Aanvraag voor bereik configureren voor Microsoft Update-verkeer in SWA

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Aanvraag voor bereik

Aanvraag voor bereik in de proxy-omgeving

Aanvraag voor bereik inschakelen voor Microsoft Updates

Stappen voor het inschakelen van Range Request alleen voor Microsoft Updates

- Stap 1. Het bereikverzoek inschakelen
- Stap 2. Een aangepaste URL-rubriek voor Microsoft Updates-URL's maken
- Stap 3. (Optioneel) Maak een identificatieprofiel om Microsoft Updates-verkeer vrij te stellen van verificatie
- Stap 4. (Optioneel) Maak een decoderingsbeleid om Microsoft Updates-verkeer door te geven
- Stap 5. Een toegangsbeleid maken om bereikaanvragen voor Microsoft Updates-verkeer toe te staan

De toegangslogboeken wijzigen

Verificatie

Gerelateerde informatie

Inleiding

In dit document worden de stappen beschreven voor het gebruik van Range Request in Secure Web Appliance (SWA) door Microsoft Traffic Updates.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SWA-beheer.

Cisco raadt u aan deze hulpprogramma's te installeren:

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

Aanvraag voor bereik

Een range request is een functie van het HTTP-protocol waarmee een client (zoals een webbrowser of downloadmanager) slechts een specifiek deel van een bestand van een server kan aanvragen, in plaats van het hele bestand in één keer te downloaden. Dit is vooral handig voor het hervatten van onderbroken downloads, het streamen van media of het efficiënt openen van grote bestanden. De client specificeert het gewenste bytebereik in de Range header van het HTTP-verzoek en de server reageert met een 206 Partial Content status code als het range requests ondersteunt, waardoor alleen het gevraagde segment van het bestand wordt geleverd.

Dit mechanisme verbetert de prestaties en gebruikerservaring in verschillende scenario's. Bijvoorbeeld, in video streaming, bereik verzoeken kunnen spelers alleen de segmenten die nodig zijn voor het afspelen te halen, het verminderen van bandbreedte gebruik en het verbeteren van de responsiviteit. Op dezelfde manier gebruiken downloadmanagers bereikverzoeken om een bestand in brokken te splitsen en ze parallel te downloaden, waardoor het proces wordt versneld. Range requests spelen ook een belangrijke rol in caching en proxy systemen, waardoor gedeeltelijke updates mogelijk worden en redundante gegevensoverdrachten worden verminderd.

Aanvraag voor bereik in de proxy-omgeving

In een proxy-omgeving spelen bereikverzoeken een cruciale rol bij het optimaliseren van het bandbreedtegebruik en het verbeteren van de efficiëntie van de levering van inhoud. Wanneer bereikverzoeken zijn ingeschakeld, kan de proxyserver alleen de vereiste bytesegmenten ophalen van de oorspronkelijke server en deze lokaal cachen. Hierdoor kunnen clients gedeeltelijke inhoud aanvragen, zoals specifieke segmenten van een video of een groot bestand, en deze snel ontvangen uit de proxy-cache, indien beschikbaar. Het maakt ook parallelle downloads en cv-mogelijkheden mogelijk, die vooral gunstig zijn in omgevingen met beperkte bandbreedte of hoge latentie.

Wanneer bereikverzoeken echter zijn uitgeschakeld, moet de proxy het volledige bestand ophalen van de oorspronkelijke server, zelfs als de client slechts een klein gedeelte nodig heeft. Dit leidt tot onnodige gegevensoverdracht, verhoogde belasting op zowel de proxy- als de oorsprongservers en langzamere responstijden voor clients. Het voorkomt ook efficiënte cachingstrategieën, omdat de proxy geen gedeeltelijke inhoud kan opslaan of serveren. In streaming-scenario's kan dit leiden tot buffervertragingen of een verslechterde gebruikerservaring. Het uitschakelen van bereik verzoeken kan worden gedaan voor de veiligheid of het beleid redenen, maar het komt vaak ten koste van de prestaties en flexibiliteit.

Denk bijvoorbeeld aan een scenario waarbij 10 gebruikers elk 1 MB proberen te downloaden van een 100MB-bestand via een proxyserver.

Aanvragen voor bereik uitgeschakeld:

Wanneer bereikverzoeken zijn uitgeschakeld, kan de proxy niet alleen het 1MB-segment ophalen dat elke gebruiker nodig heeft. In plaats daarvan moet het voor elk verzoek het volledige 100MB-bestand van de oorspronkelijke server downloaden. Dit resulteert in:

Totaal verkeer van oorsprong naar proxy: 10 × 100MB = 1000MB (1 GB)

Slechts 10 MB van die gegevens wordt daadwerkelijk gebruikt door de clients.

