Mis Microsoft Updates Traffic in Secure Web applicatie

Inhoud

Inleiding

Dit document beschrijft de stappen om Microsoft Updates Traffic in Secure Web Appliance (SWA) te omzeilen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toediening van SWA.

Cisco raadt aan deze tools te installeren:

- Fysieke of virtuele SWA
- Administratieve toegang tot de grafische gebruikersinterface (GUI) van de SWA

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Microsoft Updates

Microsoft Updates zijn essentiële patches, beveiligingsupdates en functieverbeteringen die door Microsoft zijn uitgebracht voor zijn besturingssystemen en softwaretoepassingen. Deze updates zijn van cruciaal belang voor het behoud van de beveiliging, stabiliteit en prestaties van computers en netwerkapparaten. Ze zorgen ervoor dat systemen worden beschermd tegen kwetsbaarheden, dat bugs worden gefixeerd en dat nieuwe functies of verbeteringen worden geïntegreerd in de software.

De invloed van Microsoft Updates op proxyservers, zoals Cisco SWA, kan aanzienlijk zijn. Deze updates houden vaak het downloaden van grote bestanden of talrijke kleinere bestanden in, die aanzienlijke bandbreedte en verwerkingsresources op de proxy kunnen verbruiken. Dit kan leiden tot stremming, langzamere netwerkprestaties en een verhoogde belasting op de proxy-infrastructuur, wat mogelijk van invloed is op de algemene gebruikerservaring en andere kritieke netwerkbewerkingen.

Het omzeilen van Microsoft Update verkeer van de proxy kan een veilige en effectieve manier om deze uitdagingen te beheren. Aangezien Microsoft Updates zijn afkomstig van vertrouwde Microsoft-servers, kan dit verkeer om de proxy te omzeilen helpen de belasting op de proxyserver te verminderen zonder de netwerkbeveiliging in gevaar te brengen. Dit waarborgt dat essentiële updates efficiënt worden geleverd, terwijl proxybronnen voor andere taken met betrekking tot beveiliging en contentfiltering behouden blijven. Het is echter belangrijk om dergelijke omzeilingsconfiguraties zorgvuldig te implementeren om de algehele netwerkbeveiliging en naleving van het organisatiebeleid te handhaven.

Microsoft Updates overslaan

Als u overweegt om het verkeer van Microsoft Updates te vermijden, zijn er twee belangrijke benaderingen

1. Omzeilen: hierbij moet het netwerk worden geconfigureerd om het verkeer te sturen, zodat het nooit de SWA bereikt.
2. Passthrough: Dit betekent dat de SWA moet worden geconfigureerd om het Microsoft Updates-verkeer niet te decoderen of te scannen, zodat het zonder inspectie door de proxy kan worden doorgegeven.

Bypassing Traffic in SWA

Om het verkeer van Microsoft Updates in netwerken te mijden die met SWA worden uitgerust, varieert de benadering afhankelijk van uw opstelling van de volmachtsplaatsing:

Type implementatie	Het verkeer omzeilen

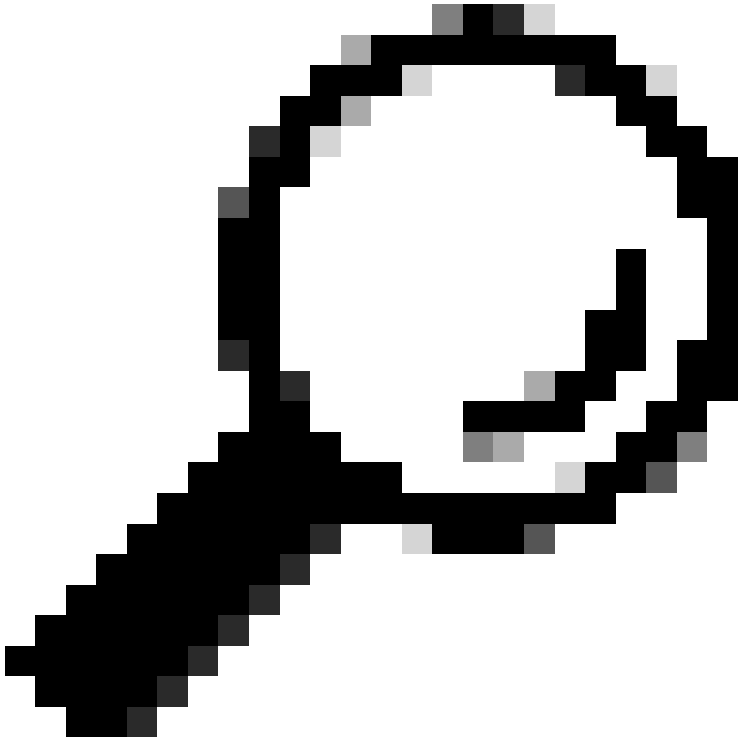
Transparante implementatie	U kunt het verkeer van Microsoft Updates bij de router of Layer 4 switches opnieuw richten die voor het door:sturen van verkeer aan de volmachtsserver verantwoordelijk zijn.
	U kunt omzeilinstellingen direct configureren binnen de grafische gebruikersinterface van de SWA (GUI).
Expliciete implementatie	Om te voorkomen dat het verkeer Microsoft Updates de SWA bereikt, moet u de omzeiling bij de bron configureren. Dit betekent dat de relevante URL's op de clientmachines worden vrijgesteld om ervoor te zorgen dat het verkeer niet wordt omgeleid naar de SWA.

