Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) pomáha IT profesionálom čeliť výzvam v oblasti mobility a chrániť evolúciu siete v rámci celého spektra útokov. Cisco ISE predstavuje najlepšiu platformu na trhu pre spravovanie politiky zabezpečenia. Spája a automatizuje kontrolu prístupu na pretlačenie prístupu do sietí a ku sieťovým zdrojom na základe rolí a jej dodržiavaní.

Tabuľka 1. Najväčšie výhody pre zákazníka

Výhoda	Popis
Extenzívna politika presadzovania	ISE predstavuje prvý softvérovo definovaný bezpečnostný regulátor. Organizácie môžu jednoducho definovať pravidlá prístupovej politiky a pružne reagovať na potreby stále sa meniacich podnikateľských potrieb. Dokážu to všetko urobiť z centralizovaného miesta, ktoré prerozdeľuje výkon činností v celej sieti a bezpečnostných infraštruktúrach. Napríklad, IT správcovia môžu centrálne definovať politiku, ktorá bude rozlišovať medzi používateľmi - hosťami (guest users) a zariadeniami registrovaných používateľov a zariadeniami. Bez ohľadu na prístupové miesto, používatelia a koncové body budú mať povolený prístup na základe svojho kontextu.
Dodržiavanie bezpečnosti	Jediná riadiaca konzola zjednodušuje tvorbu politiky, viditeľnosť a podávanie správ vo všetkých sieťach spoločnosti. IT personál môže jednoducho overovať plnenie záväzkov pre audity, regulačné požiadavky a vládne usmernenia pre štandardy IEEE 802.1X.
Podpora infraštruktúry viacerých predajcov	ISE podporuje prístup do siete zo zariadení tretích strán v závislosti od možností zariadenia.[1] ISE spolupracuje s infraštruktúrou viacerých predajcov (napríklad, switche a bezdrôtové prístupové body). Spĺňa RADIUS a štandardy IEEE 802.1x, nevyžaduje však IEEE 802.1X, aby bolo plne ovládateľné. Cisco a jeho partneri ponúkajú osvedčené usmernenia a tiež detailné praktické návrhy usmernení. Podnikoví zákazníci používajú ISE so sieťovou infraštruktúrou navrhnutou Ciscom spolu s technológiou Cisco TrustSec pre ešte väčšiu informovanosť a viditeľnosť zo svojich sietí.

[1] Pre štandardnú kontrolu prístupu s dynamickým povoľovaním (včítane integrácie profilovania do prístupového rozhodnutia) musí zariadenie na prístup do siete podporovať CoA, tak ako je definované v RFC 5176. Pri hosťoch, BYOD on boarding a posture flows, musí zariadenie na prístup do siete podporovať presmerovanie URL s notifikáciou MAC adresy.

Tabuľka 2. Funkcie a ich prínos.

Funkcia	Prínos
Presadzovanie obchodnej politiky	Poskytuje model politiky na báze pravidiel a atribútov slúžiaci na vytváranie flexibilných a obchodne relevantných politík kontroly prístupu. Poskytuje schopnosť vytvárať diferencované politiky vyťahovaním atribútov z preddefinovaných slovníkov, ktoré obsahujú informácie o používateľovi a identite koncového bodu, overenie posture, overovanie protokolov, profilovanie identity alebo ďalšie zdroje externých atribútov. Atribúty môžu byť vytvárané dynamicky a uložené na neskoršie použitie. Ponúka schopnosť integrácie s viacerými externými archívmi identít, ako sú Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), RADIUS, RSA jednorazové heslo (OTP) a certifikované úrady pre overovanie a povolenia.
Protokoly AAA	Používa RADIUS, štandardný protokol na overovanie, povolenia a účtovanie (AAA). Podporuje širokú škálu overovacích protokolov vrátane (no nie výhradne) PAP, MS-CHAP, Extensible Authentatication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), EAP-Transport Layer Security (TLS) a EAP-Tunneled Transport Layer Security (TTLS). ISE je jediný RADIUS server, ktorý podporuje EAP prepájanie stroja a používateľských poverení.
Profilovanie zariadenia	Dodáva sa s preddefinovanými šablónami zariadení pre viaceré typy koncových bodov, ako sú IP telefóny, tlačiarne, IP kamery, smartfóny a tablety. Správcovia môžu takisto vytvárať svoje vlastné šablóny zariadení. Tieto šablóny môžu byť automaticky zistené, zatriedené a pripíšu sa im identity definované administrátorom, keď sa koncové body pripoja do siete. Administrátori môžu taktiež pripisovať koncovým bodom špecifické autorizačné politiky na základe typu zariadenia. Toto riešenie zozbiera atribučné dáta koncového bodu s pasívnym monitorovaním siete a telemetriou, vyberie reálne koncové body alebo alternatívne z infraštruktúry Cisco pomocou senzorov zariadenia na switchoch Cisco Catalyst. Schopnosť switchov Catalyst rozpoznávať koncové body so zreteľom na infraštruktúru predstavujú podmnožinu rozpoznávacej technológie ISE. Táto schopnosť umožní switchu rýchlo zozbierať informácie o atribútoch koncového bodu a potom, za použitia štandardu RADIUS, posunúť túto informáciu do ISE, kde prebehne klasifikácia koncového bodu a úkon na základe politiky. Toto rozpoznávanie na báze switchu podporuje efektívny a distribuovaný zber informácií o koncovom bode pre vyššiu škálovateľnosť, nasaditeľnosť a čas na klasifikáciu.
Extenzívna podpora multiforestného Active Directory	Poskytuje komplexné overovanie a autorizáciu voči multiforestným doménam Microsoft Active Directory. Môže zoskupiť viaceré nesúvislé domény do logických skupín pre zjednodušenie konfigurácie zložitých topológií Active Directory za účelom podpory neustále sa meniaceho podnikateľského prostredia. Podporuje taktiež flexibilné pravidlá na prepisovanie identity pre hladší prechod na a integráciu tohto riešenia. Podporuje Microsoft Active Directory 2003, 2008, 2008R2, 2012 a 2012R2.