De resterende 990MB wordt verspild, wat leidt tot inefficiënt bandbreedtegebruik en verhoogde belasting op de proxy- en oorsprongservers.

Aanvragen voor bereik ingeschakeld:

Als bereikverzoeken zijn ingeschakeld, haalt de proxy alleen de gevraagde 1MB per gebruiker op:

Totaal verkeer van oorsprong naar proxy: 10 × 1 MB = 10 MB

De proxy kan deze segmenten cachen en indien nodig aan andere gebruikers leveren.

Dit resulteert in 90 keer minder verkeer, snellere responstijden en een aanzienlijk beter gebruik van bronnen.

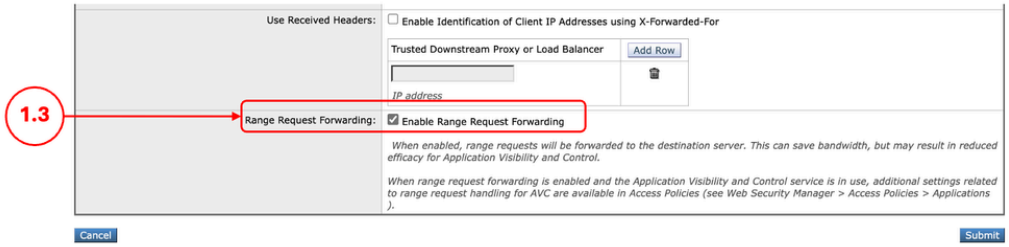
Aanvraag voor bereik inschakelen voor Microsoft Updates

Hoewel range requests de prestaties verbeteren, belemmeren ze het scannen van de beveiliging en de handhaving van het beleid binnen SWA-omgevingen, omdat deze systemen gedeeltelijke inhoud niet volledig kunnen inspecteren. Dit artikel beperkt het gebruik van het bereik van de aanvraag uitsluitend tot Microsoft Update-verkeer.

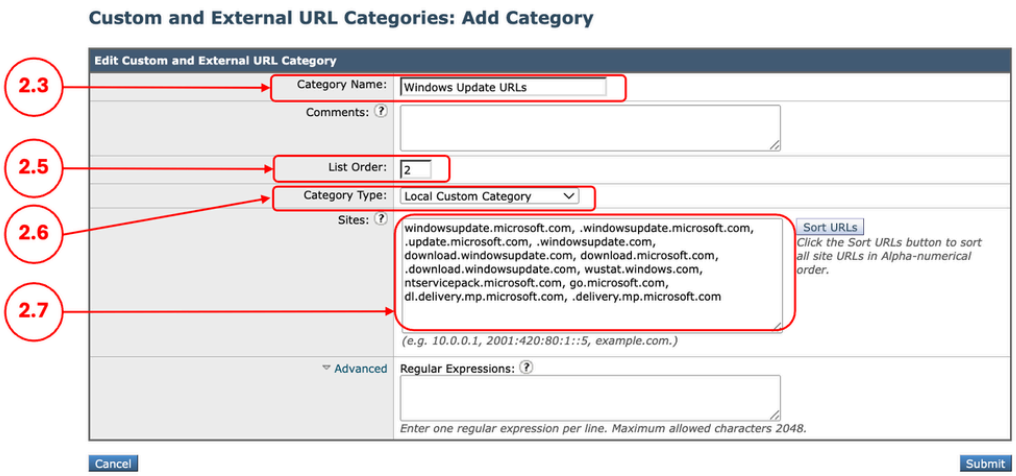
⚠ Waarschuwing: het inschakelen van range request forwarding kan de efficiëntie van AVC (Application Visibility and Control) verstoren en de beveiliging in gevaar brengen.

