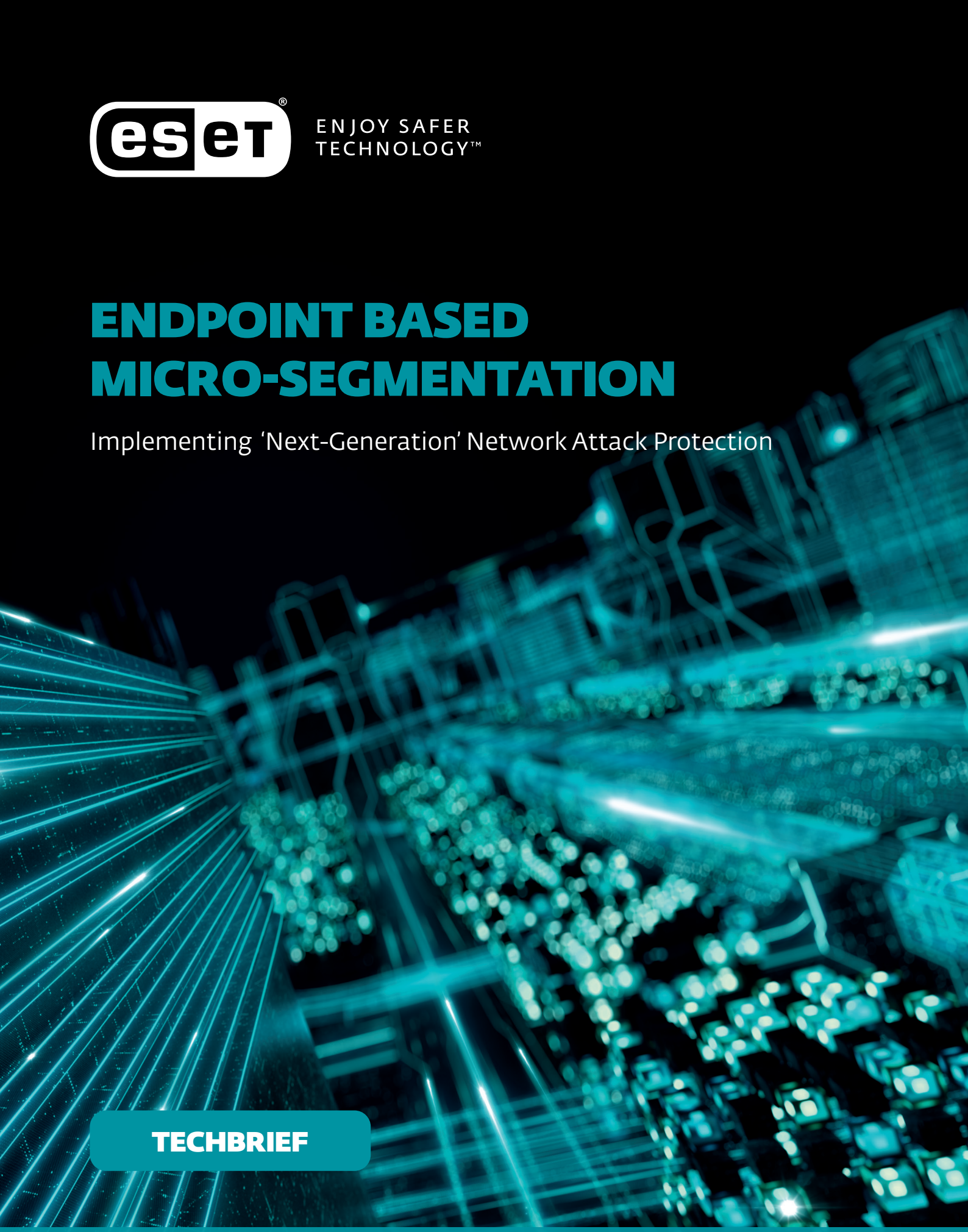
ENJOY SAFER TECHNOLOGY™

ENDPOINT BASED MICRO-SEGMENTATION

Implementing 'Next-Generation' Network Attack Protection



TECHBRIEF

Auteurs:

Michael van der Vaart - Chief Technology Officer
Donny Maasland - Lead Security Engineer
Jamil Sosa - Security Engineer

Versie 1.0

INHOUDSOPGAVE

INTRODUCTIE

De afgelopen jaren is een duidelijke verschuiving te zien in de TTP's (Tactics, Techniques and Procedures) van cybercriminelen. Waar vroeger bepaalde gegevens of systemen direct doelwit waren van aanvallen, wordt het steeds gebruikelijker voor aanvallers om eerst beperkte toegang (foothold) tot een netwerk te verschaffen en vervolgens door middel van "lateral movement" toegang te verkrijgen tot andere systemen binnen hetzelfde netwerk totdat het einddoel bereikt is. Recente voorbeelden van deze methodes zijn de aanvallen met malware als "WannaCry", "NotPetya" en "BadRabbit".

Bij deze aanvallen viel op dat niet serversystemen, maar (legitieme software op) werkstations, grotendeels misbruikt werden om de aanval uit te voeren. Deze tech brief is geschreven met het doel alle systemen binnen het netwerk optimaal te beschermen tegen dit soort aanvallen, door middel van een whitelist-principe.

DEFENSE IN DEPTH & MULTI-LAYERED SECURITY

De security oplossingen van ESET worden al meer dan 30 jaar ontwikkeld met het "defense in depth" principe. Zo biedt de meest recente versie van ESET Endpoint Security niet alleen traditionele beveiligingstechnieken, maar ook Next Gen-methodes zoals Machine Learning, Artificial Intelligence en de kracht van de Cloud. Deze technieken worden bovendien niet alleen gebruikt om het lokale systeem te beschermen, maar zijn ook volledig geïntegreerd in bijvoorbeeld de Network Attack Protection module, waarbij het systeem onder constante bescherming van netwerkgebaseerde aanvallen staat. De combinatie van deze technieken en modules bieden een geoptimaliseerde en intelligente manier van bescherming in bijna alle situaties, maar geeft beheerders en security specialisten ook de benodigde handvatten om het security maturity niveau naar nieuwe hoogten te brengen.

Let op: NAP is onderdeel van ESET Endpoint Security.

ENDPOINT BASED MICRO-SEGMENTATION

Met behulp van deze tech brief wordt de Network Attack Protection module op de endpoints in het netwerk geconfigureerd om te werken via het "whitelist" principe. Dat wil zeggen, het systeem verleent alleen toegang tot netwerkservices zoals Remote Desktop (RDP), Server Message Block (SMB), Windows Management Instrumentation (WMI) en Remote Procedure Call (RPC) interfaces aan goedgekeurde systemen binnen het netwerk. Deze whitelist staat bij de ESET security oplossingen bekend als de Trusted Zone. Voor systemen welke zich niet in de Trusted Zone bevinden, zal een endpoint zo goed als onzichtbaar zijn binnen het netwerk.

MAAK LATERAL MOVEMENT ONMOGELIJK

Het resultaat van deze configuratie is dat elk endpoint zich in een afgesloten "micro-segment" bevindt en alleen kan communiceren met systemen gespecificeerd in de Trusted Zone. In de praktijk betekent dat wanneer één van de endpoints succesvol gecompromitteerd wordt door een aanvaller, het onmogelijk is om middels lateral movement andere endpoints te compromitteren en zo een betere foothold binnen het netwerk te realiseren, of malware verder binnen het netwerk te verspreiden.

IMPLEMENTATIE VAN ENDPOINT MICRO-SEGMENTATION

De implementatie van de bovengenoemde configuratie bestaat globaal gezien uit twee stappen:

- Installeren en configureren van de "ESET Authentication Server"
- Configureren van de endpoints met de "ESET Remote Administrator"

Deze handleiding gaat uit van een werkende ESET Remote Administrator binnen het netwerk.

