Het blokkeren van het Secure Access Application Protocol voorkomt internetverbinding

Inhoud

- uitgifte
- milieu
- resolutie
  - Stap 1: Identificeer de blokkeringsregel
  - Stap 2: Toepassingsinstellingen wijzigen
  - Stap 3: Wijzigingen toepassen en verifiëren
- Oorzaak
- Gerelateerde inhoud

---

uitgifte

Na de migratie naar Cisco Secure Access kregen gebruikers te maken met een geblokkeerde internetverbinding wanneer ze toegang probeerden te krijgen tot webservices. Het specifieke symptoom was dat HTTP-verkeer werd geblokkeerd door het beveiligingsbeleid, waardoor de toegang tot legitieme websites en toepassingen werd verhinderd.

De gegevens van de blokkeringsgebeurtenis lieten deze kenmerken zien:

- Actie: geblokkeerd
- Reden gebeurtenisblok: AC_RULE_MATCH_BLOCK
- Bestemming: http://www.bing.com/api/shopping/v1/user/shoppingsettings

- Poort van bestemming: 443
- Categorieën: Uncategorized
- Toepassingscategorie: Zoeken
- Toepassingsprotocol: Hypertext Transfer Protocol
- Protocol: TCP

milieu

- Implementatie van Cisco Secure Access
- Actief beveiligingsbeleid met beperkingen van het toepassingsprotocol

resolutie

De oplossing houdt in dat de configuratie van de beveiligingsregel wordt gewijzigd om HTTP-toepassingsprotocolverkeer mogelijk te maken, terwijl de beveiligingspositie voor echt niet-vertrouwde toepassingen wordt behouden.

Stap 1: Identificeer de blokkeringsregel

Zoek de specifieke regel die het blok veroorzaakt in de beheerinterface voor beveiligde toegang:

- Regelnaam: Test
- Huidige configuratie: blok Toepassingsinstellingen gebruiken als bestemming.

Stap 2: Toepassingsinstellingen wijzigen

Open de configuratie van de regel en controleer de naam van de toepassingsinstellingen in

Bestemming:

- Navigeer naar Bronnen > Internet- en SaaS-bronnen > Toepassingslijsten. Klik vervolgens op de applicatie.
- Zoek de instellingen van het toepassingsprotocol.
- Schakel HTTP uit of verwijder het uit de lijst met geblokkeerde toepassingsprotocollen.
- Ervoor zorgen dat andere beveiligingsmaatregelen van kracht blijven voor feitelijke, niet-vertrouwde toepassingen.

Stap 3: Wijzigingen toepassen en verifiëren

Sla de regelwijzigingen op en test de connectiviteit:

1.- Pas de configuratiewijzigingen toe op het actieve beleid.

2.- Test de internetverbinding met eerder geblokkeerde bestemmingen.

3.- Bewaking van beveiligingslogs om te garanderen dat legitiem HTTP-verkeer nu is toegestaan.

4.- Controleer of andere beveiligingsmaatregelen effectief blijven.

Oorzaak

De hoofdoorzaak was een te restrictieve configuratie van beveiligingsregels in Cisco Secure Access. De regel is geconfigureerd om al het HTTP-applicatieprotocolverkeer te blokkeren, waardoor legitieme webbrowsing en applicatietoegang werden voorkomen. De brede toepassing van het blokkeren van HTTP-protocollen had gevolgen voor de normale internetverbinding voor gebruikers die toegang hadden tot legitieme webservices en toepassingen die gebruikmaken van HTTP/HTTPS-protocollen.

Gerelateerde inhoud

- 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.