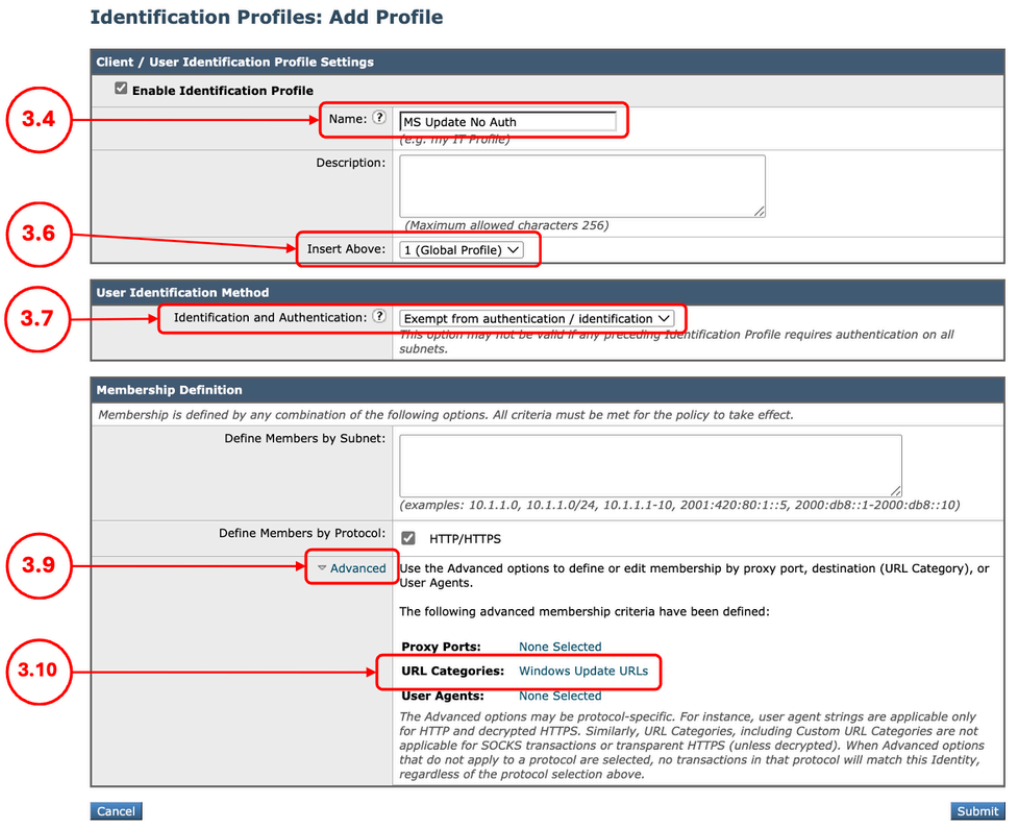
Stappen voor het inschakelen van Range Request alleen voor Microsoft Updates

Stap 1. Het bereikverzoek inschakelen	Stap 1.1. Klik in de GUI op Beveiligingsservices en kies Webproxy. Stap 1.2. Klik op Instellingen bewerken. Stap 1.3. Schakel het selectievakje Doorsturen bereikverzoek

	inschakelen in. Stap 1.4. Klik op Indienen.  Afbeelding - Doorsturen van bereikaanvraag inschakelen

Stap 2. Een aangepaste URL-rubriek voor Microsoft Updates-URL's maken	Stap 2.1.Kies Web Security Manager van GUI en klik op Aangepaste en Externe URL-categorieën.
	Stap 2.2.Klik op Categorie toevoegen om een aangepaste URL-rubriek toe te voegen.
	Stap 2.3.Een unieke categorienaam toewijzen.
	Stap 2.4. (Optioneel) Beschrijving toevoegen.
	
	Stap 2.5. Kies in Lijstvolgorde de eerste categorie die u bovenaan wilt plaatsen.
	
	Stap 2.6. Kies in de vervolgkeuzelijst Categorie de optie Lokale aangepaste rubriek.
	
	Stap 2.7. Voeg Microsoft Updates-URL's toe in de sectie Sites.
	
	Tip: U kunt de lijst met Microsoft-updates bekijken via deze link: Stap 2 - WSUS configureren | Microsoft Learn
	
	Let op: Kopieer/plak de URL's niet zoals in de Microsoft-documenten; formatteer ze op de juiste manier als SWA-indeling. Ga voor meer informatie naar: Aangepaste URL-categorieën configureren in Secure Web Appliance - Cisco
	
	Hierna volgt een voorbeeld:
	
	`http://windowsupdate.microsoft.com ===> windowsupdate.microsoft.com`
	`http://*.windowsupdate.microsoft.com ===> .windowsupdate.microsoft.com`

