Scholanova

Apprendre ensemble

BTS Services informatiques aux organisations :

Devoir sur Table

Cas Saint-Jacques

2023-2024

Table des matières

1 Mission B1 Protection contre les rançongiciels

1.1 Question B1.1 Équipements pouvant être infectés par un rançongiciel

- Postes de travail (ordinateurs fixes et portables)
- Serveurs (fichiers, Active Directory, Hyper-V, etc.)
- Supports amovibles (clés USB, disques externes)
- Stockages en réseau (NAS, SAN)
- Équipements réseau et IoT (moins courant, mais possible)

Remarques : Les répertoires partagés et les sauvegardes sont souvent ciblés pour maximiser l'impact.

1.2 Question B1.2 Impacts directs pour les utilisateurs

- **Agents** : interruption des services, impossibilité de traiter les dossiers.
- **Citoyens** : indisponibilité des services publics en ligne (état civil, paiements, etc.)
- **Services critiques** : dysfonctionnements graves (paie, élections, cadastre).
- **Informaticiens** : mobilisation pour contenir l'attaque, restaurer les données, analyser.

Remarques : Peut provoquer une perte de confiance, une pression médiatique ou politique.

1.3 Question B1.3 Prévention des infections via clé USB

- Désactiver les ports USB non autorisés via GPO ou BIOS.
- Activer la protection antivirus sur supports amovibles.
- Mettre en place un outil de "Device Control" (contrôle des périphériques).

Remarque : Utiliser des sessions utilisateurs sans privilèges réduit le risque d'infection. **Remarque 2 :** Voir Annexe 1

1.4 Question B1.4 Limiter la propagation via lien piégé

- Filtrage des courriels malveillants (anti-phishing/antispam).
- Formation des agents à l'hygiène numérique.
- Mise à jour régulière des postes et applications.
- Filtrage DNS ou proxy bloquant les domaines malveillants.

Remarque : Un EDR (Endpoint Detection and Response) détecte l'exécution anormale d'outils comme Mimikatz ou Metasploit. **Remarque 2 :** Voir Annexe 2 et 3

1.5 Question B1.5 Notification RGPD

a) Processus juridique :

- Notification à la CNIL dans les 72h.
- Notification aux personnes concernées si risque élevé.
- Enregistrement de la violation dans le registre des incidents.

b) Objectifs de la procédure :

- **CNIL** : contrôle des bonnes pratiques et potentielle sanction.
- **Personnes concernées** : anticipation des conséquences (ex. : usurpation).
- **Organisation** : conformité et réactivité.

1.6 Question B1.6 Limiter la navigation à certains sites

Exemple : utilisation d'un proxy filtrant ou d'un DNS sécurisé.

- **Proxy** : intercepte les requêtes HTTP/S et applique des politiques de filtrage (catégories de sites, réputation, liste blanche).

— **DNS filtrant** : bloque la résolution DNS des domaines malveillants ou non autorisés (ex : OpenDNS, NextDNS).

Remarque : Ces dispositifs peuvent être intégrés à des firewalls de nouvelle génération (UTM), voir Annexe 4

2 Mission B2 Sécurisation des liaisons avec les sites distants

2.1 Question B2.1 Objectifs de sécurité d'un VPN

Un VPN garantit plusieurs objectifs essentiels :

— **Confidentialité** : les données échangées sont chiffrées (personne ne peut les lire).
— **Authentification** : chaque extrémité est vérifiée (certificats, PSK).
— **Intégrité** : les données ne sont pas altérées durant leur transmission.
— **Non-répudiation** (dans certains cas) : on peut prouver qu'un message provient bien de l'émetteur.

Complément : En plus de sécuriser les échanges, un VPN peut contribuer à la continuité d'activité (ex. réplication Hyper-V), voir Annexe 5.

2.2 Question B2.2 Schéma de fonctionnement des clés symétriques

Chaque extrémité possède :

— Une clé pour **chiffrer** les données sortantes (ex : ESP-SA1 ou CHILD-SA1).
— Une clé pour **déchiffrer** les données entrantes (ex : ESP-SA2 ou CHILD-SA2).

Principe :

```
[Site A] --(Clé A->B)---> Donnée chiffrée ---(Clé A->B)---> [Site B]
<--(Clé B->A)--- Donnée chiffrée <---(Clé B->A)---
```

Remarque : Chaque canal est unidirectionnel et possède sa propre association de sécurité (SA), voir Annexe 6.

