Access Control List (ACL)

Access Control List (ACL), v českém překladu seznam řízení přístupu, je stěžejní bezpečnostní mechanismus používaný napříč informačními technologiemi. Jedná se o sekvenční seznam pravidel, která exaktně definují, jaký subjekt (např. uživatel, proces, nebo IP adresa) má oprávnění přistupovat k určitému objektu (soubor, složka, síťové rozhraní) a jakou akci s ním smí provést.

Koncept ACL se historicky rozdělil do dvou technologicky odlišných, ale logicky příbuzných větví: **Síťové ACL** (filtrování síťového provozu) a **Souborové ACL** (řízení přístupu k datům v operačním systému).

1. Síťové ACL (Network ACL)

V kontextu počítačových sítí fungují ACL jako primitivní bezstavové firewally. Konfigurují se nejčastěji na směrovačích (routerech) nebo přepínačích (switchech) a slouží k filtrování procházejících síťových paketů.

Princip fungování

Při aplikaci síťového ACL na rozhraní routeru je každý příchozí nebo odchozí paket analyzován a porovnáván se seznamem pravidel. Tento proces má dvě naprosto kritické vlastnosti:

- **Sekvenční zpracování (Top-Down):** Router čte pravidla přísně shora dolů (od prvního k poslednímu). Jakmile paket splní podmínky některého pravidla, router okamžitě provede akci (paket propustí - **Permit**, nebo zahodí - **Deny**) a zbytek seznamu již nečte. Na pořadí pravidel tedy fatálně záleží.
- **Implicitní zamítnutí (Implicit Deny):** Na úplném konci každého ACL se nachází neviditelné pravidlo, které zablokuje veškerý provoz. Pokud paket neprojde ani jedním z definovaných „Permit“ pravidel, je na konci seznamu nemilosrdně zahozen.

Typy síťových ACL (příklady dle Cisco standardu)

- **Standardní ACL:** Jsou velmi jednoduchá, ale omezená. Filtrují provoz výhradně na základě **zdrojové IP adresy** paketu. Nezajímá je, kam paket směřuje, ani jaký protokol (HTTP, FTP) využívá. Z důvodu této nepřesnosti se umisťují co nejblíže k cílové destinaci.
- **Rozšířená ACL (Extended ACL):** Poskytují granulární kontrolu. Dokáží analyzovat zdrojovou IP adresu, cílovou IP adresu, použitý protokol (TCP, UDP, ICMP) a dokonce i konkrétní zdrojové a cílové porty (např. port 80 pro webový provoz). Umisťují se co nejblíže ke zdroji provozu, aby se šetřila propustnost sítě.

2. Souborové ACL (Filesystem ACL)

V operačních systémech (Windows, Linux, macOS) řeší ACL práva k souborům a složkám. Standardní POSIX práva v systémech Unix/Linux umožňují definovat přístup pouze pro tři entity: vlastníka (User),

skupinu (Group) a všechny ostatní (Others).

Tento klasický model selhává v komplexním firemním prostředí, kdy potřebujete dát práva ke čtení konkrétnímu uživateli A a uživateli B, práva k zápisu uživateli C, a to vše bez vytváření zbytečných dedikovaných skupin. Právě zde nastupuje souborové ACL, které umožňuje k jednomu souboru připojit nekonečně dlouhý seznam konkrétních uživatelů a jejich specifických oprávnění.

Implementace v OS

- **Windows (NTFS / ReFS):** ACL je absolutním základem zabezpečení celého systému Windows. Každý objekt (soubor, složka, klíč v registrech) má svůj **DACL** (Discretionary Access Control List), který určuje, kdo má přístup, a **SACL** (System Access Control List), který určuje, jaké pokusy o přístup se mají auditovat do bezpečnostního logu.
- **Linux (ext4 / XFS):** Rozšířené atributy filesystému. Konfigurují se pomocí terminálových příkazů `setfacl` a `getfacl`.

Výhody a nevýhody používání ACL

Výhody

- **Vysoká bezpečnost a kontrola:** Umožňují mikromanagement přístupů a implementaci principu nejnižších nutných oprávnění (Principle of Least Privilege).
- **Nízká hardwarová náročnost:** Na routerech fungují díky hardwarové akceleraci obvykle rychlostí linky, bez prodlení.
- **Standardizace:** Osvědčená technologie s předvídatelným chováním napříč průmyslem.

Nevýhody

- **Extrémní náročnost na správu:** Dlouhé seznamy stovek pravidel se rychle stávají nepřehlednými. Zjišťování chyby (troubleshooting) ve špatně navrženém síťovém ACL je „noční můrou“ administrátorů.
- **Statická povaha síťových ACL:** Klasické ACL nedokáže reagovat na dynamické hrozby (nevidí obsah paketu ani nezná stav TCP spojení, pouze čte hlavičky). Tento problém dnes řeší moderní stavové firewally (Stateful Inspection).

Srovnání standardních a rozšířených síťových ACL

Parametr	Standardní ACL	Rozšířené ACL (Extended)
Kritéria pro filtraci	Pouze zdrojová IP adresa	Zdrojová a cílová IP, porty, protokoly
Přesnost (Granularita)	Velmi nízká (blokuje celý přístup ze zdroje)	Extrémně vysoká (lze povolit web, ale zakázat poštu)
Optimální umístění v síti	Co nejblíže k cíli (Destination)	Co nejblíže ke zdroji (Source)
Číslování (Cisco IOS)	1 - 99, 1300 - 1999	100 - 199, 2000 - 2699