	Stap 2.8. Klik op Indienen.  Afbeelding - Een aangepaste URL-rubriek maken
Stap 3. (Optioneel) Maak een identificatieprofiel om Microsoft Updates-verkeer vrij te stellen van verificatie Opmerking: deze actie is bedoeld om de verificatielast op de SWA voor het verkeer naar Microsoft Updates te verminderen.	Stap 3.1.Kies Web Security Manager van GUI en klik op Identificatieprofielen. Stap 3.2.Klik op Profiel toevoegen om een profiel toe te voegen. Stap 3.3.Zorg ervoor dat het selectievakje Identificatieprofiel inschakelen is ingeschakeld. Stap 3.4.Een unieke profielnaam toewijzen. Stap 3.5. (Optioneel) Beschrijving toevoegen. Stap 3.6.Kies in de vervolgkeuzelijst Invoegen hierboven waar dit profiel in de tabel moet worden weergegeven. Stap 3.7. In het gedeelte Gebruikersidentificatiemethoden kiest u Vrijstellen van verificatie/identificatie. Stap 3.8.In het Leden definiëren op subnet, Als u wilt passeren door Microsoft-verkeer voor een aantal specifieke gebruikers, voert u de IP-adressen of subnetten die van toepassing zijn, of anders laat dit veld leeg om alle IP-adres op te nemen. Stap 3.9. Kies in de sectie Geavanceerd de optie Aangepaste URL-categorieën. Stap 3.10. Voeg de aangepaste URL-categorie toe die is gemaakt voor Microsoft-updates. Stap 3.11. Klik op Gereed. Stap 3.12. Klik op Indienen.



Afbeelding - Identificatieprofiel maken

Stap 4. (Optioneel) Maak een decoderingsbeleid om Microsoft Updates-verkeer door te geven

Opmerking: Microsoft Updates gebruikt HTTP en het HTTPS-verkeer is om de updates-links te pushen. Deze actie is bedoeld om de decoderingsbelasting op de SWA te verminderen.

Stap 4.1.Van GUI, Kies Web Security Manager en klik vervolgens op Decryptie Policy.

Stap 4.2. Klik op Beleid toevoegen om een decoderingsbeleid toe te voegen.

Stap 4.3.Een unieke beleidsnaam toewijzen.
Stap 4.4. (Optioneel) Beschrijving toevoegen.
Stap 4.5.Kies het eerste beleid uit de vervolgkeuzelijst Invoegen boven beleid.

Stap 4.6.Kies in het gedeelte Identificatieprofielen en gebruikers de optie Een of meer identificatieprofielen selecteren.

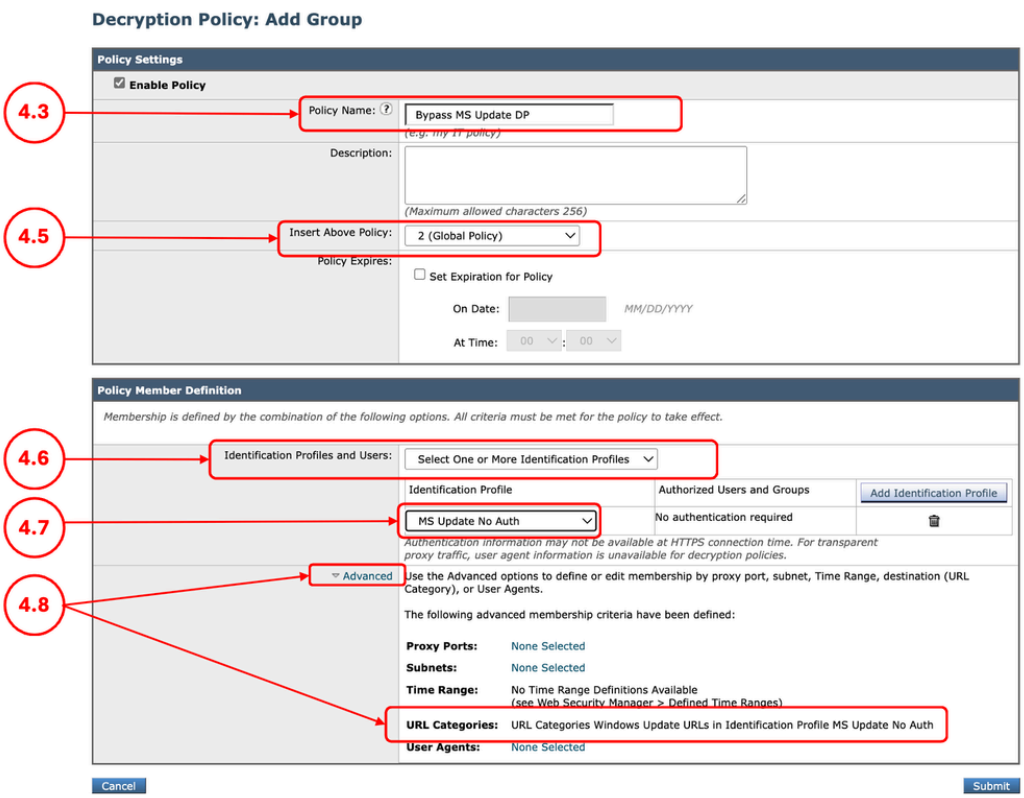
Stap 4.7. Selecteer het identificatieprofiel dat u in stap 3 hebt gemaakt en ga naar stap 4.11.