2.3 Question B2.3 Avantages d'une IGC (PKI) face au PSK

a) Objectif d'une IGC :

— Gérer des certificats (création, révocation, renouvellement).
— Assurer la **confiance** dans les identités numériques (authentification).

b) Pourquoi préférer une IGC à une PSK :

— **Scalabilité** : facile d'ajouter un nouvel équipement (pas besoin de distribuer la clé à tous).
— **Sécurité** : les certificats sont plus difficiles à voler, peuvent être rapidement révoqués.
— **Auditabilité** : on peut tracer les accès et gérer les certificats de façon centralisée.
— **PSK** : vulnérable à la divulgation, peu adapté à un environnement en production.

Remarque : L'ANSSI recommande fortement d'éviter les PSK sauf pour des tests ou dans un cadre très contrôlé. **Remarque 2 :** Voir Annexe 7.

3 Mission B3 Mise en oeuvre du télétravail

Question B3.1 Modification des règles de filtrage VPN nomade

Objectif : restreindre l'accès au seul site : https://collab.saintjacques.fr pour deux utilisateurs.
Proposition de modification :

— Créer un objet représentant lURL `collab.saintjacques.fr`.

- Créer un groupe d'utilisateurs contenant Denis Barbier et Bruno Paillard.
- Ajouter une règle dans le pare-feu :
  - Source : groupe des utilisateurs.
  - Destination : objet URL.
  - Service : HTTPS (TCP 443).
  - Action : autoriser.
- Ajouter ensuite une règle explicite interdisant tout autre trafic pour ces mêmes utilisateurs.

Remarque : On peut aussi utiliser des profils daccès par utilisateur sur le firewall Stormshield pour appliquer dynamiquement ces règles.

Question B3.2 Avantage de lauthentification par certificat en cas de vol

Réponse :
- Le certificat installé sur le poste permet dauthentifier la machine ou l'utilisateur.
- En cas de vol, on peut **révoquer le certificat** associé via la PKI.
- Cela bloque immédiatement tout accès distant, même si le mot de passe est connu.

Remarque :
- La PKI permet une gestion fine des accès (expiration, révocation, renouvellement).
- Les certificats sont beaucoup plus difficiles à dupliquer quun simple mot de passe.

Remarque : Voir Annexe 8.

4 Annexe 1 : Protection du BOIS

Le mot de passe du BIOS (Basic Input/Output System) est une fonction de sécurité conçue pour empêcher tout accès non autorisé lors du démarrage de l'ordinateur. Le mot de passe du BIOS est également appelé mot de passe de configuration du système, mot de passe UEFI, mot de passe de démarrage (BOOT) ou mot de passe de sécurité.

Lorsque l'appareil démarre, il demande à l'utilisateur de saisir le mot de passe du BIOS, et ce n'est qu'après avoir saisi le mot de passe correct que l'utilisateur peut accéder aux paramètres du BIOS, les modifier et accéder au système d'exploitation. Cela fournit une couche supplémentaire de sécurité pour empêcher les individus non autorisées de modifier les configurations matérielles ou le processus de démarrage.

Remarque : le BIOS est un micrologiciel qui s'exécute au démarrage de l'appareil, responsable de l'initialisation du matériel et du démarrage du système d'exploitation.

Vous pouvez définir trois types de mots de passe dans le BIOS : Mot de passe administrateur :

si seul le mot de passe administrateur est défini, l'accès au programme d'installation (BIOS ou UEFI) est limité. Vous devez saisir le mot de passe administrateur pour accéder au BIOS et modifier ses paramètres. Mot de passe utilisateur : si seul le mot de passe utilisateur est défini,

il sert de mot de passe de démarrage et vous devez saisir ce mot de passe lors du démarrage de Windows ou de l'entrée dans le BIOS. Dans les paramètres du BIOS, l'utilisateur disposera des droits d'administrateur. Remarque : Si le mot de passe administrateur et le mot de passe

utilisateur sont définis, lors de la saisie des paramètres du BIOS, vous devez saisir le mot de passe administrateur pour accéder aux paramètres du BIOS et les modifier. Si le mot de passe utilisateur est saisi, vous pouvez uniquement parcourir les paramètres du BIOS mais pas les modifier. Mot de passe du disque dur : si un mot de passe du disque dur est défini, lors du

démarrage de l'appareil ou de la saisie des paramètres du BIOS, le système vous demandera le mot de passe du disque dur. Ce n'est qu'après avoir entré le mot de passe correct que le

disque dur se déverrouillera, permettant à l'appareil de démarrer normalement ou d'accéder aux données stockées sur le disque dur.

