

Begrijp SWG-verkeersdecodering met ingeschakelde HTTPS-decodering

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

[Oorzaak](#)

Inleiding

In dit document wordt beschreven hoe Cisco Secure Web Gateway (SWG) omgaat met het ontsleutelen van verkeer wanneer HTTPS-decodering is ingeschakeld.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Secure Web Gateway.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

In een regel voor webbeleid die is ingesteld met HTTPS-decodering ingeschakeld, wordt verkeer alleen gedecodeerd als er een Server Name Indicator (SNI) aanwezig is in de TLS-handshake.

Oplossing

Het beleid voor beveiliging en acceptabel gebruik kan nog steeds worden toegepast op basis van de bestemmingsservers waarnaar het verzoek wordt verzonden. Bestemmingslijsten kunnen

worden gemaakt voor deze bestemmingsservers en de regels kunnen dienovereenkomstig worden afgedwongen.

Alle blokken voor DNS-beleid voor Tunnels en AnyConnect kunnen nog steeds van toepassing zijn.

Oorzaak

Dit gedrag is door ontwerp.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.