Stap 4.8. Als u geen ID-profiel hebt gemaakt voor de Windows Updates, kiest u in het gedeelte Geavanceerd de optie Aangepaste URL-categorieën.

Stap 4.9. Voeg de aangepaste URL-categorie toe die is gemaakt voor Microsoft-updates in stap 2.

Stap 4.10. Klik op Gereed.

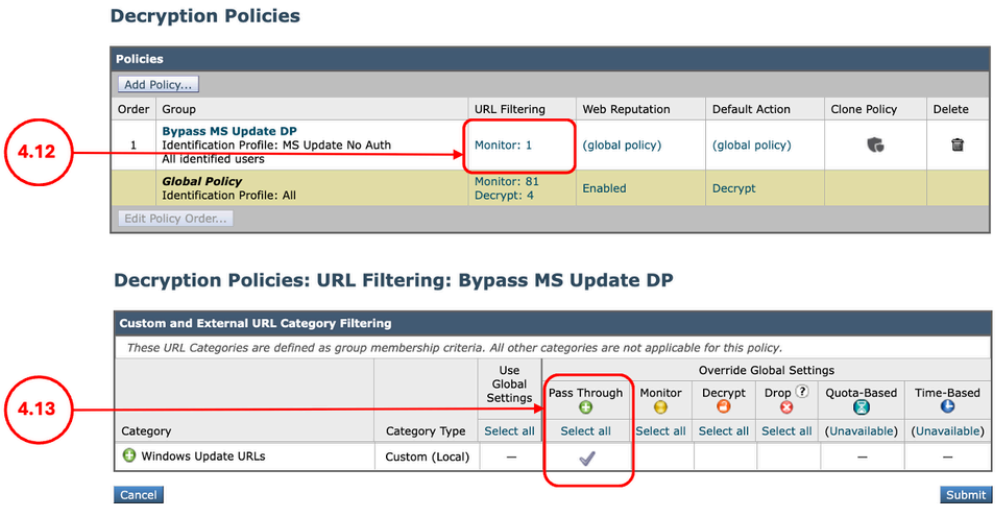
Stap 4.11. Klik op Indienen.



Afbeelding - Een decoderingsbeleid maken

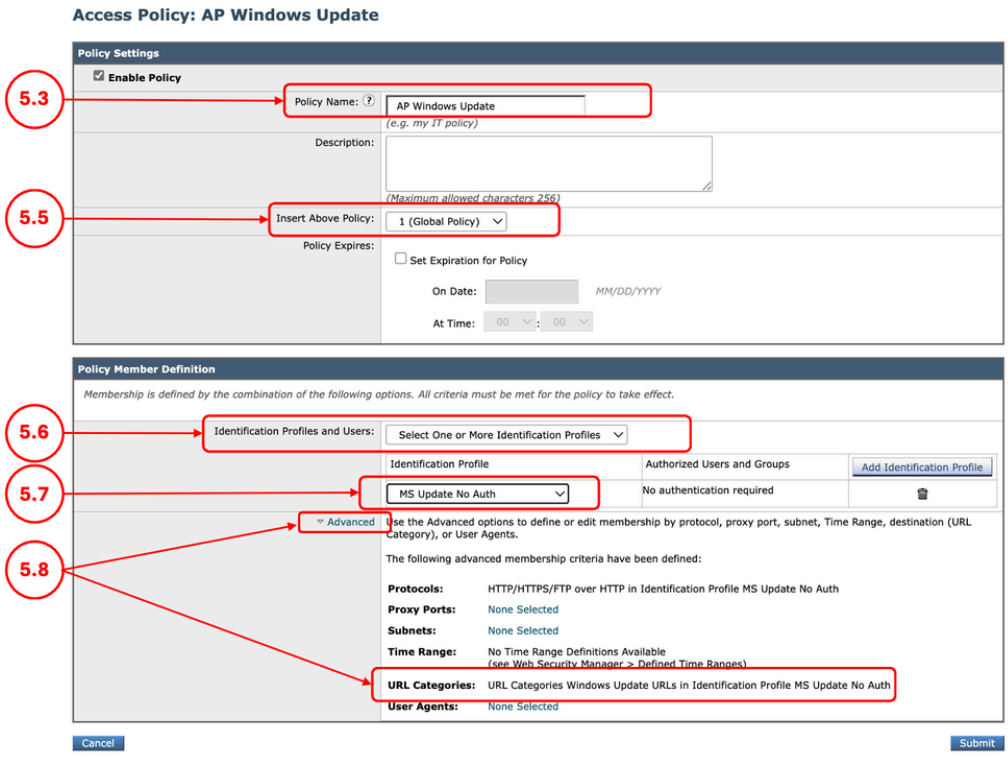
Stap 4.12.Op de pagina Decryptiebeleid, onder URL-filtering, klikt u op de link die is gekoppeld aan dit nieuwe Decryptiebeleid.