5 Annexe 2 : EDR

5.0.1 1. Qu'est-ce qu'un EDR (Endpoint Detection and Response)

5.0.2 Définition

Un **EDR** est une solution de cybersécurité installée sur les *endpoints* (postes de travail, serveurs, ordinateurs portables). Il permet de **surveiller**, **détecter**, **analyser** et **répondre** aux activités suspectes ou malveillantes.

5.0.3 Fonctionnalités principales

— Surveillance en temps réel des activités sur les postes.
— Détection des comportements anormaux, même sans signature connue.
— Analyse post-incident (forensique) pour reconstituer l'attaque.
— Réaction automatique : isolation d'un poste, blocage de processus.
— Collecte de journaux pour enquête approfondie.

5.0.4 Différences avec un antivirus traditionnel

Antivirus classique	**EDR**
Détection par signatures	Détection comportementale
Réagit à des menaces connues	Détecte aussi des attaques inconnues (zero-day)
Protection passive	Réponse active à l'incident

5.1 2. Mimikatz

Définition

Mimikatz est un outil open source qui permet d'extraire des identifiants (mots de passe, hash NTLM, tickets Kerberos) depuis la mémoire d'un système Windows.

Utilisation en attaque

— Utilisé après une compromission (post-exploitation).
— Récupération de mots de passe en clair ou de hash.
— Attaques de type Pass-the-Hash ou Pass-the-Ticket.
— Escalade de privilèges sur la machine cible.

Détection par un EDR

L'EDR peut détecter Mimikatz en observant :
— Des accès anormaux à la mémoire système.
— Des appels suspects à l'API Windows.
— L'exécution d'un binaire connu ou signature comportementale.

3. Metasploit

Définition

Metasploit est un framework d'exploitation de vulnérabilités. Il permet de simuler des attaques pour tester la sécurité des systèmes.

Fonctionnalités

- Scan de vulnérabilités.
- Exploitation automatisée de failles.
- Déploiement de payloads (reverse shell, Meterpreter, etc.).
- Utilisé en test d'intrusion (pentest).

Utilisation malveillante

- Accès non autorisé à des systèmes vulnérables.
- Prise de contrôle à distance.
- Mouvement latéral dans un réseau.

Détection par un EDR

Un EDR peut repérer Metasploit en détectant :
- Des comportements d'exploitation typiques.
- Des connexions réseau inhabituelles.
- Des modèles de payloads connus.

6 Annexe 3 : Compléments EDR

6.1 L'analyse heuristique dans les EDR

6.1.1 Définition

L'**analyse heuristique** est une méthode de détection qui repose sur l'observation de comportements ou de patterns suspects, sans se limiter aux signatures connues. Elle est largement utilisée par les EDR (Endpoint Detection and Response).

6.1.2 Fonctionnement

Elle repose sur :
- des règles comportementales (*ex : un processus lit un mot de passe en mémoire*),
- des modèles d'apprentissage automatique (machine learning),
- des analyses statistiques et contextuelles.

6.1.3 Exemple

Un fichier Word s'ouvre, exécute une macro, télécharge un exécutable et l'exécute en mémoire. Aucun antivirus ne reconnaît ce fichier, mais un EDR, grâce à l'analyse heuristique, détecte cette séquence comme suspecte.

