ESET Protect – Preporučene radnje (Best practices)

Tema

Preporučene radnje za konfiguriranje sustava ESET Protect.

Uvod

Po instalaciji su navedeni serveri konfigurirani na način koji odgovara zahtjevima većine poduzeća. No, inicijalne postavke ne moraju odgovarati uvijek i svima, stoga donosimo popis dijela radnji koje biste mogli primijeniti jednokratno/dnevno/tjedno ili ih promijeniti kako biste sustav prilagodili radu svoj mreže.

Naravno da neke od ovih radnji neće odgovarati vašem okruženju (npr. zatvorene mreže neće računalim dopustiti direktan izlaz na internet bez proksija i sl.) – provjerite prijedloge i primijenite one za koje mislite da će povećati sigurnost i pojednostaviti administraciju.

Postupak

Po instalaciji provjerite upute na stranici https://help.eset.com/protect_admin/latest/en-US/fs.html (*online* pomoć je dostupna i na hrvatskom, samo promijenite jezik u izborniku gore desno) i sljedeće prijedloge:

Kreirajte dodatnog administratora	https://help.eset.com/protect_admin/latest/en-US/admin_ar_create_native_user.html
Iskoristite 2FA	https://help.eset.com/protect_admin/latest/en-US/admin_ar_two_factor_authentification.html
Pregledajte policy za EMAgenta i po potrebi promijenite postavke	https://help.eset.com/protect_admin/latest/en-US/admin_ar_create_native_user.html?admin_pol.html
Pregledajte policy za sigurnosne programe i po potrebi promijenite postavke	https://help.eset.com/protect_admin/latest/en-US/admin_ar_create_native_user.html?admin_pol.html
Postavite lozinku na napredno podešavanje radi sprječavanja promjena	https://help.eset.com/ees/8/en-US/idh_change_password.html
Postavite lozinku na EMAgenta radi sprječavanja deinstaliranja	https://help.eset.com/protect_admin/latest/en-US/admin_pol_password_protection.html
Uključite detekciju svih triju vrsta neželjenih programa (*1)	https://help.eset.com/ees/8/en-US/idh_config_scanner.html
Administratorima i naprednim korisnicima definirajte izuzetke (*2)	https://help.eset.com/ees/8/en-US/idh_detection_exclusions.html
Iskoristite proxy (ostavite i mogućnost direktnog izlaska na internet) (*8)	https://help.eset.com/protect_install/latest/en-US/apache_http_proxy.html
Podesite Dashboard	https://help.eset.com/protect_admin/latest/en-US/client_tasks_virus_db_update.html?dashboard.html
Ograničite pristup nekim vrstama stranica	https://help.eset.com/ees/8/en-US/idh_page_setting_parental.html
Neriješene prijetnje: uklonite taskom “On-Demand scan” (In-Depth)	https://help.eset.com/protect_admin/latest/en-US/client_tasks_on_demand_scan.html
Neriješene prijetnje: ručno analizirajte svaku i ručno uklonite (*3)	n/a
Neriješene prijetnje: provjerite najčešća računala / korisnike	Ako ustanovite da uvijek isti korisnici imaju prijave prijetnji – podučite ih pravilnom korištenju računala / interneta ili ih stavite u posebnu grupu u EPx i definirajte stroži policy
Iskoristite dinamičke grupe (*4)	https://help.eset.com/protect_admin/latest/en-US/admin_dg_dynamic_group_wizard.html https://help.eset.com/protect_admin/latest/en-US/dynamic_group_examples.html
Instalirajte najnovije verzije ESET-ovih programa	https://help.eset.com/protect_admin/latest/en-US/outdated_applications.html
Provjerite nadograđuju li se moduli i forsirajte ako ima problema	https://help.eset.com/protect_admin/latest/en-US/client_tasks_virus_db_update.html
Nadogradnja operacijskog sustava	https://help.eset.com/protect_admin/latest/en-US/client_tasks_system_update.html

Provjerite stanje taskova; ponovite neuspjele ili uklonite uzrok "pada"	https://help.eset.com/protect_admin/latest/en-US/fs_post_installation_tasks.html?admin_ct_executions.html
Iskoristite izvješća	https://help.eset.com/protect_admin/latest/en-US/reports.html
Automatizirajte kreiranje izvješća; dodatno ih obradite svojim skriptama (*5)	https://help.eset.com/protect_admin/latest/en-US/reports.html?schedule_a_report.html
Namjestite slanje obavijesti (*Notifications*) u nekim uvjetima (*6)	https://help.eset.com/protect_admin/latest/en-US/admin_ntf_notifications.html
Ostala upozorenja (*7)	

(*1) Neželjene vrste programa – u pravilu krajnji korisnici nemaju potrebu za ovakvim alatima, ali mogu biti korisni administratorima i tehničkom osoblju, pa kreirajte odgovarajuća pravila (policy) i nekima uključite detekciju svega, a drugima možda dopustite malo slobodniji rad (naša preporuka je da uključite sve kategorije, a da napravite pojedinačne izuzetke alata kako je opisano u ovom dokumentu). Ovu stavku je moguće definirati i u pravilu (policyju) EP servera.

