Met een wachtwoord beveiligde configuratie voor het downloaden van ZIP-bestanden

Inhoud

uitgifte

Na de migratie naar Cisco Secure Access kunnen gebruikers geen wachtwoordbeveiligde (gecodeerde) ZIP-bestanden downloaden. De downloads mislukken consequent wanneer u probeert toegang te krijgen tot gecodeerde bestandsinhoud via de Secure Access-service. Dit probleem doet zich voor ondanks het feit dat het internetgebonden verkeersbeleid is geconfigureerd op een C8200-apparaat met meerdere beveiligingsregels, waaronder categoriegebaseerde blokkering, SSL-inspectiecontroles en sandboxfunctionaliteit.

Gebruikers ervaren volledige downloadfouten bij het proberen toegang te krijgen tot met een wachtwoord beveiligde ZIP-bestanden die eerder toegankelijk waren voordat de migratie voor beveiligde toegang plaatsvond. Het probleem blijft bestaan in meerdere tunnelgroepen en heeft gevolgen voor alle 15 geconfigureerde locaties.

milieu

- Cisco Secure Access (beveiligde toegang ORGid: 8320925)
- C8200-apparaat voor het beheer van internetgebonden verkeersbeleid
- Meerdere tunnelgroepen op 15 locaties (TK-TG en andere)
- SSL-inspectiebeleid met zowel ingeschakelde als uitgeschakelde configuraties
- Sandbox-beveiligingsprofielen ingeschakeld voor bepaalde beleidsregels
- IPS-profielen geconfigureerd volgens specifieke toegangsregels

resolutie

De oplossing voor het toestaan van met een wachtwoord beveiligde ZIP-bestandsdownloads in Cisco Secure Access omvat het configureren van de instelling Toestaan van toegang tot gecodeerde bestanden en het implementeren van de juiste oplossingen wanneer dat nodig is.

primaire configuratiemethode

Stap 1: Toegang tot de configuratie van het Cisco Secure Access-beleid

Navigeer naar het specifieke toegangsbeleid dat het getroffen verkeer in uw Cisco Secure Access-dashboard afhandelt.

Stap 2: Versleutelde bestandstoegang inschakelen

Zoek in het beleid Geavanceerde instellingen de optie Toegang tot gecodeerde bestanden toestaan en schakel deze in. Deze instelling wordt per regel geconfigureerd en bepaalt of gecodeerde inhoud via dat specifieke beleid kan worden benaderd.

Stap 3: De configuratie toepassen

Sla de beleidswijzigingen op en pas deze toe om ze actief te maken voor gebruikersverkeer.

Alternatieve workaround methode

Als de primaire methode het probleem niet oplost, voert u de in de volgende secties beschreven oplossing uit.

Stap 1: Identificeer de betreffende URL's

Bepaal de specifieke URL's of domeinen waar met een wachtwoord beveiligde ZIP-bestanden worden gehost en downloadfouten veroorzaken.

Stap 2: Configureren Niet-ontsleutelen lijst

Voeg de geïdentificeerde URL's toe aan de lijst Niet decoderen in uw Cisco Secure Access-configuratie. Dit voorkomt SSL-inspectie op deze specifieke URL's.

Stap 3: SSL-inspectiebypassbeleid maken

Zorg ervoor dat een toegangsbeleid met SSL-inspectie uitgeschakeld is geconfigureerd om verkeer naar deze URL's te verwerken.

Dit beleid moet:

- SSL-inspectie uitgeschakeld
- Alle beveiligingsprofielen uitgeschakeld
- Hogere prioriteit dan SSL-inspectiebeleid

Referentie beleidsconfiguratie

De beleidsvolgorde die in de volgende subsecties wordt beschreven en de configuraties ervan kunnen worden gebruikt als referentie voor een correcte verwerking van het verkeer.

Beleid 1: op categorieën gebaseerde blokkeringsregel

- Beleidsnaam: IA-naar-Internet Content Block
- IPS-profiel: geen

- Doel: specifieke inhoudscategorieën blokkeren
- Doel: Alle tunnelgroepen

Beleid 2: SSL-inspectie uitgeschakeld regel

- Beleidsnaam: IA-SSL-Inspection-MUKOU
- IPS-profiel: uitgeschakeld
- Beveiligingsprofielen: Alle uitgeschakeld
- Doel: Alle tunnelgroepen

Beleid 3: SSL-inspectieregel

- Beleidsnaam: IA-SSL-Inspection
- IPS-profiel: ingeschakeld
- Beveiligingsprofielen: Sandbox-functionaliteit ingeschakeld
- Doel: Alle tunnelgroepen

Belangrijke configuratieopmerkingen

Er bestaat geen equivalent van Global Settings voor de functionaliteit Allow access to encrypted files. Deze instelling moet zo nodig worden geconfigureerd op het afzonderlijke toegangsbeleid. Voor elk beleid waarvoor gecodeerde bestandstoegang vereist is, moet deze instelling expliciet zijn ingeschakeld in de configuratie Geavanceerde instellingen.

Wanneer u wijzigingen in de configuratie test, moet u voldoende tijd vrijmaken voor beleidspropagatie binnen de Cisco Secure Access-infrastructuur voordat u de functionaliteit valideert. Service-incidenten of onderhoudsvensters kunnen de testresultaten beïnvloeden en moeten worden overwogen bij het oplossen van problemen.

Oorzaak

Het probleem doet zich voor omdat Cisco Secure Access standaard de toegang tot gecodeerde bestanden blokkeert als beveiligingsmaatregel. Wanneer SSL-inspectie is ingeschakeld en wachtwoordbeveiligde of gecodeerde inhoud tegenkomt, voorkomt de service downloaden, tenzij expliciet is geconfigureerd om dergelijke toegang toe te staan. De instelling Toegang tot gecodeerde bestanden toestaan in de Geavanceerde instellingen van het toegangsbeleid regelt dit gedrag en zonder deze instelling ingeschakeld, worden gecodeerde ZIP-bestanden en soortgelijke inhoud geblokkeerd tijdens het downloadproces.

Bovendien kan SSL-inspectiebeleid interfereren met gecodeerde bestandsdownloads wanneer het inspectieproces de gecodeerde inhoud niet goed kan verwerken, waarvoor de gecodeerde bestandstoegangsinstelling of SSL-inspectiebypass voor de getroffen URL's vereist is.

Gerelateerde inhoud

- Geavanceerde beveiligingscontroles
- Cisco Technical Support en downloads

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.