ESET AUTHENTICATION SERVER

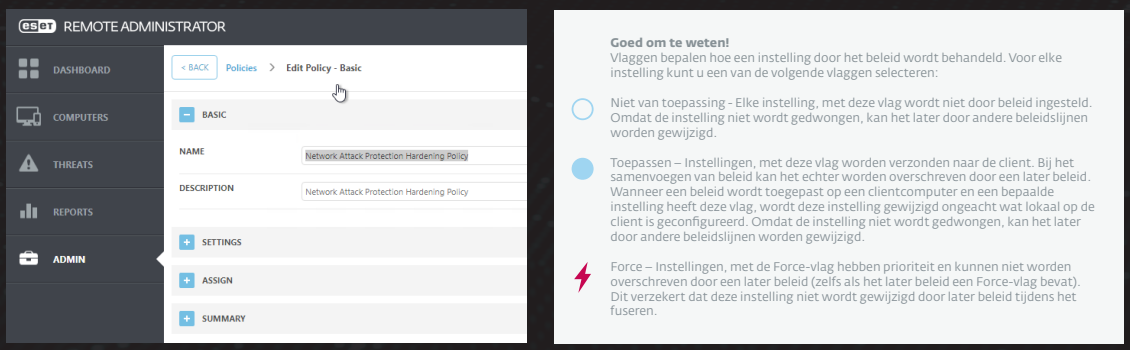
De ESET Authentication Server is een kosteloos programma waarmee het mogelijk is een netwerk op basis van "Public-key Cryptography" te authenticeren en verifiëren. Het installeren en configureren van de ESET Authentication Server valt buiten de scope van deze tech brief, maar is uitgebreid beschreven in het volgende artikel: https://support.eset.com/kb2501/.

Let op: noteer de gekozen "Zone name" bij het configureren van de ESET Authentication Server. Deze is nodig bij de configuratie van de endpoints.

ENDPOINT CONFIGURATIE

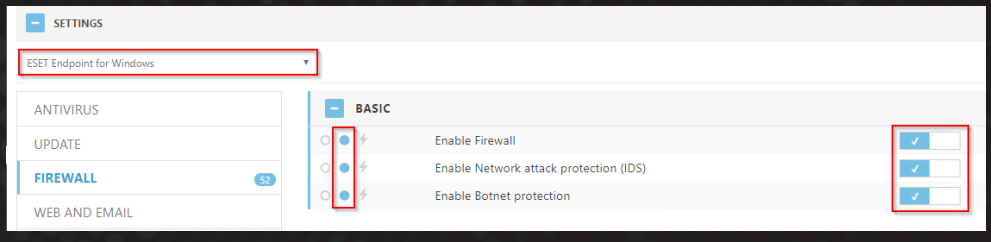
In deze tech brief worden de endpoints geconfigureerd door middel van een "Policy" met behulp van de ESET Remote Administrator. Als deze procedure niet of niet geheel bekend is, kan meer informatie verkregen worden uit het volgende artikel: https://support.eset.com/kb3594/.

Stap 1 Maak voor de configuratie van de endpoints een nieuwe policy aan en kies hiervoor een geschikte naam, bijvoorbeeld "Network Attack Protection Hardening".



Stap 2 Kies onder "Settings" als product "ESET Endpoint for Windows", en klik vervolgens op "Personal Firewall". Schakel in het gedeelte "BASIC" de volgende opties in:

- Enable Firewall
- Enable Network Attack Protection (IDS)
- Enable Botnet Protection



