnérabilités

ALC: évaluation du cycle de vie de la TOE

- - Modèle de cycle de développement (ALC_LCD)
 - Produit open-source
 - Production de release
 - Gestion de configuration (ALC_CMC, ALC_CMS)
 - Tout (code source + documentation) dans un dépôt Subversion chez SourceForge
 - Sécurité de l'environnement de développement (ALC_DVS)
 - Gestion des accès aux serveurs hébergeant le dépôt SVN: ??? il faudrait demander à SourceForge
 - Sécurité de la procédure de livraison (ALC_DEL)
 - Téléchargement du code (svn://) non protégé (FAIL) puis recompilation par l'installateur
 - Téléchargement d'une image .iso (site non authentifié http:// FAIL)
 - Remontée des vulnérabilités et production des correctifs (ALC_FLR)
 - Points de contact présents sur le site ipcop.com mais aucun engagement de prise en compte des commentaires envoyés

Avis du CESTI

- ■ Risques sur l'intégrité du code source récupéré
 - Il faut faire confiance à Sourceforge
 - Risque de faux dépôt Sourceforge
 - Pas de protection du flux de téléchargement (cf. TOR)

- ISO d'installation directement récupérée
 - Aucune confiance

Agenda

- Rédiger la cible de sécurité
- Analyser le process de développement
- **Analyser des spécifications fonctionnelles**
- Analyser des documents de conception
- Analyser le code source
- Tests fonctionnels
- Tests de vulnérabilités

Tâche ADV_FSP

- ■ Objectifs

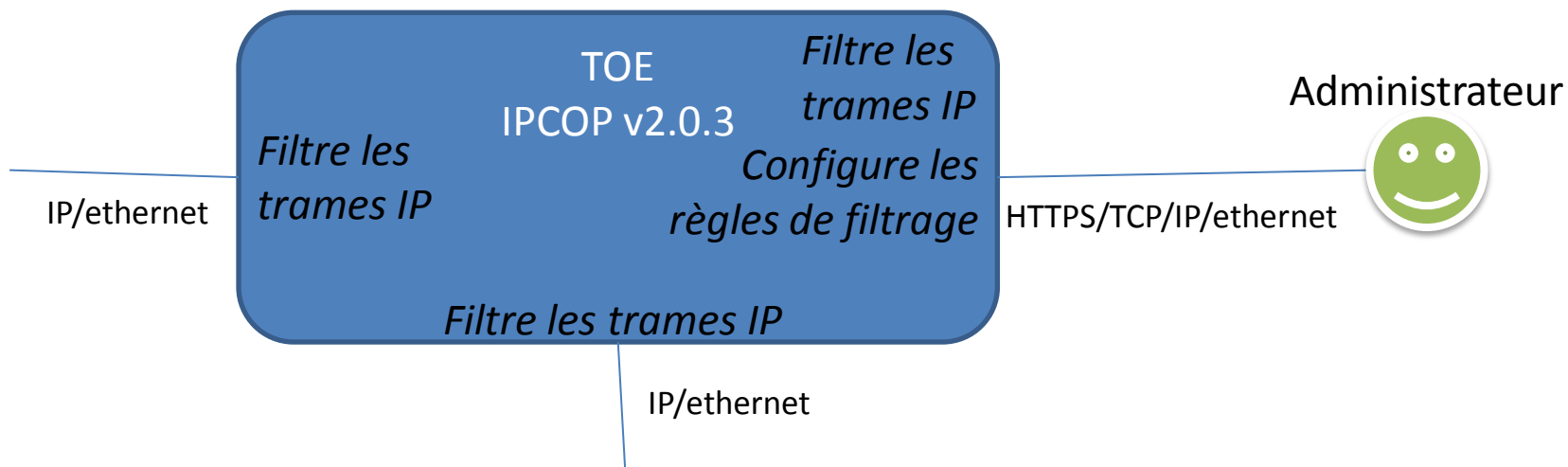
- Comprendre les moyens d'interagir avec la TOE
- Comprendre quand sont déclenchées les fonctions de sécurité?

- Données d'entrée

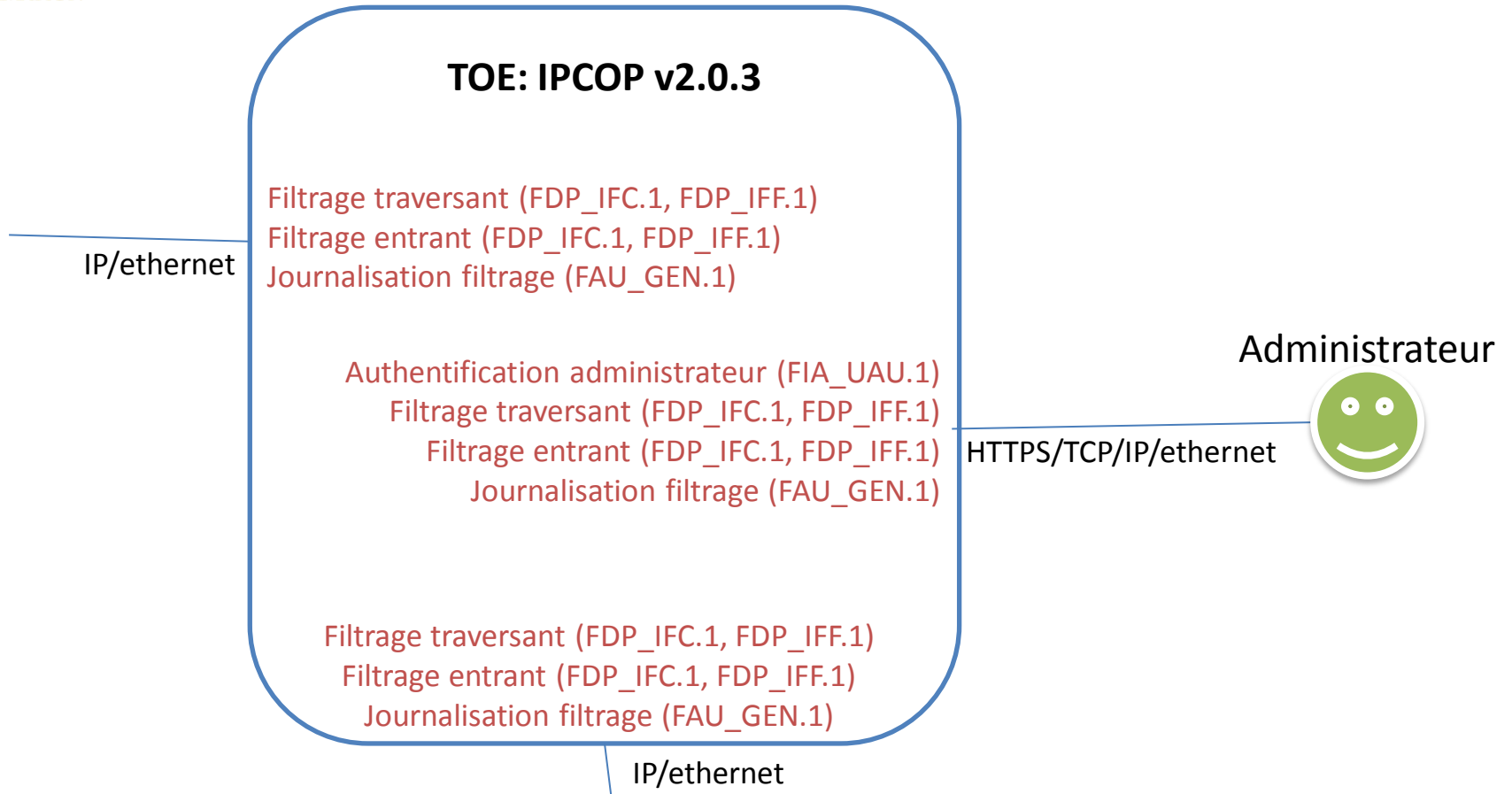
- Documents de spécifications fonctionnelles fournis par le développeur de la TOE