Als het omzeilen van specifiek verkeer een uitgebreid netwerkherontwerp vereist en niet haalbaar is, is een alternatieve benadering om de SWA te configureren om door bepaalde soorten verkeer te gaan. Dit kan worden bereikt door de SWA in te stellen op noch ontsleutelen noch scannen van het toegewezen verkeer, waardoor het door de proxy kan passeren zonder inspectie. Deze methode zorgt ervoor dat essentieel verkeer efficiënt wordt geleverd terwijl het effect op netwerkprestaties en volmachtsmiddelen wordt geminimaliseerd.

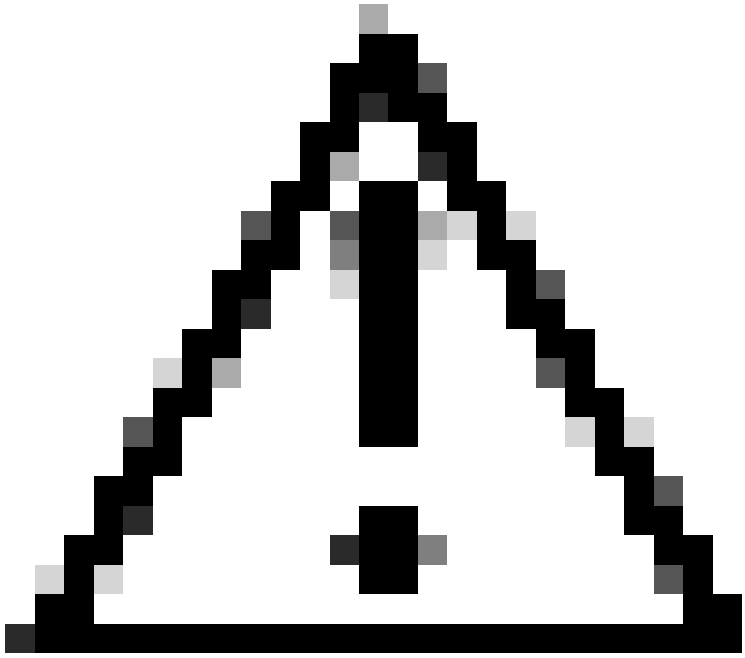
Stappen om door Microsoft Updates te gaan

Er zijn vier hoofdfasen om door Microsoft Updates-verkeer te gaan:

Fase	Stappen
1. Een aangepaste URL-categorie maken voor Microsoft Updates-URL’s	Stap 1.Kies Web Security Manager, vanuit GUI en klik vervolgens op Aangepaste en externe URL-categorieën. Stap 2.Klik op Categorie toevoegen om een aangepaste URL-categorie toe te voegen. Stap 4.Wijs een unieke CategoryName toe. Stap 5. (optioneel) Beschrijving toevoegen. Stap 6. Kies uit Lijstvolgorde de eerste categorie om deze bovenaan te plaatsen. Stap 7. Kies in de vervolgkeuzelijst Category de optie Lokale aangepaste categorie. Stap 8. Voeg Microsoft Updates URL's toe in de sectie Sites.



