Blokverkeer in beveiligde web-applicatie

Inhoud

Inleiding

Dit document beschrijft de stappen om verkeer in Secure Web Applicatie (SWA) te blokkeren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toediening van SWA.

Cisco raadt u aan het volgende te doen:

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

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.

Blokkerend verkeer

Het blokkeren van verkeer in de SWA is een cruciale stap om netwerkbeveiliging te garanderen, de naleving van intern beleid te handhaven en bescherming te bieden tegen kwaadaardige activiteiten. Hier zijn een aantal veel voorkomende redenen voor het blokkeren van verkeer:

Redenen voor blokkering via bron

- Overstroming door één of meer gebruikers: wanneer één of meer gebruikers buitensporig verkeer genereren, kan het het netwerk overweldigen, wat leidt tot verslechtering van de prestaties en mogelijke onderbrekingen van de service.
- Onvertrouwde resourcetoegang door toepassingen (User-Agents): Bepaalde toepassingen kunnen proberen toegang te krijgen tot onbetrouwbare of potentieel schadelijke bronnen. Het blokkeren van deze user-agents helpt beveiligingslekken en -lekken te voorkomen.
- Beperking van internettoegang voor specifieke IP-bereiken: sommige IP-adressen of -bereiken moeten mogelijk worden beperkt om toegang tot het internet te krijgen vanwege beveiligingsbeleid of om onbevoegd gebruik te voorkomen.
- Verdacht verkeersgedrag: verkeer dat ongebruikelijke patronen of gedrag vertoont die kunnen wijzen op schadelijke activiteit of beveiligingsbedreigingen, moet worden geblokkeerd om het netwerk te beschermen.

Redenen voor blokkering op bestemming

- Naleving van Intern Bedrijfsbeleid: Organisaties hebben vaak beleid dat de toegang tot bepaalde websites of onlinebronnen beperkt om productiviteit en naleving van wettelijke of regelgevende vereisten te verzekeren.
- Onvertrouwde Sites: Het blokkeren van de toegang tot websites die als onbetrouwbaar of potentieel schadelijk worden beschouwd, helpt gebruikers te beschermen tegen phishing, malware en andere online bedreigingen.
- Kwaadaardig gedrag: sites die gekend zijn voor het hosten van kwaadaardige content of het uitvoeren van schadelijke activiteiten moeten worden geblokkeerd om beveiligingsincidenten en inbreuken op gegevens te voorkomen.

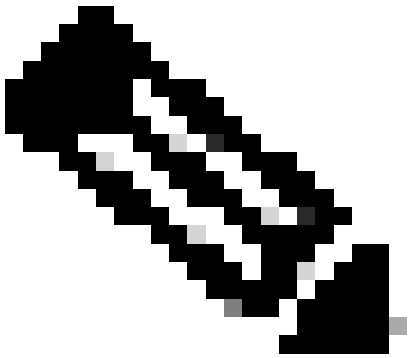
.

Stappen om verkeer te blokkeren

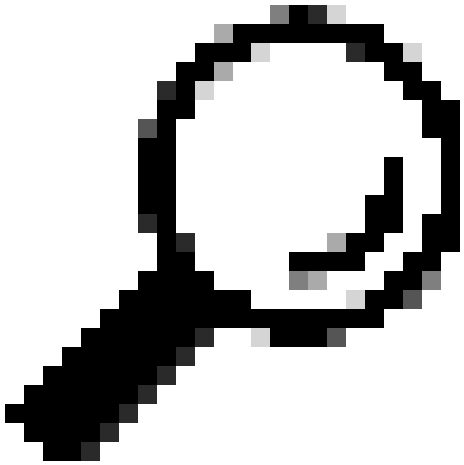
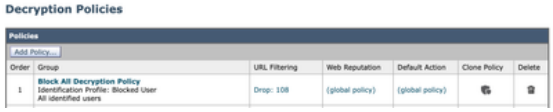
In het algemeen zijn er 3 hoofdfasen om het verkeer in SWA te blokkeren:

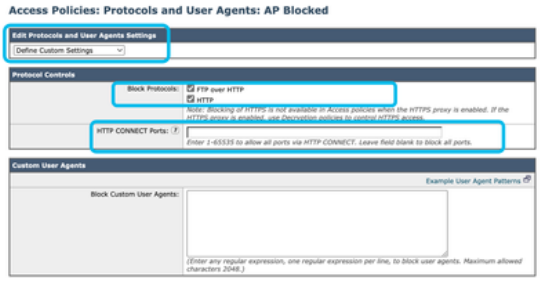
- Maak een identificatieprofiel voor de gebruiker(s).
- Blokkeer het HTTPS-verkeer in het decryptiebeleid.
- Blokkeer het HTTP-verkeer in het toegangsbeleid.