• Potentially unwanted applications
• Potentially unsafe applications
• Suspicious applications

(*2) Preporučujemo da u izuzetke stavite konkretnu datoteku i/ili konkretnu prijetnju. Stavljanje cijelog direktorija u izuzetak od detekcije može dovesti do toga da se u njemu nađe prijetnja koja je izvan kontrole administratora antivirusnog sustava. Ovu stavku je moguće definirati i u pravilu (policyju) EP servera.

(*3) Najčešće se dogodi da tijekom skeniranja korisnik odgodi brisanje prijetnji na kraj skeniranja, a u međuvremenu se uvjeti s datotekom promijene:

• datoteka je zauzeta
• Endpoint je namješten tako da ne briše detekcije, nego ih samo prijavljuje
• datoteka se nalazi u sistemskom direktoriju i nije sigurno po OS ukloniti ju bez suradnje administratora
• datoteka više ne postoji (npr. browser cache je očišćen, vanjski uređaj je iskopčan, ..)
• EFI/UEFI detekcije – ne mogu se obrisati jer su u BIOS-u

(*4) Npr. kreirajte dinamičku grupu "DynGrp_Neriješene_prijetnje"
• Neka grupa obuhvati računala koja ispune uvjet ("*Dynamic group template expression*"): "Active detections – Detection handled" = "No"
• Kreirajte policy koji ima najstroža pravila i dodijelite ga grupi (https://help.eset.com/protect_admin/latest/en-US/amin_pol_assign_policy_to_group.html)
• Kreirajte scheduled task "On Demand Scan" – "In-Depth Scan" koji će se pokrenuti ("trigger") "Joined Dynamic Group Trigger"

Na ovaj način će računala kod kojih se pojavi neriješena prijetnja biti automatki uključena u dinamičku grupu, konfiguracija će im biti postavljena "na najjače" i odmah će se pokrenuti dubinsko skeniranje. Ako imate ESET Endpoint Security možete dodati i da se računalo izdvoji (isključi) s mreže – ostat će u kontaktu sa EPx serverom, ali sve druge mrežne aktivnosti će biti spriječene.

(*5) Automatizirana izvješća

Izvješća (Reports) se mogu podesiti da se pokreću periodično i da automatski pošalju e-mail sa .PDF privitkom i spreme .CSV datoteku na disk. CSV datoteku možete dodatno obrađivati svojim skriptama, uvoziti u baze itd.

(*6) Aktivirajte obavijesti (Notifications) koje će se slati u važnim situacijama (npr. ako se u periodu od 5

minuta pojavi više od 5 detekcija); kreirajte grupnu, distribucijsku e-adresu koju po potrebi može pratiti više osoba i reagirati. Nemojte namjestiti previše obavijesti jer će dovesti do zasićenja administratora i one važne mogu kasnije biti ignorirane.

(*7) Ostala upozorenja kojima treba posvetiti pozornost:

• Anti-Phishing protection is non-functional
• Anti-Stealth is non-functional
• Computer restart required
• Detection Engine out of date
• ESET LiveGrid is not accessible
• ESET Management Agent is outdated
• Host Intrusion Prevention System (HIPS) is non-functional
• License expires
• Product malfunction
• Operating system is not up to date
• Presentation mode is enabled
• Product is installed but it is not running
• Product not activated
• Real-time file system protection is disabled
• Some of the functionality of this ESET Security Product is not supported on macOS Big Sur yet. Check for product updates regularly to get the unsupported functionality back on your macOS. More info: https://support.eset.com/news7604
• Web control is non-functional
• Windows Security Center indicates that the feature is not installed or is not running properly
• Windows updates available
• Your product is outdated
• Your security product will reach End of Life soon

(*8) HTTP proxy

Korištenje HTTP proksija koji dolazi s instalacijom administrativnog servera je naročito praktično u okruženjima u kojima je pristup internetu na neki način ograničen. Takva ograničenja mogu smetati komunikaciji klijenata s ESET-ovim serverima, što se u slučaju korištenja proksija može riješiti tako da na firewallu perimetra propustite sav promet s EPx servera (preciznije – sa HTTP proksija na serveru) prema internetu, a klijenti komuniciraju s tim proksijem.