ADV_FSP: Interfaces et actions

- Rappelez-vous les Sujets/Opérations/Objets



ADV_FSP: mapping avec les exigences fonctionnelles



Avis du CESTI

- Les fonctions déclarées dans la cible de sécurité ont l'air d'être présentes

Agenda

- Rédiger la cible de sécurité
- Analyser des spécifications fonctionnelles
- **Analyser des documents de conception**
- Analyser le code source
- Tests fonctionnels
- Tests de vulnérabilités

Tâche ADV_TDS

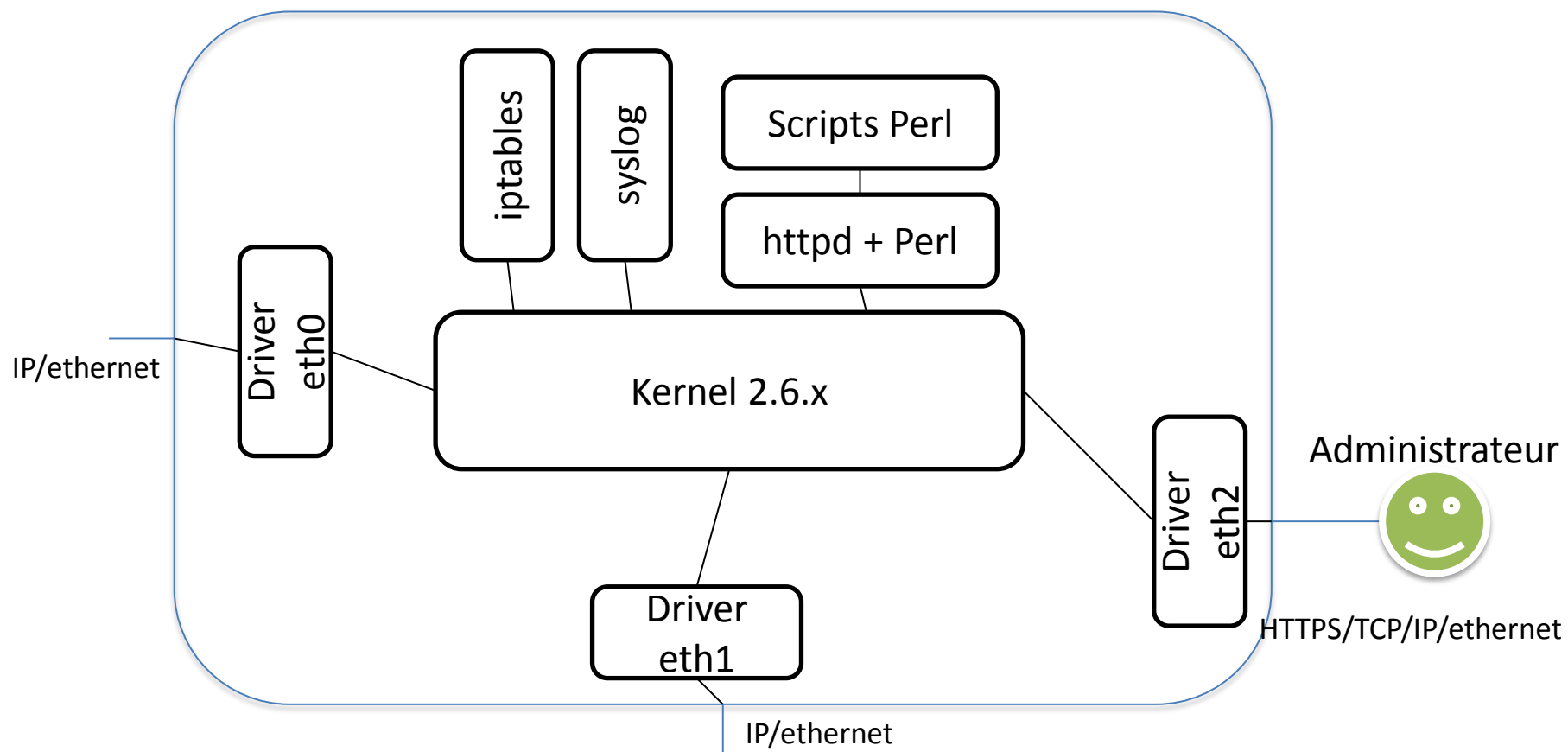
■ ■ Objectifs

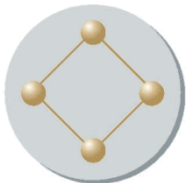
- Comprendre l'architecture de la TOE
- Identifier où sont implémentées les fonctions de sécurité