Fases	Blokkeer specifieke gebruikers van toegang tot websites	Blokkeer specifieke gebruikers van toegang tot bepaalde websites

Aangepaste URL-categorie	Niet van toepassing.	Maak een aangepaste URL-categorie voor de sites die u van plan bent te blokkeren. Voor meer informatie, bezoek: Aangepaste URL-categorieën configureren in applicatie voor beveiligd web - Cisco
Identificatieprofiel	Stap 1. Kies in GUI Web Security Manager en klik vervolgens op Identificatieprofielen. Stap 2. Klik op Profiel toevoegen om een profiel toe te voegen. Stap 3. Gebruik het aanvinkvakje Enable Identification Profile om dit profiel in te schakelen of om het snel uit te schakelen zonder het te verwijderen. Stap 4. Wijs een uniek profiel Naam toe. Stap 5. (optioneel) Beschrijving toevoegen. Stap 6. Kies in de vervolgkeuzelijst Invoegen boven waar dit profiel in de tabel moet worden weergegeven. Stap 7. Kies in het gedeelte Gebruikersidentificatiemethode Vrijstelling van verificatie/identificatie. Stap 8. Voer in het veld Leden per subnet definiëren de IP-adressen of subnetten in die dit identificatieprofiel moet toepassen. U kunt IP-adressen, Classless Inter-Domain Routing (CIDR)-blokken en subnetten gebruiken.	 Opmerking: voor het blokkeren van de toegang tot bepaalde websites voor alle gebruikers is er geen verplichting om een afzonderlijk ID-profiel te maken. Dit kan efficiënt worden beheerd via het wereldwijde decryptie/toegangsbeleid. Stap 1. Kies in GUI Web Security Manager en klik vervolgens op Identificatieprofielen. Stap 2. Klik op Profiel toevoegen om een profiel toe te voegen. Stap 3. Gebruik het aanvinkvakje Enable Identification Profile om dit profiel in te schakelen of om het snel uit te schakelen zonder het te verwijderen. Stap 4. Wijs een uniek profiel Naam toe. Stap 5. (optioneel) Beschrijving

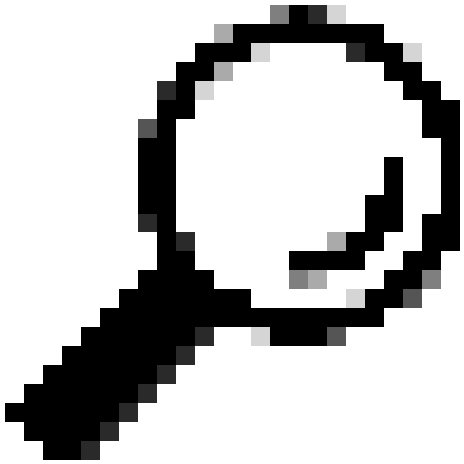
		toevoegen. Stap 6. Kies in de vervolgkeuzelijst Invoegen boven waar dit profiel in de tabel moet worden weergegeven. Stap 7. Kies in het gedeelte Gebruikersidentificatiemethode Vrijstelling van verificatie/identificatie. Stap 8. Voer in het veld Leden per subnet definiëren de IP-adressen of subnetten in die dit identificatieprofiel moet toepassen. U kunt IP-adressen, Classless Inter-Domain Routing (CIDR)-blokken en subnetten gebruiken. Stap 9. Klik op Advanced en voeg de URL-categorie toe die u wilt blokkeren.
Decryptie beleid	Stap 1. Kies Web Security Manager uit GUI en klik vervolgens op Decryptie Beleid. Stap 2. Klik op Beleid toevoegen om een decryptie-beleid toe te voegen. Stap 3. Gebruik het aanvinkvakje Beleid inschakelen om dit beleid in te schakelen. Stap 4. Wijs een unieke naam van het Beleid toe. Stap 5. (optioneel) Beschrijving toevoegen. Stap 6. Kies in de vervolgkeuzelijst Invoegen boven beleid de eerste optie Beleid. Stap 7. Kies het Identificatieprofiel en de Gebruikers dat u in de vorige stappen hebt gemaakt. Stap 8. Indienen. Stap 9. Klik op de pagina Decryptie Beleid onder URL-filtering op de link die aan dit nieuwe decryptie beleid is	Stap 1. Kies Web Security Manager uit GUI en klik vervolgens op Decryptie Beleid. Stap 2. Klik op Beleid toevoegen om een decryptie-beleid toe te voegen. Stap 3. Gebruik het aanvinkvakje Beleid inschakelen om dit beleid in te schakelen. Stap 4. Wijs een unieke naam van het Beleid toe. Stap 5. (optioneel) Beschrijving toevoegen. Stap 6. Kies in de vervolgkeuzelijst Invoegen boven beleid de eerste optie Beleid. Stap 7. Kies het Identificatieprofiel en de Gebruikers dat u in de vorige stappen hebt gemaakt. Stap 8. Indienen. Stap 9. Klik op de pagina Decryptie Beleid onder URL-filtering op de link die aan dit nieuwe decryptie beleid is