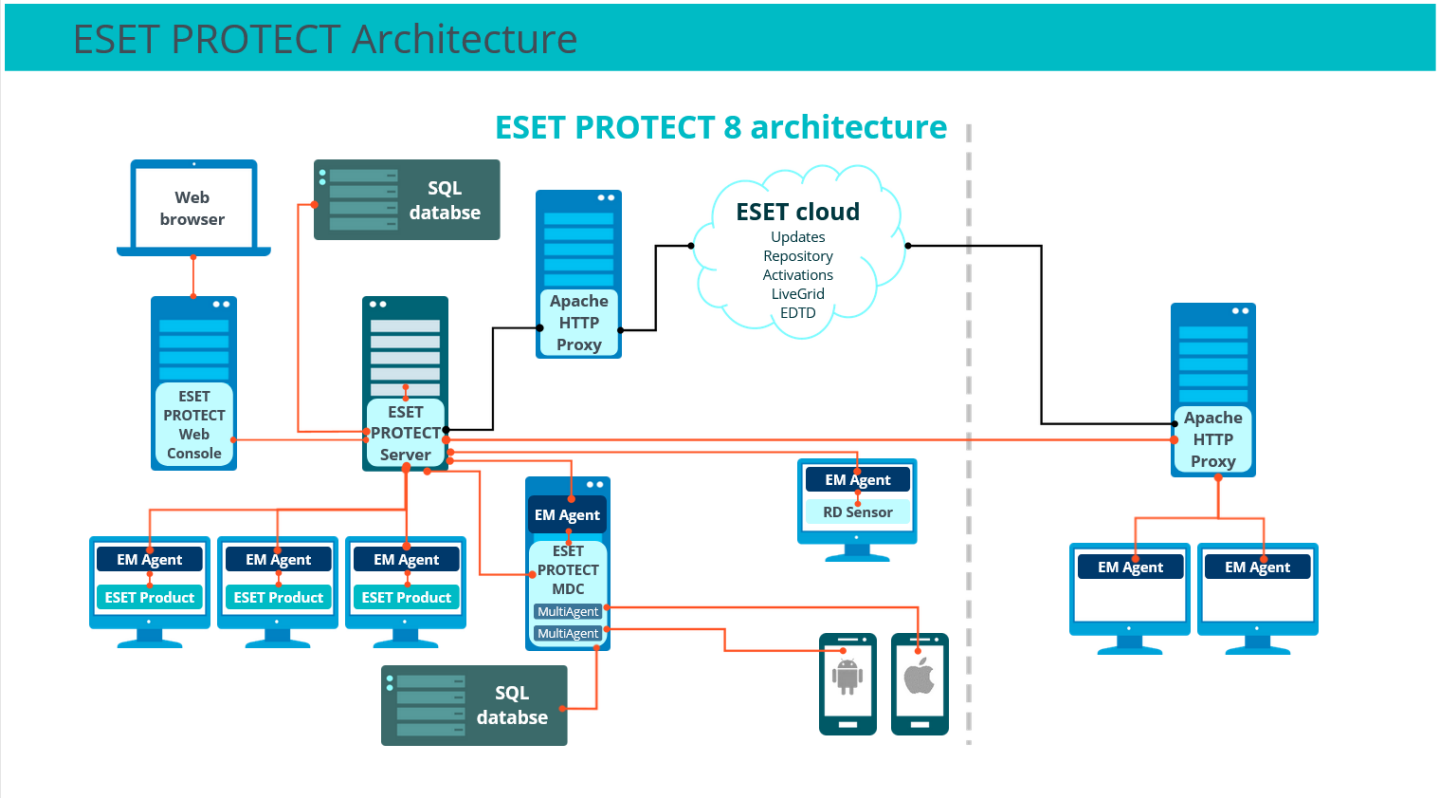
Ako koristite ESETBridge uveden s ESET Protect v.10 obavezno prođite kroz dokumente za konfiguraciju: https://help.eset.com/ebe/latest/en-US/?configure.html i privjerite odgovara li policy vašim zahtjevima.

Razno

n/a

Slike

• Arhitektura



ESET Protect EPx – Arhitektura Architecture

https://help.eset.com/protect_install/latest/en-US/architecture.html

---

epx xepx bestpractices xbestpracticesx xpreporuceneradnjex emagent agent xemagent xagent policy xpolicy