

Secure Access Client-based ZTA-postuur configuratie en gedragsspecificaties

Inhoud

uitgifte

Er zijn vragen gerezen over het specifieke gedrag en de configuratiemogelijkheden van de Cisco Secure Access client-based Zero Trust Access (ZTA) posture functionaliteit bij gebruik voor internettoegang. De specifieke punten van zorg waren onder meer:

- Of de postuur-eisen van het besturingssysteem een configureerbare respijtpriode van maximaal 365 dagen ondersteunen waarin apparaten de ZTA-module nog steeds kunnen gebruiken om toegang te krijgen tot internetbestemmingen, zelfs als ze niet voldoen aan de vereiste OS-versie.
- Of andere houdingseisen dan het besturingssysteem, zoals firewall, systeemwachtwoord, onder andere, resulteren in onmiddellijke blokkering van de bestemmingstoegang wanneer niet wordt voldaan.
- Of aangepaste waarschuwingsberichten of andere acties dan blokkering (zoals bewaking) kunnen worden geconfigureerd voor defecten in de posturatievereisten via de interface voor beveiligde toegang.

milieu

- Cisco Secure Access met Zero Trust Access (ZTNA)-functionaliteit
- Implementatie van ZTA-houding op clientbasis
- Gebruiksscenario voor internettoegang
- Houdingseisen, waaronder voorwaarden voor besturingssysteem, firewall en systeemwachtwoord

resolutie

De verduidelijkingen die in de volgende secties worden beschreven, zijn verstrekt met betrekking tot het gedrag en de configuratiemogelijkheden van ZTA op basis van Secure Access-client.

Aflossingsvrije periode van de houding van het besturingssysteem

Het beschreven gedrag van de postuur van het besturingssysteem is correct. Wanneer een postuur van het besturingssysteem is geconfigureerd, ondersteunt deze een configureerbare respijtp periode van maximaal 365 dagen. Tijdens deze respijtp periode kunnen apparaten die niet voldoen aan de vereiste OS-versie nog steeds de ZTA-module gebruiken om toegang te krijgen tot internetbestemmingen terwijl ze upgraden naar de doelversie.

Houdingseisen voor niet-werkend systeem

Voor andere houdingsomstandigheden dan het besturingssysteem (zoals firewall, systeemwachtwoord en andere beveiligingsmaatregelen) wordt de toegang tot bestemmingen onmiddellijk geblokkeerd wanneer niet aan deze vereisten wordt voldaan. Deze houdingstypen ondersteunen niet de functionaliteit van de respijtp periode die beschikbaar is voor vereisten van het besturingssysteem.

Houdingsfouten en aangepaste berichten

Acties voor defecten in de houdingsvereisten worden beheerd via de configuratie van het toegangsbeleid.

Het toegangsbeleid ondersteunt meerdere actietypen, waaronder:

- Allow (toestaan)
- Block (blokkeren)
- waarschuwen

- isoleren

Aangepaste waarschuwingsberichten en meldingspagina's voor houdingsfouten kunnen worden geconfigureerd via de profielinstellingen voor toegangsbeleid en beveiliging. Het beheer van de waarschuwings- en meldingspagina's verloopt via de documentatie- en configuratieinterface van de meldingspagina's beheren.

Dit betekent dat andere acties dan blokkeren (zoals monitoring via de Warn-actie) beschikbaar zijn en kunnen worden geconfigureerd, in tegenstelling tot de eerste beoordeling dat alleen blokkerende acties mogelijk waren.

Oorzaak

De vragen vloeiden voort uit de noodzaak om de specifieke gedragsverschillen tussen de houdingseisen van het besturingssysteem en andere houdingstypen te begrijpen, evenals verduidelijking van de beschikbare configuratieopties voor het verwerken van houdingsfouten die niet onmiddellijk zichtbaar zijn in de Secure Access GUI-interface.

Gerelateerde inhoud

- Documentatie over meldingspagina's beheren voor beveiligde toegang
- [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.