	gekoppeld.  Tip: Aangezien u alle URL-categorieën blokkeert, kunt u het beleid optimaliseren door aangepaste URL-categorieën te verwijderen en alleen de vooraf gedefinieerde URL-categorieën te gebruiken. Dit vermindert de verwerkingsbelasting op de SWA door de extra stap van het aanpassen van URL's met aangepaste URL-categorieën te vermijden. Stap 10. Selecteer Drop als de actie voor elke URL-categorie. Stap 11. Blader op dezelfde pagina naar Niet-gecategoriseerde URL's en kies Drop uit vervolgkeuzelijst. Stap 12. Indienen.  Afbeelding - Decryptie Beleid om Alle Website voor Bepaalde Gebruikers te blokkeren	gekoppeld. Stap 10. Selecteer Drop als de actie voor de Aangepaste URL categorie gemaakt voor de geblokkeerde websites. Stap 11. Klik op Verzenden.  Afbeelding - Een aantal URL's blokkeren in het decryptie beleid
Toegangsbeleid	Stap 1. Kies in GUI Web Security Manager en klik vervolgens op Toegangsbeleid.	Stap 1. Kies in GUI Web Security Manager en klik vervolgens op Toegangsbeleid.

	Stap 2. Klik op Beleid toevoegen om een toegangsbeleid toe te voegen. Stap 3. Gebruik het aanvinkvakje Beleid inschakelen om dit beleid in te schakelen. Stap 4. Wijs een unieke naam van het Beleid toe. Stap 5. (optioneel) Beschrijving toevoegen. Stap 6. Kies in de vervolgkeuzelijst Invoegen boven beleid de eerste optie Beleid. Stap 7. Kies het Identificatieprofiel en de Gebruikers dat u in de vorige stappen hebt gemaakt. Stap 8. Indienen. Stap 9. Klik op de pagina Toegangsbeleid onder Protocollen en Gebruikersagenten op de koppeling die aan dit nieuwe toegangsbeleid is gekoppeld. Stap 10. Kies in de vervolgkeuzelijst Protocollen bewerken en Instellingen gebruikersagents de optie Aangepaste instellingen definiëren. Stap 11. In Blokprotocollen selecteren het selectievakje voor beide FTP via HTTP en HTTP. Stap 12. In HTTP CONNECT-poorten, verwijder elk poortnummer om alle poorten te blokkeren.  Afbeelding - Protocollen blokkeren en poorten verbinden in toegangsbeleid	Stap 2. Klik op Beleid toevoegen om een toegangsbeleid toe te voegen. Stap 3. Gebruik het aanvinkvakje Beleid inschakelen om dit beleid in te schakelen. Stap 4. Wijs een unieke naam van het Beleid toe. Stap 5. (optioneel) Beschrijving toevoegen. Stap 6. Kies in de vervolgkeuzelijst Invoegen boven beleid de eerste optie Beleid. Stap 7. Kies het Identificatieprofiel en de Gebruikers dat u in de vorige stappen hebt gemaakt. Stap 8. Indienen. Stap 9. Klik op de pagina Toegangsbeleid onder URL-filtering op de link die aan dit nieuwe toegangsbeleid is gekoppeld Stap 10.Selecteer Blok als de actie voor de Aangepaste URL categorie gemaakt voor de geblokkeerde websites. Stap 11. Indienen. Stap 12. Wijzigingen vastleggen.  Afbeelding - Blokkeer enkele URL's in het toegangsbeleid

Stap 13. Indienen.