6.2 Comparaison entre EDR, IDS et IPS

6.2.1 Tableau comparatif

Critère	EDR	IDS	IPS
Nom complet	Endpoint Detection and Response	Intrusion Detection System	Intrusion Prevention System
Positionnement	Sur les postes ou serveurs	Réseau (NIDS) ou hôte (HIDS)	Principalement réseau
Mode de détection	Heuristique, comportementale, signatures	Signatures ou heuristique	Signatures ou heuristique
Réaction	Active (blocage, isolation, suppression)	Passive (alerte seulement)	Active (blocage de trafic)
Objectif principal	Réagir aux compromissions locales	Détecter les intrusions réseau ou système	Empêcher les intrusions en temps réel
Exemples de détection	Mimikatz, exécution anormale, exfiltration de données	Scan de ports, attaque brute force	Injection SQL, exploit connu
Limites	Nécessite des agents sur les endpoints	Ne bloque rien, dépend d'un humain	Risque de faux positifs ou de déni de service
Complémentarité	Avec antivirus, SIEM, firewall	Avec EDR, SIEM	Avec IDS, firewall

6.2.2 Complémentarité des outils

Ces outils ne sont pas exclusifs, ils se **complètent** :
- L'EDR agit sur les postes de travail.
- L'IDS surveille passivement le réseau.
- L'IPS bloque activement les menaces réseau.
- Le **SIEM** centralise et corrèle les alertes pour aider à la réponse globale.

6.2.3 Exemple de scénario d'attaque

1. Un utilisateur reçoit un fichier Word malveillant.
2. Il l'ouvre, une macro s'exécute, télécharge un binaire et l'exécute.
3. L'**EDR** détecte le comportement suspect et isole la machine.
4. Si l'attaque tente de contacter un serveur distant, l'**IPS** peut bloquer la connexion.
5. L'**IDS** peut également enregistrer le trafic pour analyse.
6. Le **SIEM** regroupe tous ces événements pour reconstituer l'incident.

7 Annexe 4 :

7.1 Quest-ce quun UTM (Unified Threat Management) ?

7.1.1 Définition

Un **UTM (Unified Threat Management)** est un **pare-feu de nouvelle génération** qui regroupe plusieurs fonctions de sécurité au sein dun même appareil ou logiciel. Il centralise la **protection réseau**, simplifie la gestion et améliore la visibilité sur les menaces.

7.1.2 Fonctionnalités typiques dun UTM

Un UTM peut inclure :

- **Pare-feu (Firewall)** : filtre les connexions entrantes et sortantes.
- **IDS/IPS** : détection et prévention des intrusions.
- **Antispam / Filtrage de mails** : bloque les courriers indésirables.
- **Filtrage web (URL)** : contrôle laccès à certains sites.
- **Antivirus réseau** : scanne les fichiers en transit.
- **VPN** : permet des connexions sécurisées à distance.
- **Contrôle des applications** : autorisation ou blocage dapplications réseau.
- **Logs et rapports** : centralisation des événements pour analyse.

7.2 Quest-ce quun pare-feu (firewall) ?

7.2.1 Définition

Un **pare-feu** (ou *firewall*) est un dispositif de sécurité réseau chargé de filtrer le **trafic entrant et sortant** en fonction de règles définies (ex : bloquer un port, une IP, ou un protocole spécifique).

7.2.2 Types de pare-feu

- **Pare-feu matériel** : boîtier dédié installé sur le réseau.
- **Pare-feu logiciel** : installé sur un poste ou un serveur.
- **Pare-feu applicatif (WAF)** : protège les applications web.
- **Pare-feu de nouvelle génération (NGFW)** : offre des fonctions avancées (filtrage applicatif, détection dintrusion, etc.).

7.3 Différences entre UTM et pare-feu classique

Fonction	Pare-feu classique	UTM
Filtrage réseau	✓	✓
Filtrage applicatif	× (ou limité)	✓
IDS/IPS	×	✓
Antivirus intégré	×	✓
VPN	× (souvent séparé)	✓
Filtrage Web/URL	×	✓
Gestion centralisée	×	✓
Coût	Moins cher	Plus cher mais plus complet

7.4 Pare-feux classiques

- **Cisco ASA** : solution robuste pour les entreprises.
- **pfSense** : pare-feu open source, idéal pour les PME.
- **iptables / nftables** : pare-feu intégré aux distributions Linux.
- **Windows Defender Firewall** : pare-feu logiciel intégré à Windows.
- **OPNsense** : alternative open source à pfSense.