■ Données d'entrée

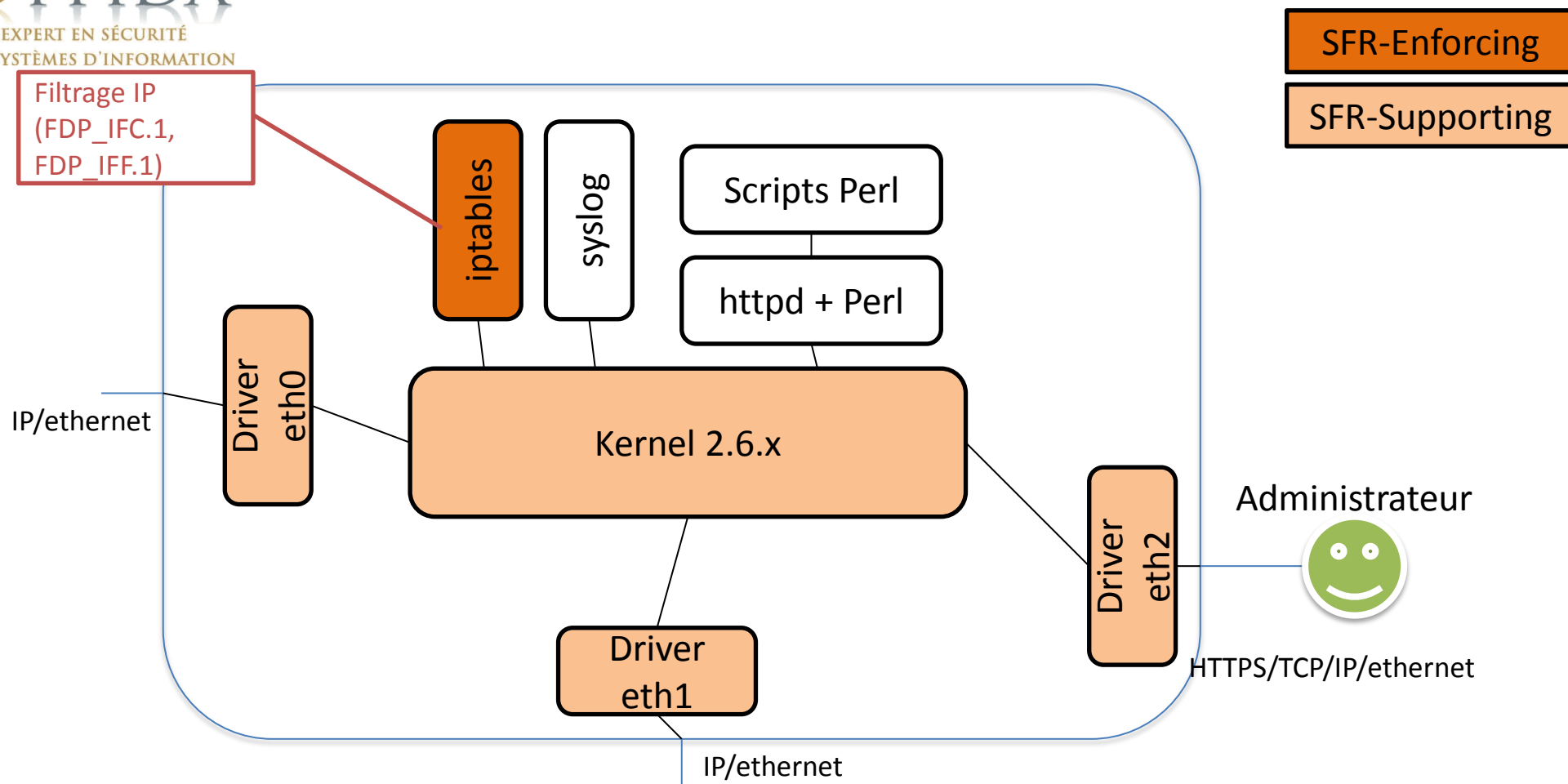
- Documents de description de la conception de la TOE fournis par le développeur
 - On imagine que ces documents existent ;-)

