

Fail2ban op UniFi activeren

Om je UniFi Network Application beter te beveiligen, kan je met Fail2ban foute inlogpogingen op je controller blokkeren.

Wat is Fail2ban?

Fail2ban is een tool wat op je server draait. Deze tool controleert de logboeken van je server op foute inlogpogingen. Wanneer een bepaald aantal inlogpogingen bereikt zijn, dan wordt het IP adres van deze persoon voor enige tijd geblokkeerd. Zo wordt voorkomen dat kwaadwilligen je continu je account proberen te hacken.

Fail2ban is bijvoorbeeld steeds actief voor SSH verbindingen, op de NGINX webserver, enz.

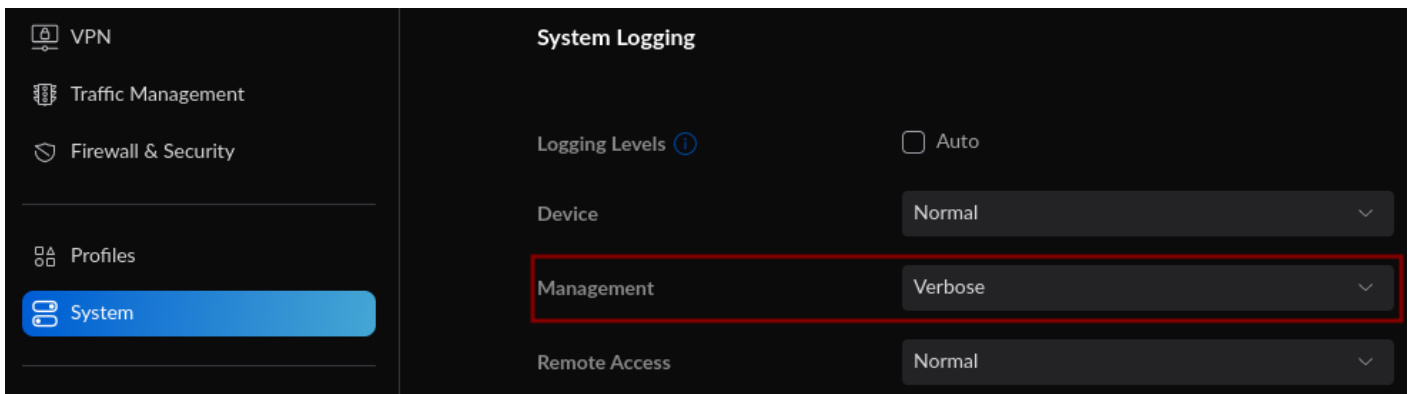
Fail2ban voor UniFi

Fail2ban kan ook de inlogpogingen op jouw UniFi Network Application monitoren. Wanneer er binnen de 10 minuten 5 foute inlogpogingen gedetecteerd worden, dan wordt het IP adres 15 minuten geblokkeerd.

Om Fail2ban op jouw UniFi Network Application te activeren, moet je enkel nog het log-level aanpassen.

1. Ga naar de instellingen van je Controller.
2. Ga naar '**System**'.
3. Onder '**System Logging**':
 1. Vink bij de instelling '**Logging Levels**' het vakje '**Auto**' uit.
 2. Pas de instelling '**Management**' aan naar '**Verbose**'.

Fail2ban zal vanaf nu foute inlogpogingen detecteren en blokkeren.



Ben je zelf geblokkeerd?

Was je niet meer heel zeker van je wachtwoord en heb je jezelf buitengesloten? Kan gebeuren. Wacht een kwartiertje tot de blokkade van jouw IP adres opgeheven wordt. Op het aanmeldscherm van UniFi vind je een link om je wachtwoord te herstellen.

Tip: gebruik een wachtwoord manager zoals [Bitwarden](#) om sterke wachtwoorden te maken, te maken en te delen met je collega's.

Revisie #7

Gemaakt: 23 mei 2022 14:52:34 door Kris Lowet

Bijgewerkt: 23 mei 2022 15:22:55 door Kris Lowet