7.5 Solutions UTM

Marque	Avantages	Public cible
Fortinet FortiGate	Solution complète, très répandue, bon rapport qualité/prix	Entreprises, établissements publics
Sophos XG Firewall	Interface intuitive, intégration antivirus efficace	PME, écoles
WatchGuard Firebox	Facile à déployer, bon filtrage de contenu	PME, collectivités
Stormshield (Airbus)	Conforme aux normes ANSSI, made in France	Secteur public, santé, collectivités
Palo Alto Networks	Très haut de gamme, sécurité avancée	Grandes entreprises, environnements critiques
SonicWall	Populaire chez les intégrateurs, bon compromis	PME
Untangle (NG Firewall)	Solution open source simple à gérer	Petites structures, écoles

7.6 À retenir

— Le **pare-feu** est une *brique de base* pour sécuriser un réseau.
— Le **UTM** est une *solution tout-en-un* plus complète qui intègre plusieurs protections.
— LUTM est recommandé pour les **PME**, les **établissements scolaires**, ou toute structure souhaitant centraliser la sécurité sans multiplier les outils.

8 Annexe 5 : Le VPN et la continuité dactivité

8.1 Quest-ce quun VPN ?

Un **VPN** (*Virtual Private Network*) permet de créer un **tunnel sécurisé** entre deux points dun réseau, généralement entre un utilisateur distant et linfrastructure de lentreprise. Toutes les communications sont chiffrées, garantissant confidentialité et intégrité des données.

8.2 Utilité dun VPN dans la continuité dactivité

Au-delà de la protection des connexions distantes, un VPN peut contribuer à la **continuité dactivité**, en permettant :
— la liaison sécurisée entre plusieurs **sites distants** (ex : siège et succursale),
— la **synchronisation ou réplication de données** entre serveurs,
— la **haute disponibilité** ou la **reprise après sinistre** (PRA).

8.3 Exemple concret : Réplication Hyper-V via VPN

Hyper-V est une solution de virtualisation développée par Microsoft. Elle propose une fonction de **réplication** des machines virtuelles dun serveur principal vers un serveur secondaire. Cette réplication est essentielle pour assurer la continuité des services.
— **Sans VPN** : la réplication entre deux serveurs distants (dans des sites géographiques différents) serait risquée car non sécurisée, voire impossible si les flux sont bloqués par un pare-feu.
— **Avec VPN** : un tunnel sécurisé est établi entre les deux serveurs. Les données des machines virtuelles peuvent alors être **répliquées en toute sécurité**, assurant la continuité de service en cas de défaillance du serveur principal.

8.4 Conclusion

Le VPN ne se limite pas à la sécurisation des accès utilisateurs. Il constitue un **élément clé de linfrastructure réseau**, permettant la **protection des échanges inter-sites**, la **synchronisation des systèmes critiques** et la **résilience de lentreprise** face aux incidents.

9 Annexe 6 : VPN IPsec

Dans le cadre des VPN de type IPsec, la protection des échanges repose sur la mise en place de **clés de chiffrement** associées à des **associations de sécurité** (SA). Ces SA déterminent les règles de chiffrement, d'intégrité et d'authentification utilisées pour sécuriser les paquets IP.

9.1 Clé de chiffrement pour les données sortantes (ex : ESP-SA1 ou CHILD-SA1)

Une fois un tunnel IPsec établi, chaque sens de communication (émission et réception) est associé à une **Security Association** (**SA**) spécifique. Chaque SA contient :
- Une clé de chiffrement symétrique (ex : AES-256),
- Un algorithme de chiffrement et/ou dauthentification,
- Des paramètres de durée de vie (temps ou volume),
- Un identifiant SPI (Security Parameter Index).

Par exemple, une SA nommée **ESP-SA1** ou **CHILD-SA1** est utilisée pour chiffrer les données sortantes du client VPN vers le serveur distant. Une autre SA (différente) est utilisée pour les données entrantes.

9.2 ESP : Encapsulating Security Payload

9.2.1 Définition

ESP (Encapsulating Security Payload) est un protocole IPsec permettant de :
- **Chiffrer** les données (confidentialité),
- **Authentifier** les paquets (intégrité, HMAC),
- **Prévenir les rejets et attaques par rejeu** (anti-replay).

9.2.2 Fonctionnement

ESP encapsule la charge utile du paquet IP. Il peut être utilisé de deux façons :
- **Mode transport** : seul le contenu du paquet IP est protégé. Utilisé entre deux hôtes.
- **Mode tunnel** : tout le paquet IP (entête + données) est encapsulé dans un nouveau paquet. Utilisé entre deux passerelles (VPN site-à-site).