ADV_TDS: décomposition en sous-systèmes et modules

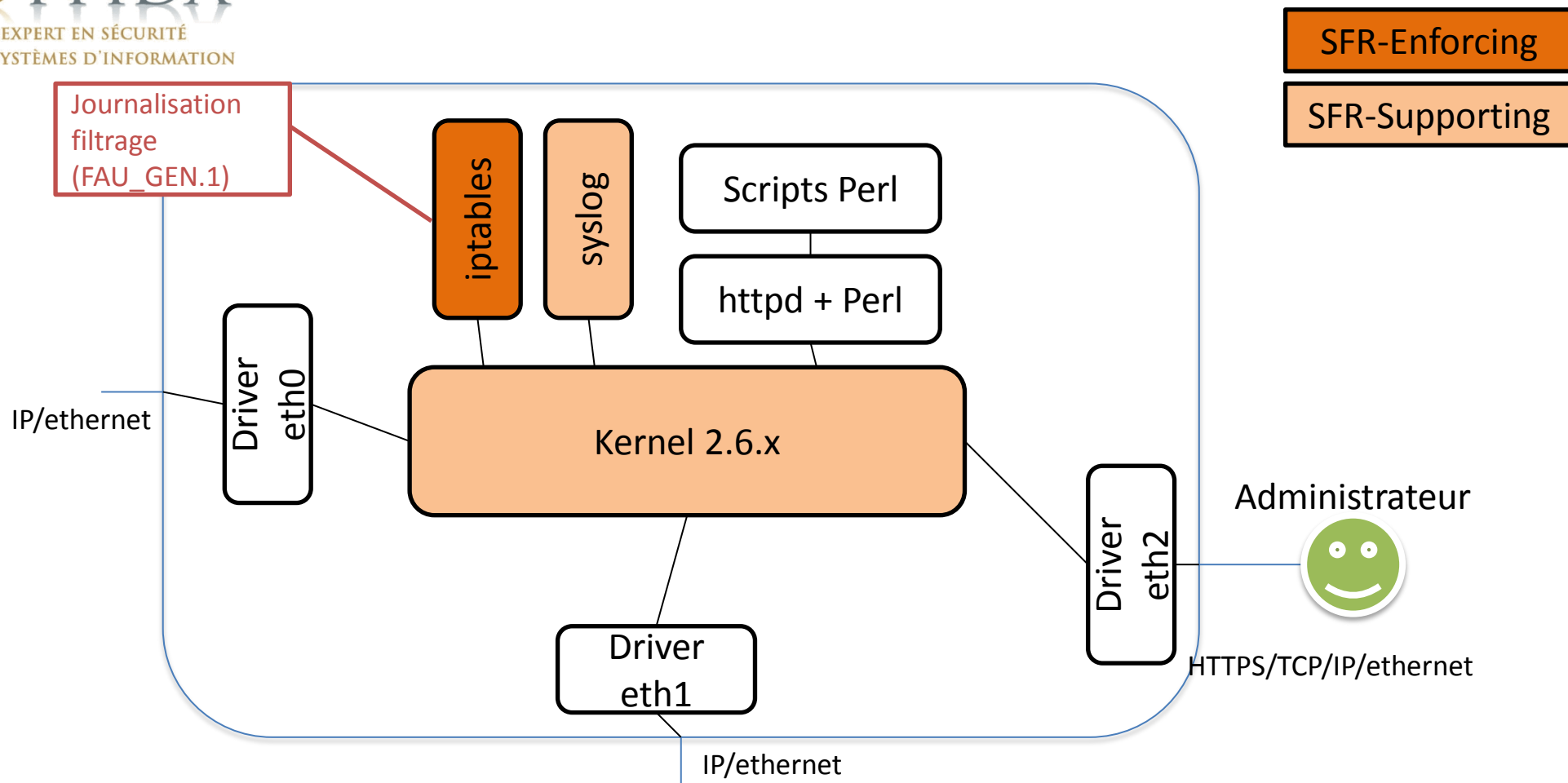




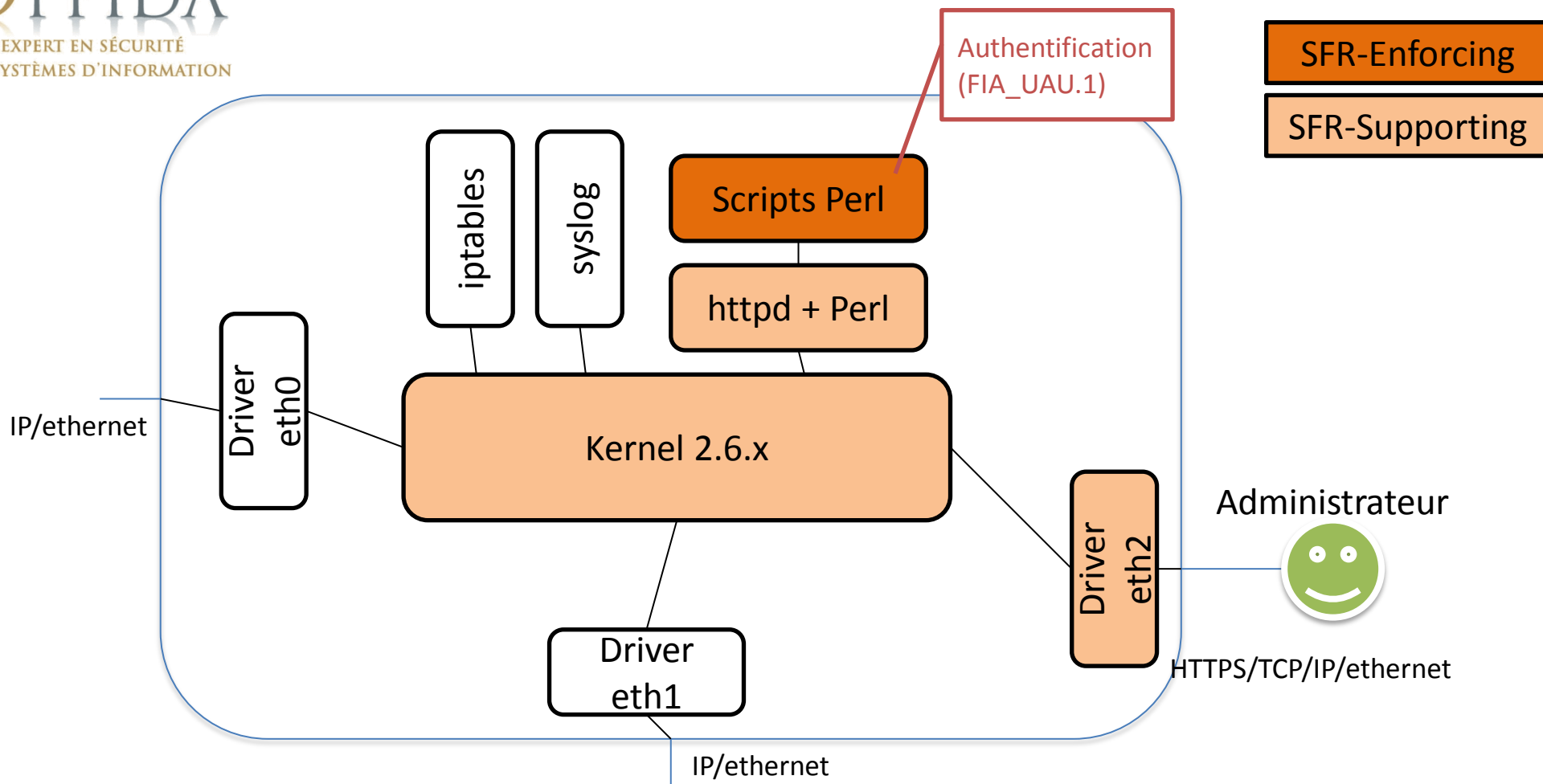
Délimitation de la TSF: Filtrage IP



Délimitation de la TSF: Journalisation



Délimitation de la TSF: Authentification



Agenda

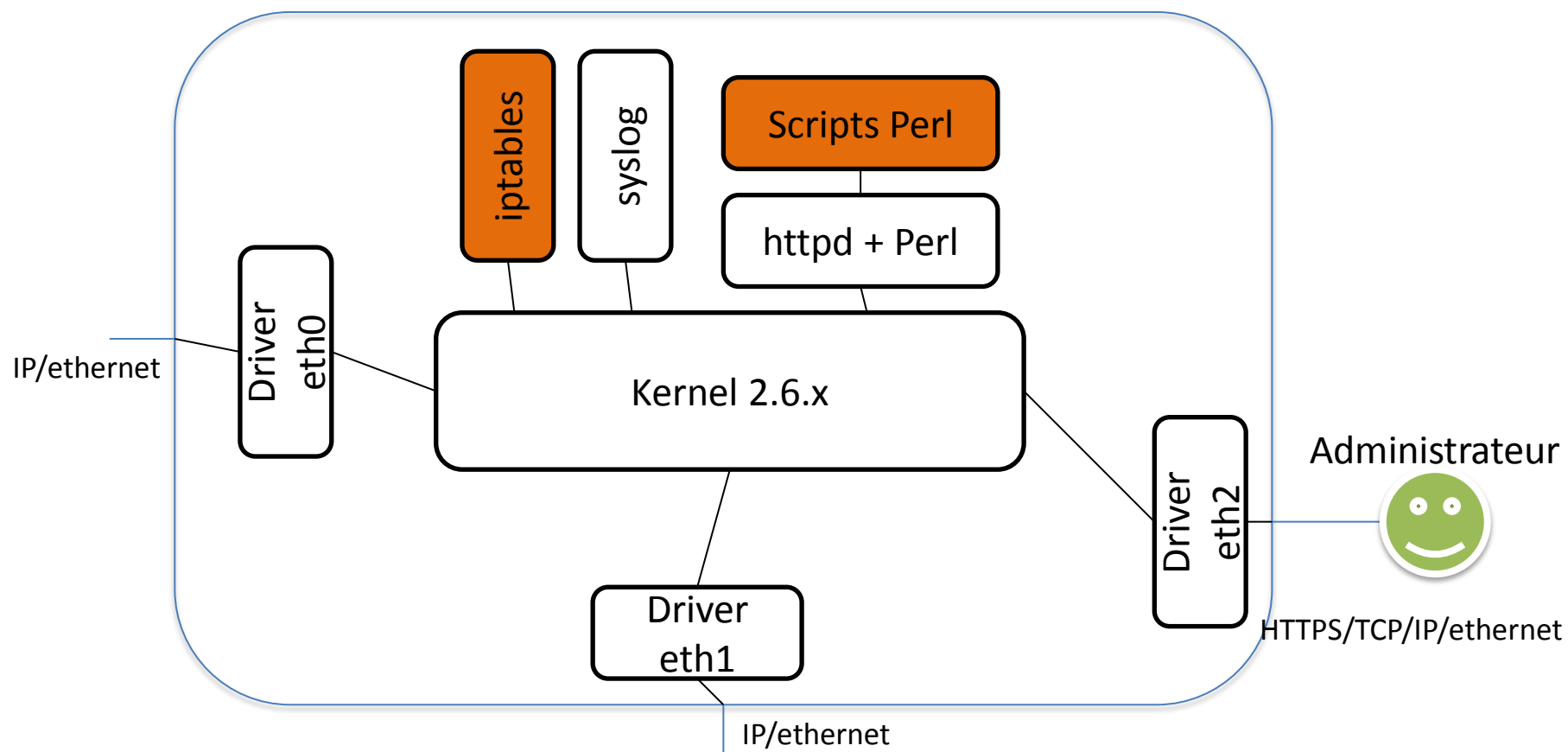
- - Rédiger la cible de sécurité
 - Analyser des spécifications fonctionnelles
 - Analyser des documents de conception
 - Analyser le process de développement
 - **Analyser le code source**
 - Tests fonctionnels
 - Tests de vulnérabilités

ADV_IMP: TSF implementation

- ■ Conformité
 - Vérifier la réalisation effective des SFR
 - Code source
 - Configuration
- À partir du niveau EAL4 seulement

ADV_IMP: TSF implementation

SFR-Enforcing



ADV_IMP: TSF implementation

- ■ Filtrage & journalisation
 - Réalisation dépend de la configuration: `iptables -L`
- Authentification
 - Réalisation dans le code source: scripts cgi-Perl
 - `\html\cgi-bin\webaccess.cgi`

Avis du CESTI

- Les fonctions déclarées dans la cible de sécurité sont bien présentes dans le produit

Agenda

- - Rédiger la cible de sécurité
 - Analyser le process de développement
 - Analyser des spécifications fonctionnelles
 - Analyser des documents de conception
 - Analyser le code source
- **Tests fonctionnels**
 - Tests de vulnérabilités

- 1. Valider le plan de tests du développeur
 - 1. Il existe?
 - 2. La couverture des fonctions de sécurité est-elle complète?