Stap 4.13.Selecteer Doorgeven als de actie voor de URL-categorie Microsoft Updates.



Afbeelding - De actieroute voor de URL-categorie instellen

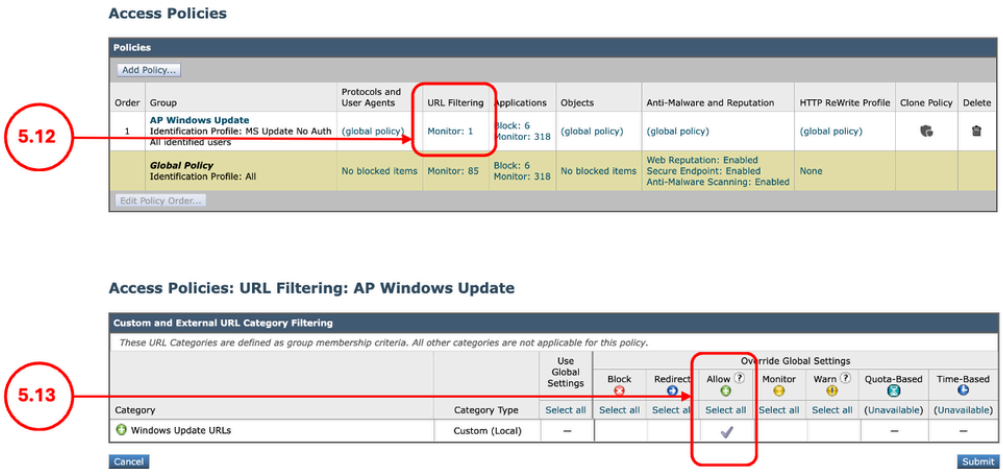
Stap 4.12. Klik op Indienen.

Stap 5. Een toegangsbeleid maken om bereikaanvragen voor Microsoft Updates-verkeer toe te staan	Stap 5.1.Klik vanuit GUI op Web Security Manager en kies Access Policy. Stap 5.2. Klik op Beleid toevoegen om een toegangsbeleid toe te voegen. Stap 5.3.Een unieke beleidsnaam toewijzen. Stap 5.4. (Optioneel) Beschrijving toevoegen. Stap 5.5.Kies het eerste beleid uit de vervolgkeuzelijst Invoegen boven beleid. Stap 5.6.Kies in het gedeelte Identificatieprofielen en gebruikers, Selecteer een of meer identificatieprofielen. Stap 5.7. Selecteer het identificatieprofiel dat u in stap 3 hebt gemaakt en ga naar stap 5.11. Stap 5.8. Als u geen ID-profiel hebt gemaakt voor de Windows Updates, kiest u in het gedeelte Geavanceerd de optie Aangepaste URL-categorieën. Stap 5.9. Voeg de aangepaste URL-categorie toe die is gemaakt voor Microsoft-updates in stap 2. Stap 5.10. Klik op Gereed. Stap 5.11. Verzenden.  Afbeelding - Toegangsbeleid maken

Stap 5.12. Klik op de pagina Toegangsbeleid, onder URL-filtering, op de koppeling die is gekoppeld aan dit nieuwe toegangsbeleid