9.2.3 Exemple de chiffrement avec ESP

Lorsquun poste envoie une requête HTTP via un tunnel IPsec :

1. Le paquet HTTP est encapsulé dans un paquet IP.
2. ESP chiffre la charge utile (et parfois lentête IP, selon le mode).
3. Le paquet chiffré est envoyé via Internet.
4. Le destinataire déchiffre grâce à la SA correspondante.

9.3 CHILD SA : Security Association de phase 2

9.3.1 Architecture IPsec

Le protocole IPsec fonctionne en deux phases (dans IKEv2) :
- **Phase 1** : négociation de l**IKE SA**, utilisée pour authentifier les pairs et échanger les clés.
- **Phase 2** : création dune ou plusieurs **CHILD SA**, utilisées pour protéger le trafic réel avec ESP.

9.3.2 Rôle des CHILD SA

Une **CHILD SA** contient :
- Les clés symétriques de chiffrement pour chaque sens,
- Les algorithmes de chiffrement et dintégrité,
- Les paramètres de durée de vie,
- Les flux à protéger (ex : tous les paquets entre 10.0.0.0/24 et 192.168.0.0/24).

9.3.3 Pourquoi CHILD ?

Parce que la SA est **enfant** de lIKE SA : elle est négociée après létablissement dune relation de confiance via IKEv2.

9.3.4 Exemple de session IPsec complète

1. **IKE SA** est établie (Phase 1), via échange sécurisé de clés.
2. **CHILD SA1** est créée (Phase 2) avec une clé utilisée pour chiffrer les paquets sortants (ex : ESP-SA1).
3. Une **deuxième SA** est créée pour les paquets entrants.
4. Des paquets IP passent dans le tunnel, protégés via ESP.

9.4 Résumé

- **ESP** est le protocole responsable du chiffrement/authentification des paquets IP dans IPsec.
- Une **clé de chiffrement** est définie pour chaque direction (envoi/réception) via une **Security Association**.
- **CHILD SA** est créée dans la phase 2 de la négociation IKEv2 et sert à sécuriser le trafic réel (données).
- Une **IKE SA** peut gérer plusieurs CHILD SA.

10 Annexe 7 : Authentification

10.1 PSK Pre-Shared Key (Clé partagée à lavance)

Définition : une clé secrète est partagée manuellement entre les deux extrémités du VPN (client et serveur).
Avantages :
- Mise en place simple.
- Aucune infrastructure supplémentaire requise.

Inconvénients :
- Peu sécurisé si la clé est faible ou divulguée.

— Non évolutif : une seule clé pour tous les pairs.
— Impossible de distinguer les utilisateurs individuellement.

10.2 PKI Public Key Infrastructure (IGC Infrastructure de Gestion des Clés)

Définition : système reposant sur la cryptographie asymétrique. Chaque entité possède une clé privée et un certificat public signé par une autorité de certification (AC).
Composants :
— Certificats numériques.
— Clés publiques / privées.
— Autorité de certification (AC).
— Mécanismes de révocation (CRL, OCSP).
Avantages :
— Haut niveau de sécurité.
— Identification unique de chaque utilisateur ou appareil.
— Possibilité de révocation centralisée.
Inconvénients :
— Déploiement et gestion complexes.
— Nécessite une infrastructure PKI (interne ou externe).

10.3 RADIUS Remote Authentication Dial-In User Service

Définition : protocole client-serveur permettant d'externaliser lauthentification à un serveur central (souvent lié à un annuaire LDAP ou Active Directory).
Avantages :
— Authentification centralisée.
— Intégration facile avec lActive Directory.
— Contrôle daccès par groupe ou par politique.
Utilisation : le serveur VPN interroge un serveur RADIUS pour valider les identifiants utilisateur.

10.4 MFA Multi-Factor Authentication (Authentification Multi-Facteurs)

Définition : méthode dauthentification combinant plusieurs éléments :
— **Connaissance** : mot de passe, code PIN.
— **Possession** : téléphone, token physique, carte à puce.
— **Inhérence** : empreinte digitale, reconnaissance faciale.
Avantages :
— Renforce considérablement la sécurité.
— Protège contre le vol d'identifiants seuls.
Exemples :
— Code SMS après mot de passe.
— Application dauthentification (OTP).