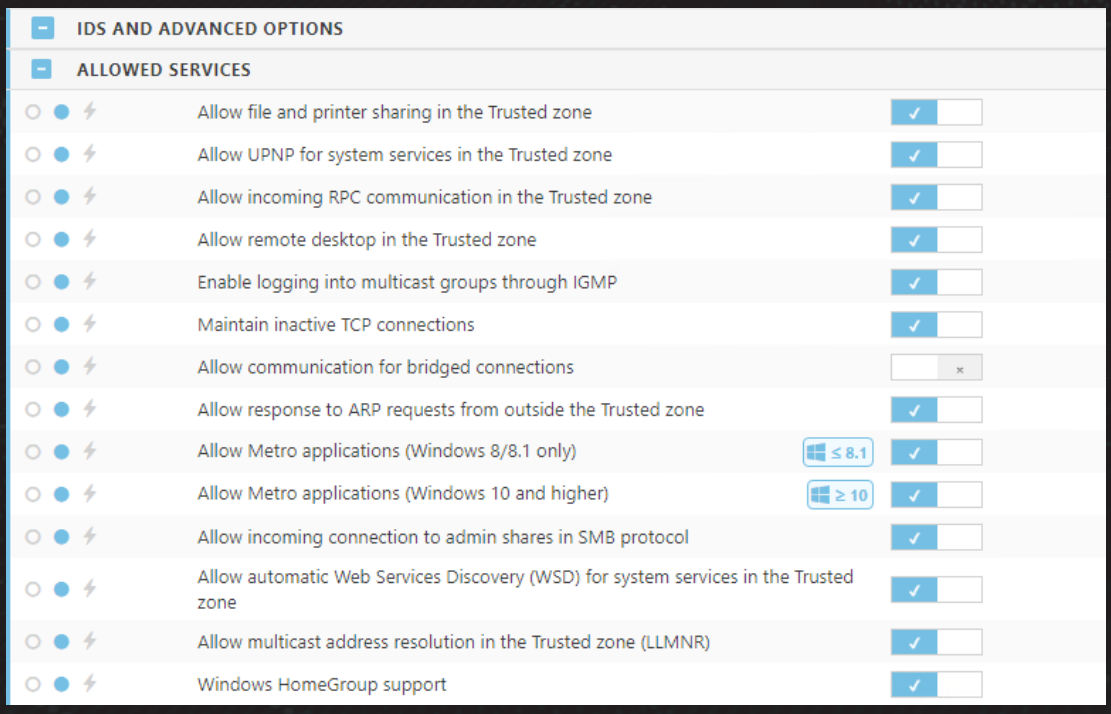
ENDPOINT CONFIGURATIE

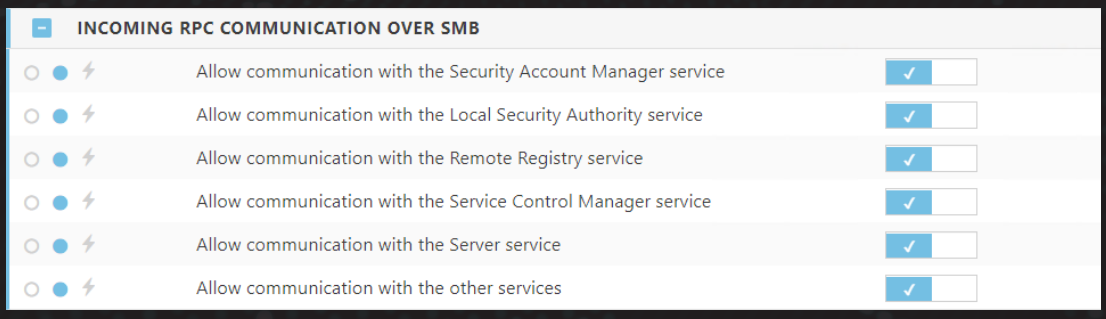
Stap 3

Navigeer vervolgens naar "ADVANCED" -> "IDS AND ADVANCED OPTIONS", en neem de configuratie zoals vertoond over, dit biedt een solide basisconfiguratie. Controleer welke opties mogelijk anders geconfigureerd dienen te worden voor een optimale bescherming van de omgeving in kwestie. Meer achtergrondinformatie over (één van) de instellingen is te vinden op de volgende pagina:

https://help.eset.com/ees/6/en-US/idh_config_epfw_advanced_settings.htm?zoom_highlightsub=ids+options

BELANGRIJK
De beschikbaarheid van bepaalde opties in dit venster kan variëren en is afhankelijk van het type of de versie van uw ESET-product en module voor de firewall, maar ook van de versie van uw besturingssysteem.