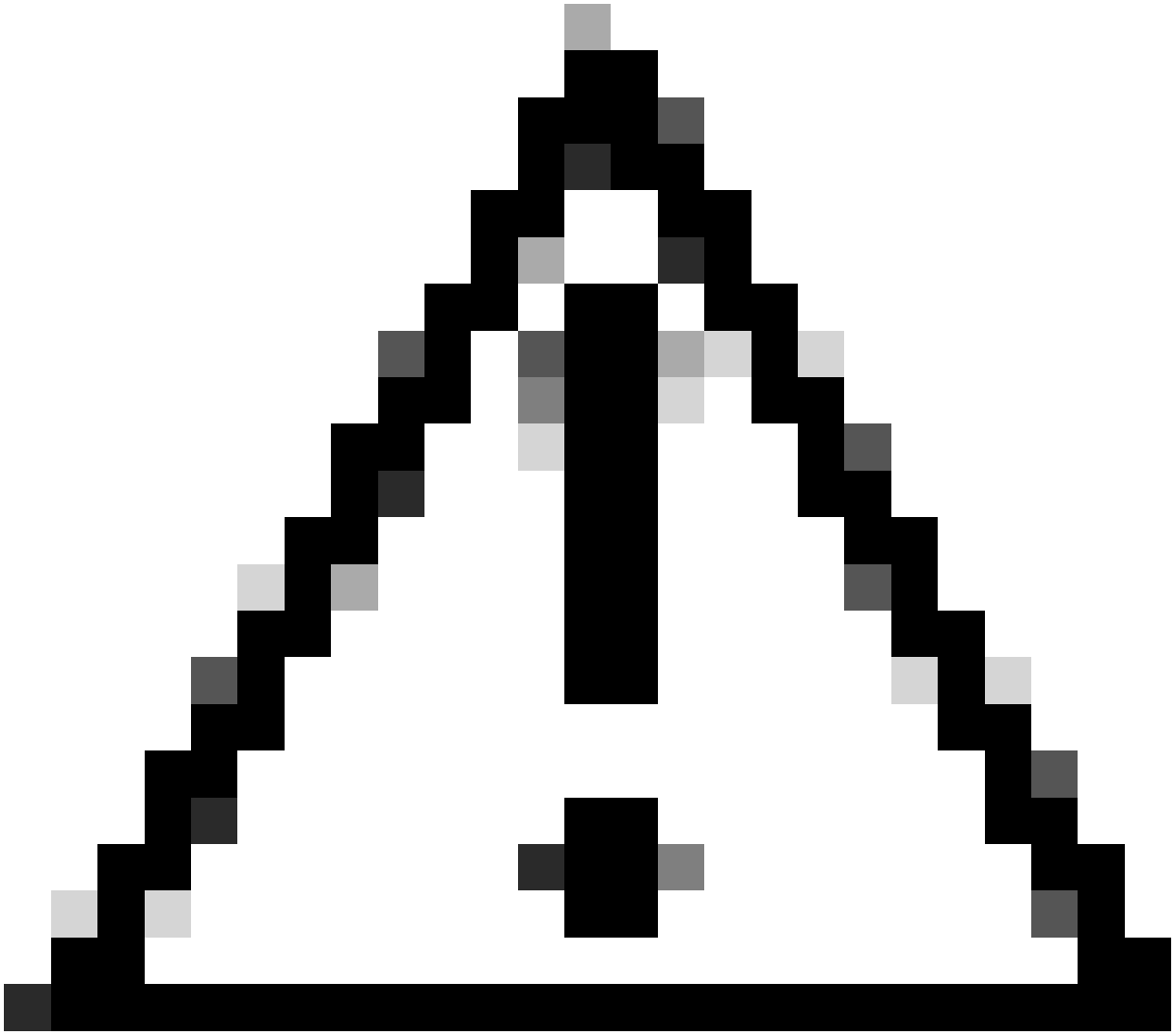
Stap 14. (optioneel) Klik op de pagina Toegangsbeleid onder URL-filtering op de link die aan dit nieuwe toegangsbeleid is gekoppeld en Selecteer Blok als actie voor elke URL-categorie en de Niet-gecategoriseerde URL's en vervolgens verzenden.



Tip: Aangezien u alle URL-categorieën blokkeert, kunt u het beleid optimaliseren door aangepaste URL-categorieën te verwijderen en alleen de vooraf gedefinieerde URL-categorieën te gebruiken. Dit vermindert de verwerkingsbelasting op de SWA door de extra stap van het aanpassen van URL's met aangepaste URL-categorieën te vermijden.

Stap 16. Wijzigingen vastleggen.

Image- Access Policy om alle locaties te blokkeren



Waarschuwing: bij een transparante proxyimplementatie kan SWA geen gebruikersagents of de volledige URL voor HTTPS-verkeer lezen tenzij het verkeer wordt gedecodeerd. Als u het Identificatieprofiel configureert met gebruikersagents of een aangepaste URL-categorie met reguliere expressies, dan komt dit verkeer niet overeen met het Identificatieprofiel.

Blokkerende Sites met Reguliere Expressies in Transparent Proxy-implementatie

In Transparent proxy-implementatie, als u van plan bent om een Aangepaste URL-categorie te blokkeren die Regular Expressions-voorwaarde heeft - u blokkeert bijvoorbeeld de toegang tot sommige YouTube-kanalen - kunt u deze stappen gebruiken:

Stap 1. Maak een aangepaste URL-categorie voor de hoofdsite. (In dit voorbeeld: YouTube.com).

Stap 2. Maak een decryptie beleid, wijs deze aangepaste URL categorie toe en stel de actie in om

te decrypteren.

Stap 3. Maak een toegangsbeleid, wijs de aangepaste URL-categorie toe aan de Reguliere expressies (in dit voorbeeld de aangepaste URL-categorie voor de YouTube-kanalen) en stel de actie in om te blokkeren.

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

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.