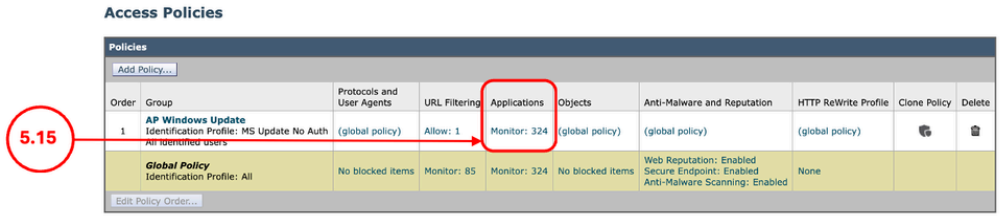
Stap 5.13.Selecteer Toestaan als de actie voor de categorie Aangepaste URL die is gemaakt voor de Microsoft Updates.

Stap 5.14. Klik op Indienen.



Afbeelding - De actie Toestaan voor de URL-categorie instellen

Stap 5.15. Klik op de pagina Toegangsbeleid onder Toepassingen op de koppeling die aan dit nieuwe toegangsbeleid is gekoppeld

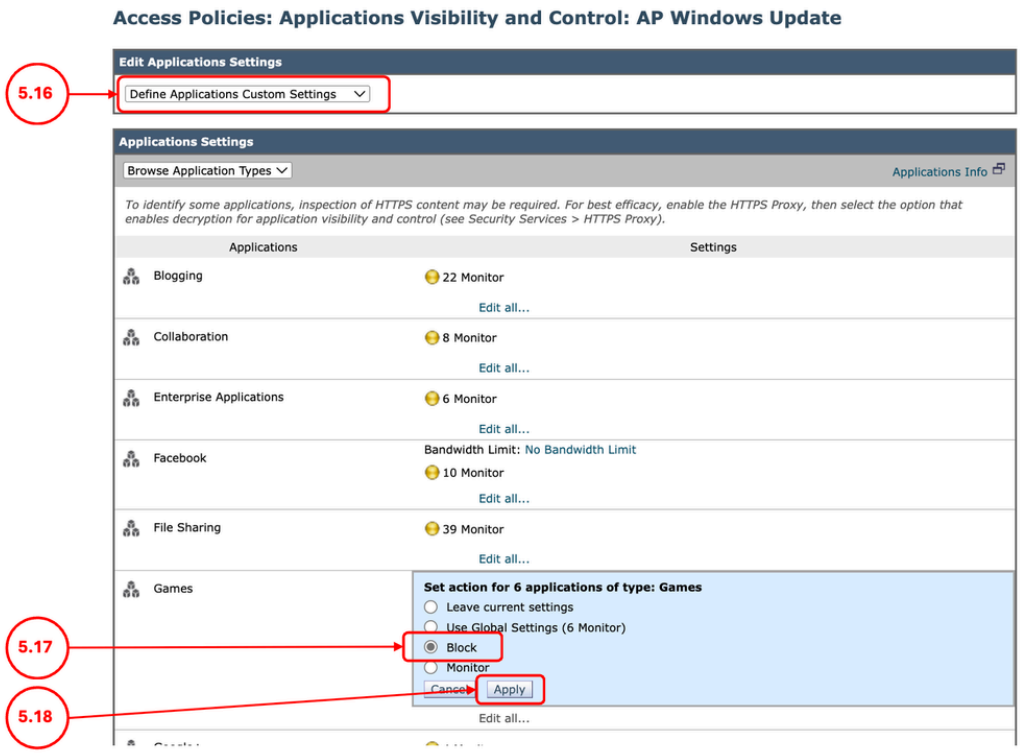


Afbeelding - Toepassingszichtbaarheid en -besturing bewerken

Stap 5.16. Selecteer in het gedeelte Toepassingsinstellingen bewerken de optie Aangepaste instellingen voor toepassingen definiëren.

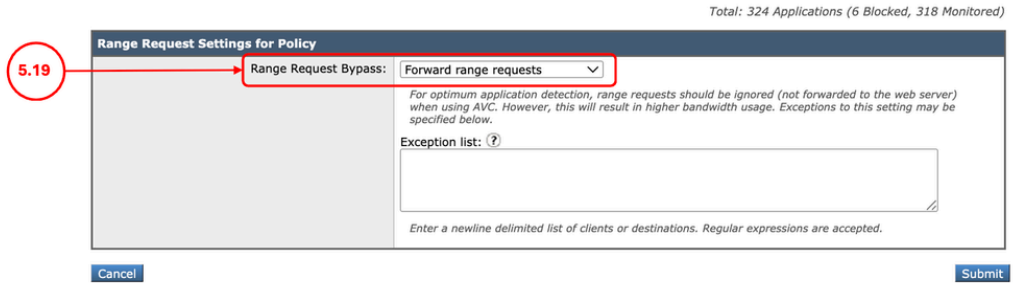
Stap 5.17. Klik in de sectie Toepassingsinstellingen op Alles bewerken voor Games-toepassing en stel de actie in op Blokkeren.