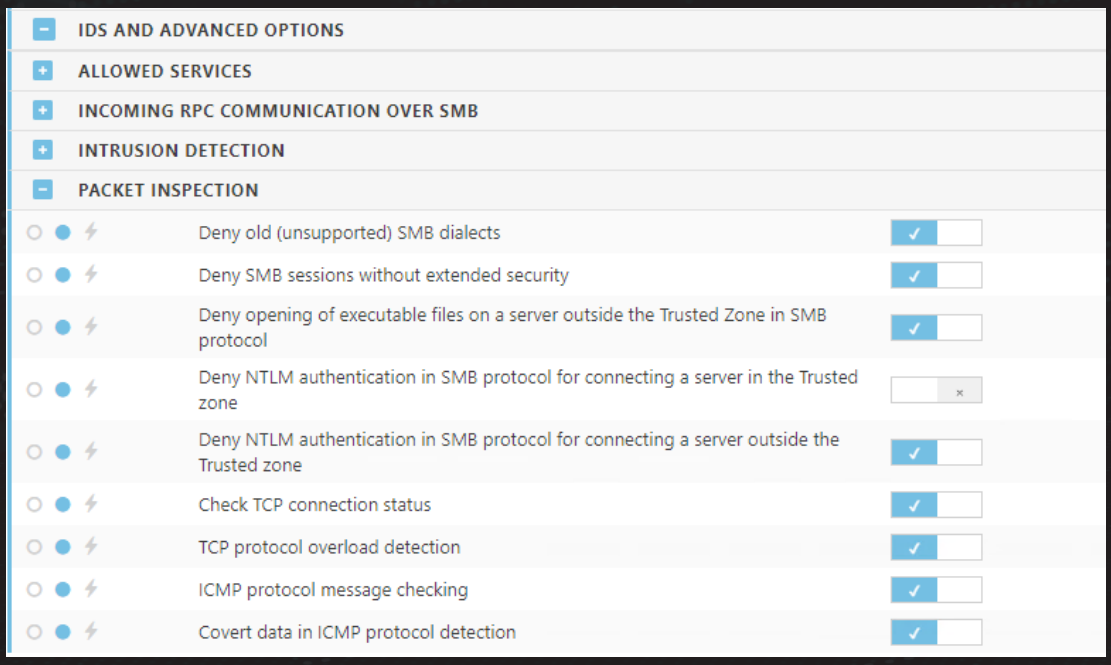


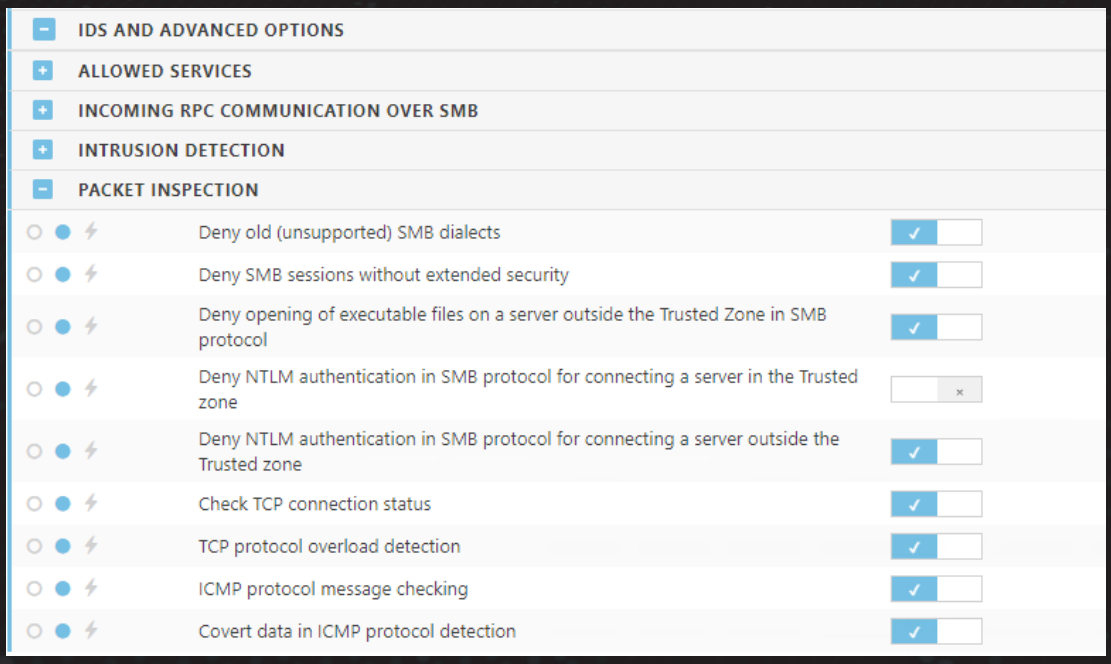
ENDPOINT CONFIGURATIE

Stap 3

Navigeer vervolgens naar "ADVANCED" -> "IDS AND ADVANCED OPTIONS", en neem de configuratie zoals vertoond over, dit biedt een solide basisconfiguratie. Controleer welke opties mogelijk anders geconfigureerd dienen te worden voor een optimale bescherming van de omgeving in kwestie. Meer achtergrondinformatie over (één van) de instellingen is te vinden op de volgende pagina:

https://help.eset.com/ees/6/en-US/idh_config_epfw_advanced_settings.htm?zoom_highlightsub=ids+options