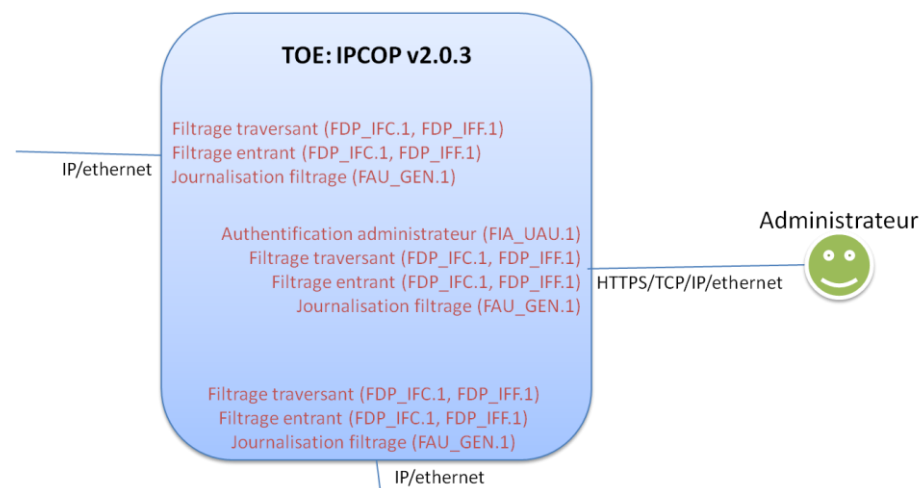
- 2. Réaliser des tests indépendants
 - 1. Rejeu d'une partie des tests fournis par le développeur
 - 2. Elaboration de nouveaux tests

Plan de tests fonctionnels indépendant

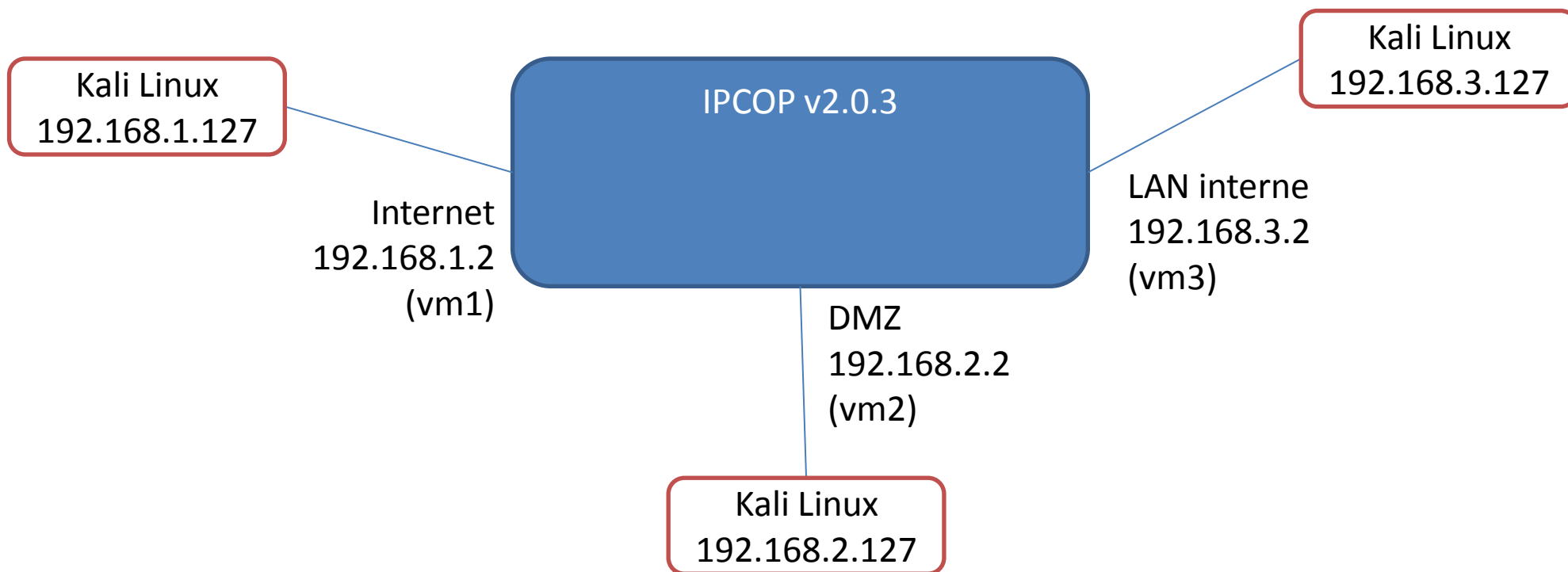
- Vérifier [Filtrage traversant] sur [Interface WAN]
- Vérifier [Filtrage entrant] sur [Interface WAN]
- Vérifier [Journalisation filtrage] sur [Interface WAN]

- Vérifier [Filtrage traversant] sur [Interface DMZ]
- Vérifier [Filtrage entrant] sur [Interface DMZ]
- Vérifier [Journalisation filtrage] sur [Interface DMZ]

- Vérifier [Authentification administrateur] sur [Interface LAN]
- Vérifier [Filtrage traversant] sur [Interface LAN]
- Vérifier [Filtrage entrant] sur [Interface LAN]
- Vérifier [Journalisation filtrage] sur [Interface LAN]