Stap 5.18. Klik op Apply (Toepassen).



Afbeelding - Eén toepassingsactie instellen om te blokkeren

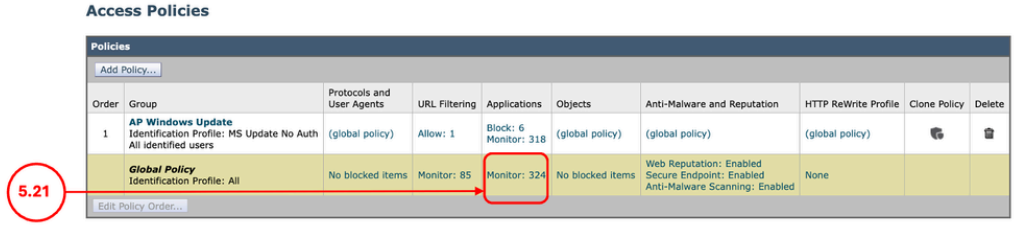
Stap 5.19. Blader omlaag naar het gedeelte Instellingen bereikaanvraag voor beleid, zorg ervoor dat Bereikaanvragen doorsturen is geselecteerd,



Afbeelding - Instellingen voor bereik-aanvraag voor beleid

Stap 5.20. Verzenden.

Stap 5.21. Klik op de pagina Toegangsbeleid onder Toepassingen op de koppeling gekoppeld aan het Algemeen beleid.



Afbeelding - Toepassingsinstellingen voor standaardtoegangsbeleid

Stap 5.22. Blader omlaag naar het gedeelte Instellingen bereikverzoek

	voor beleid, zorg ervoor dat bereikverzoeken niet doorsturen is geselecteerd, Stap 5.23. Wijzigen doorvoeren.

De toegangslogboeken wijzigen

Als u meer inzicht wilt krijgen in het bereik van de aanvragen uit de toegangslogboeken, kunt u de volgende aangepaste velden toevoegen:

[Clientbereik = %<bereik:]	Toont het bereik dat door de client is aangevraagd (bytes)
[content= %>Lengte inhoud:]	Geeft de grootte van de gedownloade inhoud (bytes) weer

Ga voor meer informatie over het toevoegen van een aangepast veld aan de SWA Access Logs naar deze link: Prestatieparameter configureren in Access Logs

Verificatie

Gebruik deze opdracht CURL om een bereikverzoek naar de SWA te sturen:

```
curl -vvvk -H "Pragma: no-cache" -x 10.48.48.181:3128 -H 'Range: bytes=0-100' 'http://catalog.sf.dl.del
```

Aan de uitgang van de CURL kun je zien dat het HTTP-antwoord HTTP/1.1 206 is:

```
> GET http://catalog.sf.dl.delivery.mp.microsoft.com/filestreamingservice/files/f263aa64-f367-42f0-9cad
> Host: catalog.sf.dl.delivery.mp.microsoft.com
> User-Agent: curl/8.7.1
> Accept: */*
> Proxy-Connection: Keep-Alive
> Pragma: no-cache
> Range: bytes=0-100
>
* Request completely sent off
< HTTP/1.1 206 Partial Content
```

In de toegangslogboeken ziet u de actie TCP_CLIENT_REFRESH_MISS/206:

```
1773942471.096 14 10.190.0.206 TCP_CLIENT_REFRESH_MISS/206 860 GET http://catalog.sf.dl.delivery.mp.mic
```

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Appliance - GD(General Deployment) - Eindgebruikers classificeren voor beleidstoepassing [Cisco Secure Web Appliance] - Cisco
- Aangepaste URL-categorieën configureren in Secure Web Appliance - Cisco
- Hoe Office 365-verkeer vrij te stellen van verificatie en decodering op Cisco Web Security Appliance (WSA) - Cisco
- Prestatieparameter configureren in toegangslogboeken
- Best practices voor veilige webapparaten gebruiken - Cisco
- Verificatie omzeilen in Secure Web Appliance - 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.