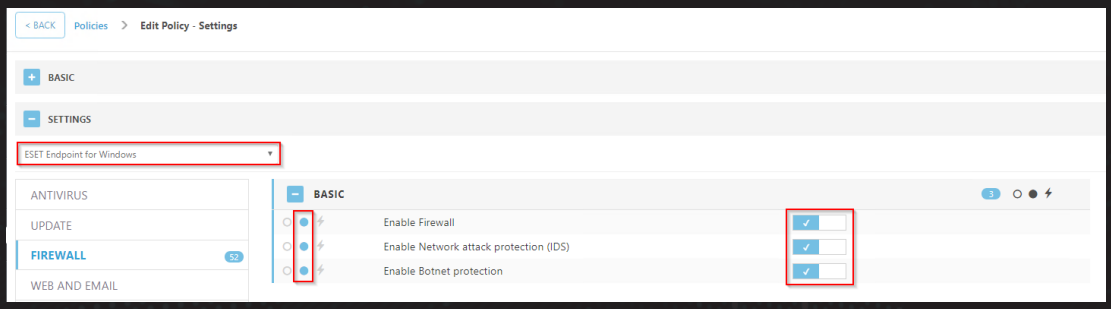




ENDPOINT CONFIGURATIE

Stap 4

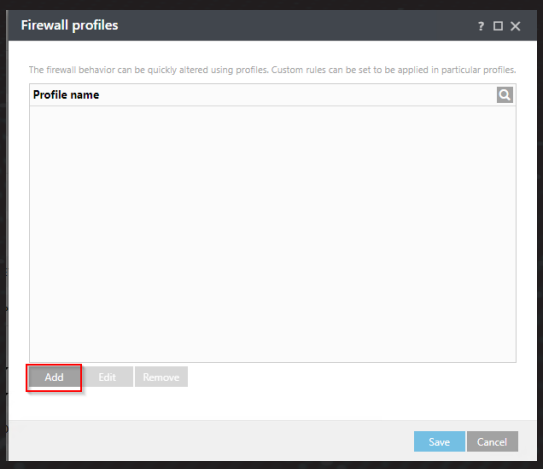
Navigeer vervolgens naar "KNOWN NETWORKS". Selecteer hier "Mark as public" voor de optie "Protection type of new networks". Schakel vervolgens "Do not ask for protection type of new networks. Automatically mark new networks as public" in. Klik daarna naast "Known networks" op "Edit".

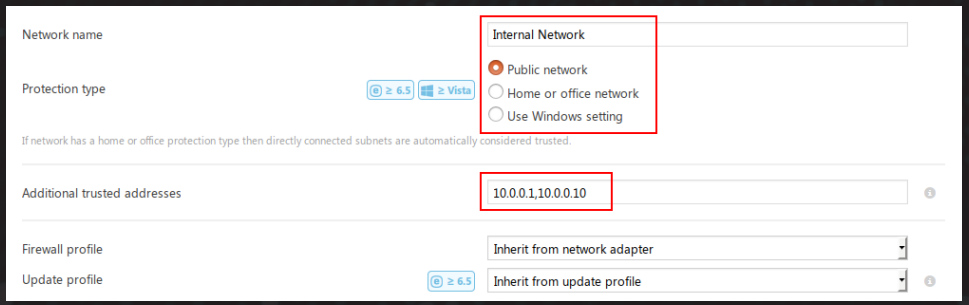


Stap 4

Klik in het venster dat opent op "Add" en configureer de volgende opties:

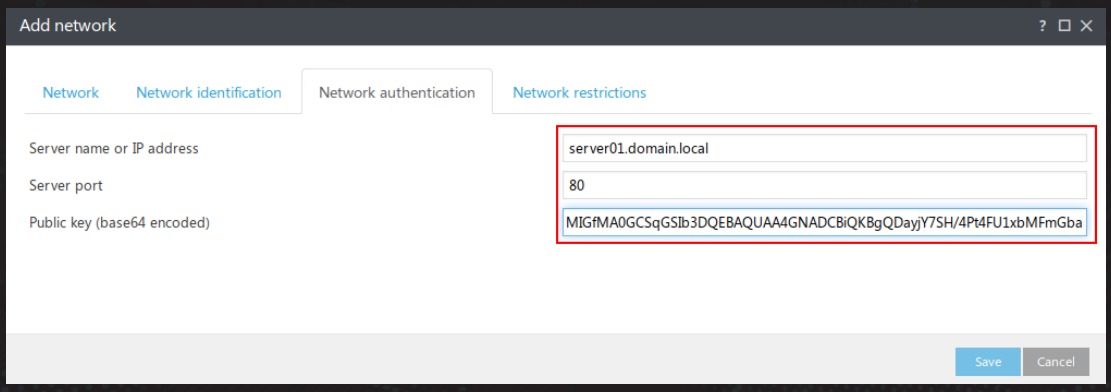
- **Network name:** Internal Network (**BELANGRIJK:** Kies hier voor dezelfde naam als voor de "Zone name" die tijdens de configuratie van de ESET Authentication Server gekozen is.)
- **Protection Type:** Public network
- **Additional trusted addresses:** Voer hier de systemen in welke toegestaan zijn om verbinding te maken met de netwerk-services van de endpoints. Denk hier bijvoorbeeld aan de Domain Controller, SCCM server of generieke beheerserver. Let op dat u het aantal adressen zo laag mogelijk houdt.
- **(Optioneel) Firewall Profile:** een firewall profiel welke alleen voor deze zone geldt.
- **(Optioneel) Update Profile:** een update profiel welke alleen voor deze zone geldt.





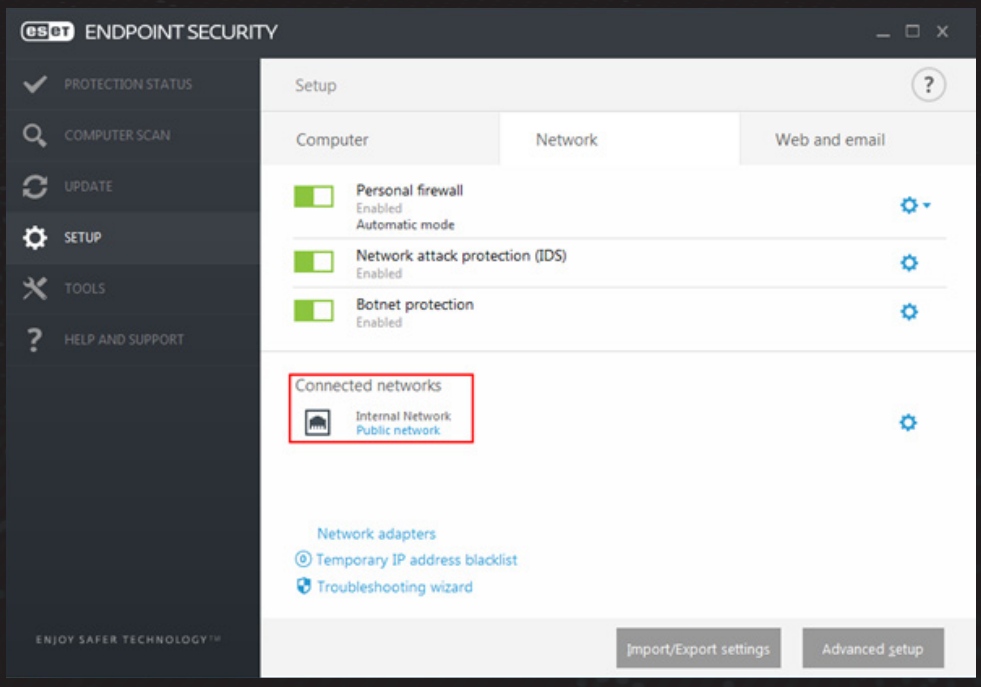
ENDPOINT CONFIGURATIE

Stap 4 Klik vervolgens op de kop "Network Authentication", en vul de details van de ESET Authentication Server in.