10.5 IKE Internet Key Exchange

Définition : protocole utilisé par IPsec pour négocier les paramètres de sécurité, authentifier les pairs et générer les clés.
Fonctionnement par phases :
- **Phase 1** : création de la IKE SA (canal sécurisé initial).
- **Phase 2** : création de CHILD SA pour le trafic chiffré réel.

Version actuelle : IKEv2 (plus rapide, plus robuste, meilleure gestion de la mobilité).

10.6 SA Security Association

Définition : ensemble de paramètres utilisés pour sécuriser une communication (clés, algorithmes, durée de vie, SPI).
Types :
- **IKE SA** : pour la négociation et lauthentification.
- **CHILD SA** : pour le chiffrement du trafic utilisateur.

Chaque SA est unidirectionnelle : une pour envoyer, une pour recevoir.

10.7 CRL / OCSP Méthodes de révocation des certificats

- **CRL (Certificate Revocation List)** : liste publiée régulièrement par lAC contenant les certificats révoqués.
- **OCSP (Online Certificate Status Protocol)** : permet de vérifier en temps réel si un certificat est valide.

Utilité : permet de désactiver un certificat compromis sans redéployer toute linfrastructure.

11 Annexe 8 : Autorité de certification

1. Objectif

Permettre à un client (utilisateur, machine ou service) de prouver son identité à un serveur (ex : VPN, site web, API) à laide dun **certificat numérique**, signé par une **Autorité de Certification (CA)**.

2. Enregistrement auprès de la CA

2.1 Génération de la paire de clés

Le client génère :
- une **clé privée** (secrète),
- une **clé publique** (diffusable).

2.2 Création dune CSR (Certificate Signing Request)

Le client crée une **CSR** contenant :
- sa **clé publique**,
- ses informations didentification (nom, email, organisation, etc.),
- une signature numérique faite avec sa **clé privée**.

2.3 Envoi de la CSR à la CA

La CSR est envoyée à lAutorité de Certification via :
- une interface web,
- un outil CLI,
- ou un protocole automatisé (ex : ACME).

3. Validation par la CA

La CA vérifie :
- que le certificat est demandé par une entité légitime,
- que les informations sont correctes,
- que lidentité peut être prouvée.

Types de validation :
- Validation de domaine (via DNS ou fichier HTTP),
- Validation didentité (administratif ou email),
- Validation dorganisation (dossiers officiels).

Si la demande est validée, la CA signe la CSR avec sa **clé privée** et génère le **certificat** du client.

4. Délivrance du certificat

Le client reçoit un certificat contenant :
- sa **clé publique**,
- ses informations didentité,
- la **signature numérique de la CA**.

Ce certificat est ensuite :
- stocké localement,
- ou installé dans un navigateur, un OS, un serveur VPN.

5. Authentification avec le certificat (ex : connexion VPN)

Étape 1 : présentation du certificat

Le client se connecte au serveur VPN et envoie son certificat.

Étape 2 : vérification par le serveur

Le serveur vérifie que :
- le certificat est signé par une CA de confiance,
- il est encore valide (date),
- il na pas été révoqué (CRL ou OCSP),
- le nom commun (CN) correspond à lattendu.

Étape 3 : vérification de la signature

Le serveur utilise la **clé publique de la CA** pour vérifier lauthenticité du certificat.

Étape 4 : authentification réussie

Si tout est conforme, la connexion est acceptée. Une **clé symétrique** est ensuite négociée pour le chiffrement des données.

6. Rôle des clés dans le processus PKI

Élément	Contient / sert à	Utilisation
Clé publique du client	Dans le certificat	Permet de vérifier la signature dune CSR
Clé privée du client	Gardée secrète	Sert à signer la CSR et à sauthentifier
Clé privée de la CA	Secrète	Sert à signer les certificats des clients
Clé publique de la CA	Publiée et utilisée par les serveurs	Permet de vérifier lauthenticité du certificat du client

Conclusion

Linfrastructure PKI repose sur la séparation entre :
- une clé privée (gardée secrète),
- une clé publique (diffusée et signée),
- une CA qui joue le rôle de tiers de confiance.

Cette architecture garantit à la fois :
- lidentification des entités,
- la sécurisation des échanges,
- la possibilité de gérer le cycle de vie des certificats (délivrance, expiration, révocation).