Plateforme de tests



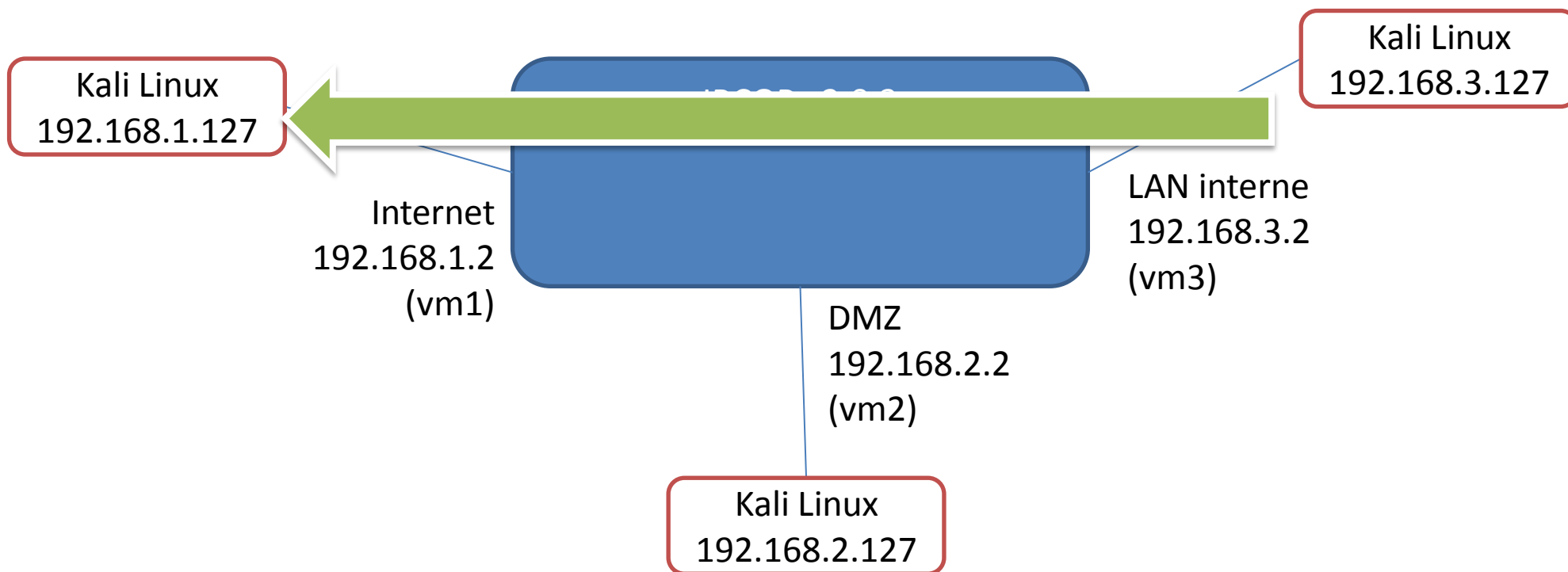
- ■ Kali.org
- Tutos en français sur <http://www.kali-linux.fr/>
- Distribution Debian Linux (ex Backtrack) contenant la plupart des outils de tests préinstallés

Wireshark

- Wireshark.org
- Analyseur de paquets

- <http://www.secdev.org/projects/scapy/>
- Outil de génération de paquet en python
- Principales commandes:
 - ls() pour lister les attributs modifiables pour le protocole
 - Ex: ls(IP), ls(TCP)
 - a=IP()/TCP()
 - a.show()
 - a.dst= "192.168.2.127"
 - send(a)
 - Envoi uniquement
 - b=sr1(a)
 - Envoi et récupération de la réponse
 - b.show()

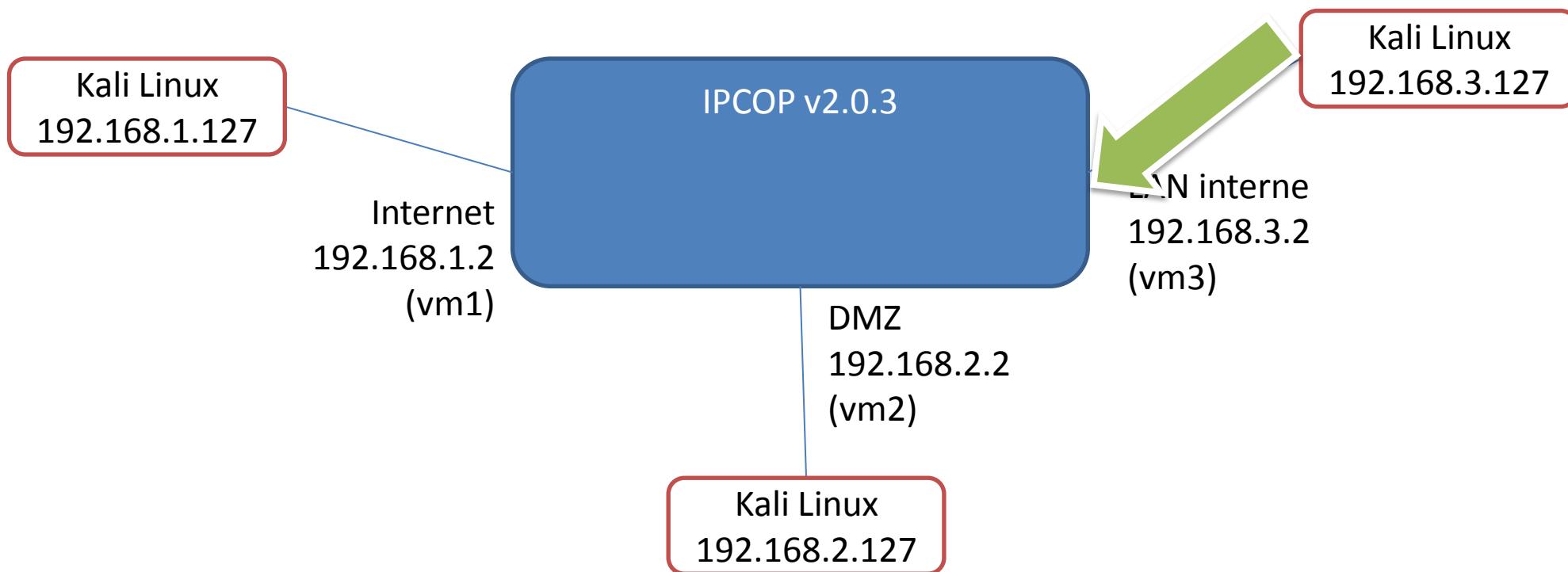
Test : filtrage interne -> wan



Test du filtrage

- ■ Utilisation de scapy pour envoyer des trames TCP
 - `send(IP(dst="192.168.1.127")/TCP(dport=(1,35635)))`
- Utilisation de wireshark sur la machine destination pour voir ce qui passe

