Extra Veilig Internet

Wat is Extra Veilig Internet?

Met Extra Veilig Internet (EVI) maak je gebruik van een beter beveiligde internetverbinding. Zo kunnen jij en je medewerkers nog zorgelozer internetten. Extra Veilig Internet is gebaseerd op de FortiGate security-oplossing die is geïmplementeerd in het netwerk. hoeft hiervoor dus geen extra apparatuur of software te installeren op locatie. EVI maakt gebruik van het FortiGuard internetfilter; DNS-filter, webfilter en antivirusfunctionaliteit, om de verbinding te beschermen tegen malware, ransomware en virussen en onveilige websites te blokkeren.

Waar beschermt Extra Veilig Internet mij tegen?

Extra Veilig Internet werkt op alle werkplekken, smartphones en andere devices die via de met EVI uitgeruste EVC naar het internet gaan.

Let op: EVI is geen firewall en beschermd niet tegen virussen die op andere manieren op een device terecht kunnen komen (USB, VPN etc). Een goede endpoint security zoals F-Secure of Microsoft Defender blijft dan ook noodzakelijk.

EVI beschermt de gebruikers wel tegen:

- ✓ **Phishing**
  Een e-mail met een foute link erin is een veelgebruikte manier om je gegevens te achterhalen of je over te halen om geld over te maken.

- ✓ **Ransomware**
  Ransomware is een type malware, ofwel kwaadaardige software, die een computer blokkeert of bestanden versleutelt. Pas als je losgeld (ransom) betaalt zou je de computer of de bestanden weer kunnen gebruiken.

- ✓ **Cryptojacking**
  Cryptojacking is een online bedreiging die zich op een computer of mobiel apparaat verbergt en de rekenkracht van het apparaat gebruikt om vormen van online geld, die bekend staan als cryptovaluta's, te "delven". Het is een dreiging die webbrowsers kan overnemen en allerlei apparaten kan binnendringen, van desktops en laptops tot smartphones en zelfs netwerkservers.

- ✓ **Malware**
  Marlware of "kwaadaardige software", is een overkoepelende term die een kwaadaardig programma of code beschrijft die schadelijk zijn voor computersystemen.

- ✓ **Botnets**
  Een vorm van een virus waarmee een device geïnfecteerd kan zijn. Botnets gebruiken besmette hosts om veelal kwaadwillende acties te ondernemen. Is een werkplek onderdeel van een botnet dan kan deze worden ingezet voor spam of een ddos aanval op een website zonder dat de gebruiker zich hiervan bewust is.

- ✓ **Downloaden van virussen en schadelijke content.**
  Het downloaden virussen en sites die proberen scripts uit te voeren met schadelijke content worden geblokkeerd. Ook als een website is gecompromitteerd maar nog niet opgenomen in EVI werkt deze bescherming. Https downloads kunnen niet worden ingezien en vereisen separatie endpoint security.

Op welke IP adressen werkt Extra Veilig Internet?

EVI werkt met zowel losse IPv4 adressen als met subnets. Voor bestaande verbindingen geldt dat het oorspronkelijke IP adres (subnet) wordt meegenomen naar EVI. EVI kan op dit moment nog niet worden gebruikt in combinatie met IPv6.

Hoe worden de alerts getoond?

Als een gebruiker middels een browser naar een website of IP adres gaat welke voorkomt in de Fortiguard database dan toont EVI een waarschuwingspagina. Applicaties maar ook virussen die “onder water” naar zo’n website gaan worden wel geblokkeerd maar krijgen geen melding.

Is er een log beschikbaar?

EVI kan helaas geen logging beschikbaar stellen op gebruikersniveau van wat er wordt geblokkeerd. De kans is hierbij namelijk groot dat er veel (bijzondere) persoonsgegevens worden verwerkt. In het kader van de AVG is de optie logging dan ook niet actief.

Heeft Extra Veilig Internet een looptijd?

Extra Veilig Internet heeft geen looptijd en geen opzegtermijn. Dit betekend dat EVI per direct kan worden uitgeschakeld. Het modem zal wel een nieuwe PPP sessie moeten opzetten om de opheffing af te ronden. Alle eventueel verzamelde informatie van de order wordt direct vernietigd en is na opheffen niet meer beschikbaar.