Monitorovanie a riešenie problémov	Obsahuje zabudovanú webovú konzolu pre monitorovanie, hlásenie a riešenie problémov, určenú pre help desk a prevádzkovateľov siete pre rýchle identifikovanie a odstránenie problémov. Ponúka robustné podávanie správ v historickom režime i v reálnom čase pre všetky služby, logovanie všetkých činností a metriku na prístrojovom panely v reálnom čase zachytávajúcu všetkých používateľov a koncové body, ktoré sa prípájajú do siete.
Možnosti platformy	Dostupné ako fyzické alebo virtuálne zariadenie. Sú dve fyzické platformy a tiež virtuálne možnosti na báze VMware ESXi alebo KVM. Aj fyzické aj virtuálne varianty môžu byť použité na vytváranie ISE klastrov pre potreby väčších organizácií a poskytovať potrebnú škálu, redundanciu a failover potrebné pri kritických podnikových systémoch.
Certifikácie	Spĺňa požiadavky Federal Information Processing Standard (FIPS) 140-2, Spoločné kritéria (CC) a Unified Capabilities Approved Product List. Je tiež pripravené na IPv6. Poznámka: Certifikácie nemusia byť dostupné pre všetky vydania resp. môžu byť v rôznych štádiach schvaľovania. Aktuálne certifikácie a vydania nájdete v Global Government Certifications.

Balík 10 Cisco ISE virtuálnych zariadení: R-ISE-10VM-K9=

Cisco ISE Balíky licencií		
ISE Balíky licencií	Perpetuálne/Predplatenie (Podmienky dostupné)	ISE Funkcionalita
Base	Perpetuálne	● Základný prístup k sieti: AAA, IEEE-802.1X ● Správa hostí (guest management) ● Šifrovanie prepojenia (MACSec) ● TrustSec ● ISE rozhrania aplikačného programovania
Plus		● BYOD, profiling

Ostatné parametre:

- Škálovateľnosť pre počet overení 1000/sec, (s možnosťou rozšírenia)
- podpora protokolu RADIUS pre autentifikáciu, autorizáciu a accounting (AAA),
- podpora integrovanej užívateľskej databázy,
- podpora integrácie s externými identity databázami Windows Active Directory a LDAP, možnosť súčasného použitia viacerých externých užívateľských databáz,
- Podpora autentifikačného protokolov: Password Authentication Protocol (PAP), Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)
- podpora modelu vytvárania politík na základe rôznych pravidiel a atribútov akými sú rôzne autentifikačné protokoly, obmedzenia plynúce z autentifikačných zariadení, obmedzenia dané časovým údajom, validácia atribútov operačných systémov a antivírusového softwérového vybavenia, prípadne iné prístupové obmedzenia.
- podpora webovej autentifikácie pre návštevy pomocou protokolu HTTP aj HTTPS. Webový portál je možné hosťovať priamo v riadiacom systéme alebo na externom serveri.
- Možnosť filtrovania prístupu k obsahu a blokovania nevhodného obsahu podľa rôznych kritérií v spolupráci s ďalšími prvkami, napríklad podľa skupín užívateľov