De functie Bypass Behavior verifiëren voor Microsoft 365-compatibiliteit met beveiligde toegang

Inhoud

uitgifte

Bij het configureren van Cisco Secure Access met Microsoft 365-compatibiliteitsfunctie ingeschakeld, is er onzekerheid over de vraag of specifieke Microsoft-gerelateerde volledig gekwalificeerde domeinnamen (FQDN's) automatisch worden omzeild van Secure Web Gateway (SWG)-verwerking en TLS-decodering. Meer bepaald moet het bypass-gedrag voor deze domeinen worden verduidelijkt:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

Het primaire probleem draait om de vraag of deze domeinen handmatige toevoeging aan de lijst Niet decoderen vereisen of dat ze automatisch worden uitgesloten wanneer Microsoft 365-compatibiliteit is ingeschakeld. Bovendien is er verwarring over de interactie tussen SWG-niveau bypasses en IPS-niveau decryptie-instellingen, met name voor manage.microsoft.com, die wordt weergegeven in de documentatie suggereert handmatige Do Not Decrypt List configuratie kan nog steeds nodig zijn.

milieu

- Cisco Secure Access
- Microsoft 365-compatibiliteitsfunctie ingeschakeld
- Secure Web Gateway (SWG)-inspectie en TLS-decodering geconfigureerd
- IPS-decoderingsbeleid in gebruik
- Microsoft-beheer- en updateservices waarvoor connectiviteit vereist is

resolutie

Het gedrag van de Microsoft 365-compatibiliteitsfunctie werd geverifieerd door middel van laboratoriumtests met deze bevindingen:

Microsoft 365 Compatibility Feature Scope

De compatibiliteitsfunctie Microsoft 365 stelt Microsoft 365-gerelateerde domeinen die zijn gemarkeerd als "Optimize" en "Allow" in de eindpuntcategorieën van Microsoft vrij van SWG-inspectie en beleidshandhaving. Hierdoor kan het verkeer naar die domeinen ongewijzigd door de SWG-laag gaan.

Resultaten van laboratoriumtests

Het testen werd uitgevoerd in een gecontroleerde laboratoriumomgeving met Microsoft 365-compatibiliteit ingeschakeld. Dit gedrag werd waargenomen voor de gespecificeerde FQDN’s:

Stap 1: Microsoft 365-compatibiliteitsfunctie inschakelen

De compatibiliteitsfunctie van Microsoft 365 is geactiveerd in de configuratie voor beveiligde toegang.

Stap 2: Test het verkeer naar doel-FQDN's

Webverkeer werd gegenereerd naar elk van de drie FQDN's met behulp van een standaard internetbrowser:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

Stap 3: Het bypass-gedrag in het dashboard verifiëren

Analyse van het Dashboard voor beveiligde toegang bevestigde dat de inspectie en decodering van webverkeer niet plaatsvond voor verkeer naar deze specifieke bestemmingen toen de compatibiliteitsfunctie Microsoft 365 werd ingeschakeld.

Stap 4: DNS-stuurgedrag bevestigen

Het DNS-verkeer naar deze bestemmingen werd nog steeds gestuurd via Secure Access, wat overeenkomt met gedocumenteerd gedrag, tenzij een specifieke DNS-vrijstelling is geconfigureerd.

Belangrijkste gedragsbevindingen

Op basis van de testresultaten en de documentatieanalyse:

- SWG-bypass: De drie opgegeven FQDN's worden overgeslagen uit de inspectie van webverkeer wanneer Microsoft 365-compatibiliteit is ingeschakeld.
- TLS-decodering: decodering wordt omzeild op de SWG-laag voor deze domeinen.
- DNS-sturing: DNS-query's worden nog steeds verwerkt via Secure Access, tenzij expliciet vrijgesteld.
- Domein dekking: Terwijl "*.microsoft.com" als een hele domein niet volledig wordt omzeild door specificatie, worden de specifieke geteste URL's in de praktijk omzeild.

Overwegingen bij IPS-laag

De compatibiliteitsfunctie van Microsoft 365 werkt op de SWG-laag. Voor IPS-niveau decryptie bypass, handmatige configuratie kan nog steeds nodig zijn:

- Als IPS-decoderingsbypass ook voor deze domeinen gewenst is, kan handmatige toevoeging aan de lijst Niet decoderen noodzakelijk zijn.
- De Do Not Decrypt List heeft voornamelijk invloed op IPS-side decryptie in plaats van SWG-verwerking.
- Dit verklaart waarom documentatie kan verwijzen naar het toevoegen van manage.microsoft.com aan de Do Not Decrypt List, zelfs wanneer Microsoft 365 Compatibility is ingeschakeld.

Oorzaak

De verwarring komt voort uit de gelaagde architectuur van Cisco Secure Access, waar Microsoft 365 Compatibility invloed heeft op SWG-niveau verwerking, terwijl IPS-decryptie werkt als een aparte laag met zijn eigen configuratie-eisen. De Microsoft 365-compatibiliteitsfunctie verwerkt automatisch SWG-bypass voor kwalificerende Microsoft-domeinen, maar IPS-decoderingsbeleid kan een aparte configuratie vereisen via de lijst Niet decoderen.

Gerelateerde inhoud

- Cisco Secure Access Microsoft 365-compatibiliteitsdocumentatie
- Effectieve niet-ontsleutelingslijst maken voor Cisco Secure Access
- 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.