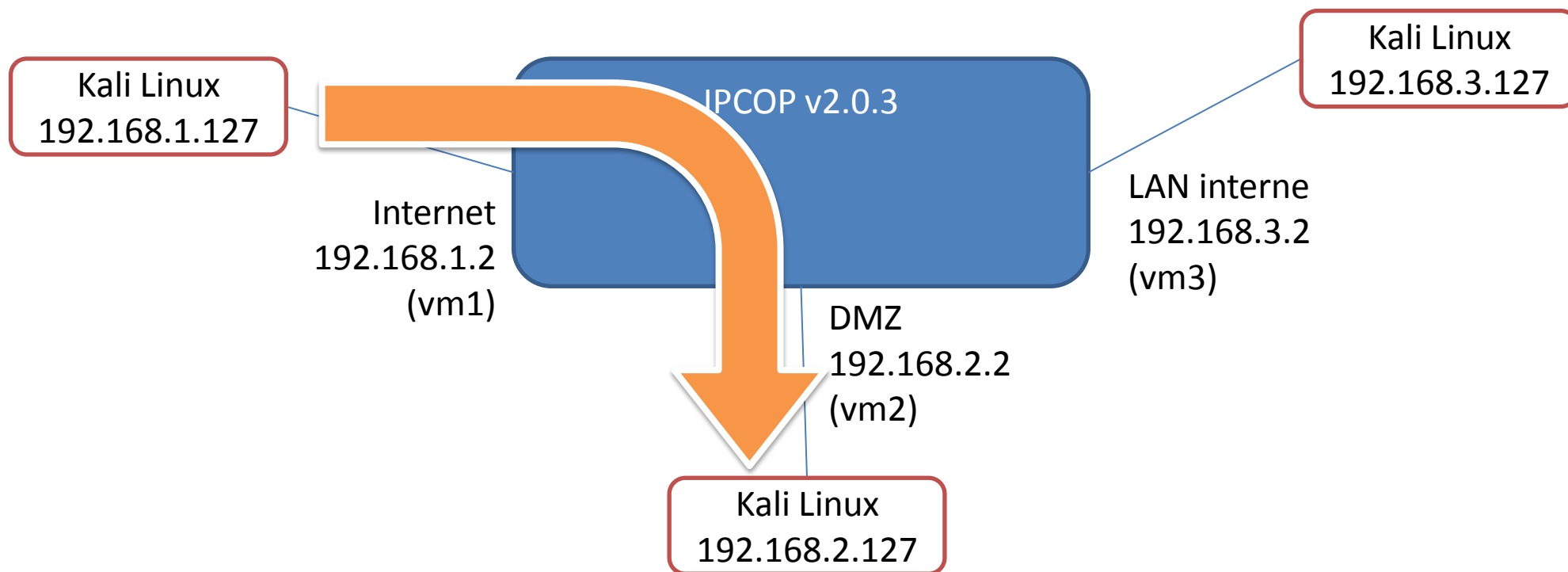
Test : Authentification interface interne



Test de l'authentification de l'interface d'administration





- ■ Connexion sur l'interface d'administration
<https://192.168.3.2:8443/>
 - Vulnérabilité 1: certificat autosigné => risque d'usurpation
- Tentative de présentation d'un mot de passe
 - vide
 - random

Test : règles de filtrage WAN -> DMZ



Test filtrage WAN -> DMZ

Transferts de ports:

#	Réseau Interface	Source	Réseau Interface	Destination interne	Remarque	Action
1	Tout	Any	➡ ORANGE	192.168.2.127 : http		<input checked="" type="checkbox"/>    

- Utilisation de scapy pour envoyer des trames TCP
 - `send(IP(dst="192.168.2.127")/TCP(dport=(1,35635)))`
- Utilisation de wireshark sur la machine destination pour voir ce qui passe

Agenda

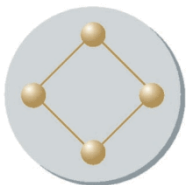
- Rédiger la cible de sécurité
- Analyser le process de développement
- Analyser des spécifications fonctionnelles
- Analyser des documents de conception
- Analyser le code source
- Tests fonctionnels
- **Tests de vulnérabilités**

Organisation de l'analyse de vulnérabilités

- 1. Vulnérabilités connues
- 2. Analyse indépendante de vulnérabilités
 - 1. Brainstorming, base de connaissances
 - 2. Tests

Vulnérabilités connues

- ■ Pour la TOE
- ■ Pour des composants intégrés dans la TOE
- ■ Base CVE
 - cvedetails.com
 - Securityfocus
 - ...



OPPIDA CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#)

[Home](#)
Browse :

[Vendors](#)
[Products](#)
[Vulnerabilities By Date](#)
[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)
[CVSS Score Distribution](#)

Search :

[Vendor Search](#)
[Product Search](#)
[Version Search](#)
[Vulnerability Search](#)
[By Microsoft References](#)

Top 50 :

[Vendors](#)
[Vendor Cvss Scores](#)
[Products](#)
[Product Cvss Scores](#)
[Versions](#)

Other :

[Microsoft Bulletins](#)
[Bugtraq Entries](#)
[CWE Definitions](#)
[About & Contact](#)
[Feedback](#)
[CVE Help](#)
[FAQ](#)
[Articles](#)

cvedetails

Google™ Custom Search

Search

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View CVE

Vulnerability Feeds & Widgets [New](#) www.itsecdb.com

Ipcop : Vulnerability Statistics

[Products \(2\)](#) [Vulnerabilities \(5\)](#) [Search for products of Ipcop](#) [CVSS Scores Report](#) [Possible matches for this vendor](#) [Related Metasploit Modules](#)

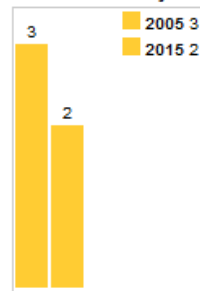
[Vulnerability Feeds & Widgets](#)

Vulnerability Trends Over Time

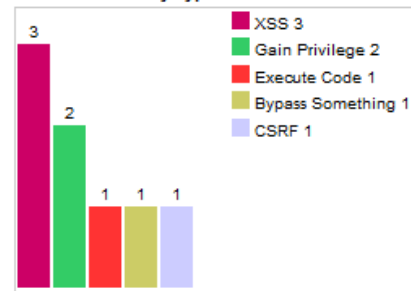
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2005	3						1					2			
2015	2		1				2			1			1		
Total	5		1				3			1		2	1		
% Of All		0.0	20.0	0.0	0.0	0.0	60.0	0.0	0.0	20.0	0.0	40.0	20.0	0.0	

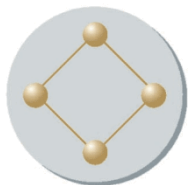
Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year



Vulnerabilities By Type





Ipcop : Security Vulnerabilities

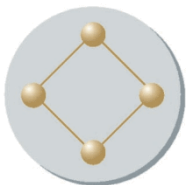
CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#) [Select Table](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-7418	77		Exec Code XSS	2015-01-02	2015-01-05	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
cgi-bin/iptablesgui.cgi in Ipcop (aka Ipcop Firewall) before 2.1.5 allows remote authenticated users to execute arbitrary code via shell metacharacters in the TABLE parameter. NOTE: this can be exploited remotely by leveraging a separate cross-site scripting (XSS) vulnerability.														
2	CVE-2013-7417	79		XSS Bypass CSRF	2015-01-02	2015-01-05	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in cgi-bin/ipinfo.cgi in Ipcop (aka Ipcop Firewall) before 2.1.3 allows remote attackers to inject arbitrary web script or HTML via the QUERY_STRING. NOTE: this can be used to bypass the cross-site request forgery (CSRF) protection mechanism by setting the Referer.														
3	CVE-2005-4660			+Priv	2005-12-31	2008-09-05	1.2	None	Local	High	Not required	None	Partial	None
Race condition in Ipcop (aka Ipcop Firewall) before 1.4.10 might allow local users to overwrite system configuration files and gain privileges by replacing a backup archive during the time window when the archive is owned by "nobody" but not yet encrypted, then executing ipcoprsfsg to restore from this backup.														
4	CVE-2005-4659			+Priv	2005-12-31	2008-09-05	2.1	None	Local	Low	Not required	Partial	None	None
Ipcop (aka Ipcop Firewall) before 1.4.10 has world-readable permissions for the backup.key file, which might allow local users to overwrite system configuration files and gain privileges by creating a malicious encrypted backup archive owned by "nobody", then executing ipcoprsfsg to restore from this backup.														
5	CVE-2004-1210			XSS	2005-01-10	2008-09-05	6.8	User	Remote	Medium	Not required	Partial	Partial	Partial
Cross-site scripting (XSS) vulnerability in proxylog.dat in Ipcop 1.4.1 and possibly other versions, allows remote attackers to inject arbitrary web script or HTML via the (1) url or (2) part variables.														