Tip: U kunt de lijst met Microsoft updates controleren via deze link: [Stap 2 - WSUS configureren | Microsoft Learn]



Waarschuwing: kopieer/plak de URL's niet zoals in de Microsoft Documenten; formatteer ze correct als een SWA-bestand. Ga voor meer informatie naar: [Aangepaste URL-categorieën configureren in]

	Secure Web Applicatie - Cisco Stap 9. Indienen.
2. Een identificatieprofiel maken om Microsoft Updates-verkeer vrij te stellen van verificatie	Stap 10.Kies Web Security Manager, vanuit GUI en klik vervolgens op Identificatieprofielen. Stap 1.Klik op Profiel toevoegen om een profiel toe te voegen. Stap 12.Gebruik het vakje Enable Identification Profilecheck om dit profiel in te schakelen of snel uit te schakelen zonder het te verwijderen. Stap 13.Wijs een uniek profileName toe. Stap 14. (optioneel) Beschrijving toevoegen. Stap 15.Kies in de vervolgkeuzelijst Invoegen waar dit profiel in de tabel moet worden weergegeven. Stap 16. Kies in de sectie Gebruikersidentificatiemethode de optieVrijstellen van verificatie/identificatie. Stap 17.In het tabblad Leden definiëren op Subnet, Als u Microsoft-verkeer wilt doorsturen voor bepaalde specifieke gebruikers, voert u de IP-adressen of subnetten in die van toepassing zijn, of laat u dit veld leeg om al uw IP-adres op te nemen. Stap 18. Kies in de sectie Geavanceerd de optie Aangepaste URL-categorieën. Stap 19. Voeg de aangepaste URL-categorie toe die is gemaakt voor Microsoft-updates. Stap 20. Klik op Gereed. Stap 21. Indienen.
3. Een decryptie-beleid maken om door Microsoft Updates Traffic te gaan	Stap 2.Kies Web Security Manager, vanuit GUI en klik vervolgens op Decryptie. Stap 23. Klik op Beleid toevoegen om een decryptie-beleid toe te voegen. Stap 24.Gebruik het aankruisvakje Beleid inschakelen om dit beleid in te schakelen. Stap 25.Wijs een unieke PolicyName toe.

	Stap 26. (optioneel) Beschrijving toevoegen. Stap 27.Kies het eerste beleid in de vervolgkeuzelijst Invoegen boven Beleid. Stap 28.Kies uit de Identificatieprofielen en Gebruikers het Identificatieprofiel dat u in de vorige stappen hebt gemaakt. Stap 29. Indienen. Stap 30.Op de pagina Decryptie Policy, onder URL-filtering, klikt u op de link die aan dit nieuwe decryptie-beleid is gekoppeld. Stap 32.SelectPassthrough als de actie voor Microsoft Updates URL categorie. Stap 32. Indienen.
4. Een toegangsbeleid maken om Microsoft Updates Traffic toe te staan	Stap 3.Kies Web Security Manager, vanuit GUI en klik vervolgens op Toegangsbeleid. Stap 34. Klik op Beleid toevoegen om een toegangsbeleid toe te voegen. Stap 35.Gebruik het aankruisvakje Beleid inschakelen om dit beleid in te schakelen. Stap 36.Wijs een unieke PolicyName toe. Stap 37. (optioneel) Beschrijving toevoegen. Stap 38.Kies het eerste beleid in de vervolgkeuzelijst Invoegen boven Beleid. Stap 39.Kies uit de Identificatieprofielen en Gebruikers het Identificatieprofiel dat u in de vorige stappen hebt gemaakt. Stap 40. Indienen. Stap 9. Klik op de pagina Toegangsbeleid onder URL-filtering op de link die aan dit nieuwe toegangsbeleid is gekoppeld Stap 10.Selecteer Toestaan de actie voor de Aangepaste URL-categorie die is gemaakt voor de Microsoft Updates. Stap 11. Indienen. Stap 12. Wijzigingen vastleggen.

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Applicatie - GD (Algemene implementatie) - Classificatie van eindgebruikers voor beleidstoepassing [Cisco Secure Web Applicatie] - Cisco
- Aangepaste URL-categorieën configureren in applicatie voor beveiligd web - Cisco
- Office 365 Traffic vrijstellen van verificatie en decryptie op Cisco Web Security Applicatie (WSA) - Cisco
- Best practices voor beveiligde web applicatie gebruiken - Cisco
- Bypass-verificatie in beveiligde web-applicatie - Cisco

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.