Secure Access Policy Enforcement voor bepaalde toepassingsprotocollen

Inhoud

Inleiding

Dit document beschrijft de handhaving van het beleid voor beveiligde toegang bij het gebruik van bepaalde toepassingsprotocollen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beveiligde toegang
- File Transfer Protocol (FTP)
- Transmission Control Protocol (TCP)
- Firewall as a Service (FWaaS)
- Secure Shell (SSH)
- Hyper Text Transfer Protocol (HTTP)
- Snelle UDP-internetverbinding (QWIC)
- Secure Mail Transfer Protocol (SMTP)

Achtergrondinformatie

Een typische FWaaS-test om de handhaving van het toepassingsprotocol te evalueren is een test van het protocolmisbruik.

De test voor dit scenario bestaat meestal uit het maken van een beleid dat een specifiek toepassingsprotocol blokkeert, zoals FTP/SSH op een niet-standaard poort. Bijvoorbeeld het toestaan van FTP alleen op TCP poort 21 en het blokkeren van FTP op TCP poort 80.

Secure Access maakt gebruik van OpenAppID-protocoldetectie om toepassingsprotocollen zoals FTP, SSH, QUIC, SMTP en andere te detecteren. en gebruikt een Secure Web Gateway om HTTP(S)-verkeer te beveiligen.

Probleem: De test van de beleidshandhaving voor bepaalde toepassingsprotocollen op TCP 80/443 resulteert in verbindingsonderbreking en geen logboeken worden geproduceerd in Veilige Toegang

Onder bepaalde omstandigheden, zoals pogingen om bepaalde protocollen zoals FTP toe te staan/te blokkeren op TCP-poort 80/443, komen we een situatie tegen waar de eerste verbinding tussen de client en de server wordt onderschept door de proxy-engine, de TCP-handdruk is voltooid en dan de proxy-engine in Secure Access wacht op de client om verkeer te verzenden, maar het protocol vereist een server-side signaal om de client te bereiken.

Deze situatie leidt tot de verbindingstiming uit wegens de cliënt die op het serversignaal wachten en de volmacht vertraagt uiteindelijk de verbinding. En Secure Access genereert geen logbestanden voor dit type sessies.

Oplossing

Dit is een verwacht gedrag als gevolg van de manier waarop webverkeer wordt beveiligd door de Secure Access-architectuur en aangezien een dergelijke test niet-webverkeer betreft (FTP, SSH, Telnet, SMTP, IMAP en andere protocollen die in eerste instantie uitgaan van een server-side signaal) op webpoorten, worden er voor een dergelijke sessie geen logs gegenereerd.

Gerelateerde informatie

- Gebruikershandleiding voor Secure Access
- Secure Access-communitypagina
- Technische ondersteuning en documentatie – Cisco Systems

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.