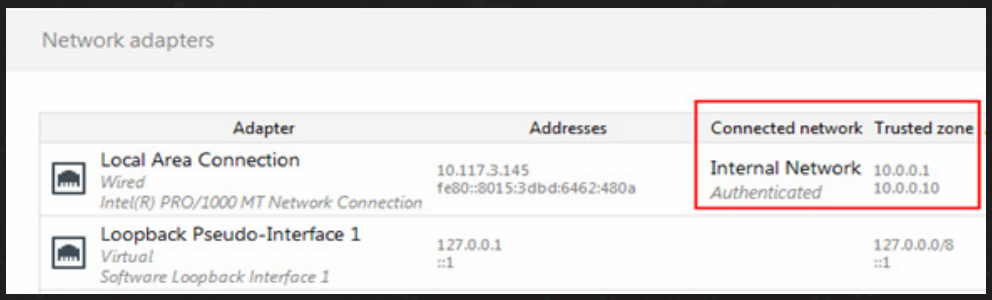
Stap 4 Kies vervolgens tweemaal voor "Save". Klap hierna het gedeelte "ASSIGN" uit en klik op "ASSIGN...". Selecteer in het venster wat zich opent op welke systemen de Policy van toepassing is. Klik hierna op "Finish".

Stap 5 Als de configuratie succesvol is afgerond kan op de endpoints worden gecontroleerd of de instellingen correct zijn door te navigeren naar "Setup -> Network". Controleer of onder "Connected Networks" het opgegeven netwerk wordt genoemd, en dat "protection type" op "Public Network" staat.



ENDPOINT CONFIGURATIE

Stap 5 Klik vervolgens op "Network adapters" en controleer of de trusted zone juist is toegepast, en of de tekst "Authenticated" te zien is onder het kopje "Connected Network".



Stap 5 Indien dit het geval is, zal het endpoint de adressen in de Trusted Zone toegang verlenen tot de beschikbare netwerkservices, mits het in staat is het netwerk succesvol te authentiseren met behulp van de ESET Authentication Server. Indien deze authenticatie mislukt, of als de ESET Authentication Server niet bereikt kan worden, zal de Trusted Zone leeg blijven en zal geen enkel systeem in staat zijn met het endpoint te verbinden.

TOT SLOT

Door de configuratie zoals beschreven in deze tech brief over te nemen wordt het security maturity level van de organisatie naar een hoger niveau gebracht. Het verdient echter de aanbeveling om kritisch te kijken naar de beschikbare opties van NAP in ESET Endpoint Security om de configuratie meer toe te spitsen op de organisatie.

Zo kunnen bijvoorbeeld firewall profielen worden gebruikt om te zorgen dat een endpoint buiten het interne netwerk enkel een VPN verbinding met het bedrijf kan maken alvorens verder netwerkverkeer wordt toegestaan, of kan zelfs Address Resolution Protocol (ARP) verkeer van buiten de trusted zone worden geblokkeerd, waardoor het eindpoint op laag 2 van het OSI-model onzichtbaar wordt voor andere endpoints.

ESET technologie wordt continu doorontwikkeld waardoor deze tech brief eveneens aangepast zal worden aan moderne ontwikkelingen.

CYBERSECURITY EXPERTS ON YOUR SIDE

ESET NEDERLAND
Trapezium 304
3364 DL, Sliedrecht

VRAGEN OF INFORMATIE?
0184 - 64 77 40
Verkoop@eset.nl

TECHNISCH SUPPORT?
0184 - 64 77 45
Support@eset.nl