Total number of vulnerabilities : 5 Page : 1 (This Page)



CVE-2013-7417

Vulnerability Details : [CVE-2013-7417](#)

Cross-site scripting (XSS) vulnerability in cgi-bin/ipinfo.cgi in IPCop (aka IPCop Firewall) before 2.1.3 allows remote attackers to inject arbitrary web script or HTML via the QUERY_STRING. NOTE: this can be used to bypass the cross-site request forgery (CSRF) protection mechanism by setting the Referer.

Publish Date : 2015-01-02 Last Update Date : 2015-01-05

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [▼ Scroll To](#) [▼ Comments](#) [▼ External Links](#)

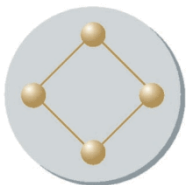
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

– CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Cross Site Scripting Bypass a restriction or similar CSRF
CWE ID	79

– Products Affected By CVE-2013-7417

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Ipcop	Ipcop	2.1.2				Version Details Vulnerabilities



OPPIDA

CVE-2013-7418

Vulnerability Details : [CVE-2013-7418](#)

cgi-bin/iptablesgui.cgi in IPCop (aka IPCop Firewall) before 2.1.5 allows remote authenticated users to execute arbitrary code via shell metacharacters in the TABLE parameter. NOTE: this can be exploited remotely by leveraging a separate cross-site scripting (XSS) vulnerability.

Publish Date : 2015-01-02 Last Update Date : 2015-01-05

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [▼ Scroll To](#) [▼ Comments](#) [▼ External Links](#)

[Search Twitter](#) [Search YouTube](#) [Search Google](#)

– CVSS Scores & Vulnerability Types

CVSS Score	6.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
Gained Access	None
Vulnerability Type(s)	Execute Code Cross Site Scripting
CWE ID	77

– Products Affected By CVE-2013-7418

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Ipcop	Ipcop	2.1.4				Version Details Vulnerabilities

Des exploits disponibles

- Sur <http://packetstormsecurity.com/>

Tests de vulnérabilités indépendants

- ■ Définir les points d'attaque
 - WAN
 - DMZ
 - LAN

- Méthodologie tests d'intrusion
 - Collecte d'information
 - Recherche de points faibles
 - Attaque
 - Camouflage

« THE outil » pour la collecte d'info : NMAP



- ■ nmap.org
- Liste de principaux ports ouverts
 - nmap @IP
 - Ne pas oublier que tous les ports ne sont pas testés, et qu'il ne s'agit que de TCP
- Reconnaissance de l'OS
 - nmap -O --osscan-guess @IP
- Utilisation des scripts installés sur la machine du testeur
 - nmap -A @IP

À partir du LAN

- ■ *Nmap*
 - dnsmasq-2.59
 - OpenSSH 5.9
 - Attention aux tailles des clés SSH
- *sslyze*
 - sslyze –regular @IP
 - Récupération des suites SSL supportées et des certificats présentés
- *nikto*
 - nikto -port 8443 -h 192.168.3.2
 - Scanner web basique (pas très performant, beaucoup de faux-positifs)
 - Lui préférer *burp*, *qualys*, *arachni*, *acunetix*, ...

À partir du WAN

- ■ *Nmap*
 - SSH en écoute sur TCP/8022
- Attaque authentification SSH
 - Attaque par dictionnaire (wordlist.txt)
 - *medusa*
 - `medusa -h 192.168.1.2 -n 8022 -M ssh -u root -P wordlist.txt`
 - Pour les serveurs connectés sur internet, ne vous inquiétez pas, quelqu'un l'a déjà fait pour vous

Cotation de l'attaque

- ■ Besoin d'évaluer le niveau de complexité de l'attaque
- Permet d'en déduire le niveau de résistance de la TOE
 - AVA_VAN.1: résistance aux CVE publiées
 - AVA_VAN.2: résistance aux attaques de niveau *basic* (boite noire)
 - AVA_VAN.3: résistance aux attaques de niveau *enhanced-basic* (l'attaquant a le code source)
 - AVA_VAN.4: résistance aux attaques de niveau *moderate*
 - AVA_VAN.5: résistance aux attaques de niveau *high*

Table de cotation des attaques: CEM

- ■ CEM annexe B.4 (p428/433)
 - *Elapsed Time*: temps passé à trouver + exploiter la vulnérabilité
 - *Expertise*: type de compétence nécessaire (identification et exploitation)
 - *Knowledge of TOE*: connaissance du produit nécessaire
 - *Window of Opportunity*: difficulté d'accès au produit
 - *Equipment*: type d'outils nécessaires (identification et exploitation)

Sur un exemple

■ Attaque par dictionnaire sur SSH

Facteur	Valeur	Cotation
Elapsed Time	10 minutes (< 1 day)	0
Expertise	Compétent (proficient)	3
Knowledge of TOE	Adresse IP (public)	0
Window of Opportunity	Accès au WAN + connectivité IP (easy)	1
Equipment	Spécialisé (specialised)	4

■ Total = 8

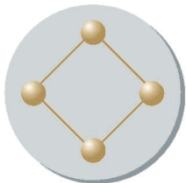
Cotation de l'attaque

Values	Attack potential required to exploit scenario:	TOE resistant to attackers with attack potential of:	Meets assurance components::	Failure of components:
0-9	Basic	No rating	-	AVA_VAN.1 , AVA_VAN.2 , AVA_VAN.3 , AVA_VAN.4 , AVA_VAN.5
10-13	Enhanced-Basic	Basic	AVA_VAN.1 , AVA_VAN.2	AVA_VAN.3 , AVA_VAN.4 , AVA_VAN.5
14-19	Moderate	Enhanced	AVA_VAN.1	AVA_VAN.4

- La TOE ne satisfait pas les exigences AVA_VAN.1
 - Il faut modifier le produit OU il faut ajouter dans la cible de sécurité une hypothèse (choix d'un mot de passe complexe par l'administrateur)

Cotation des vulnérabilités

- ■ La liste de toutes les vulnérabilités trouvées est fournie dans le Rapport Technique d'Evaluation
 - mais pas dans la version publique: le rapport de certification
- Vulnérabilité exploitable
 - Pas de certificat
- Vulnérabilité résiduelle
 - Niveau de complexité de l'attaque > niveau AVA_VAN demandé
 - Hypothèse de la cible de sécurité empêche l'exploitation
 - D'où l'importance de lire la cible de sécurité et de respecter les hypothèses



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Des questions ?

OPPIDA recrute :

- pour du pentest
- pour du reverse
- pour de l'expertise crypto
- pour des évaluations CSPN et CC

Conseil & Expertise
en sécurité des systèmes d'information



contact@oppida.fr