Onbekende toepassingen van Secure Web Appliance blokkeren

Inhoud

[Inleiding](#)
[Methoden om onbekende toepassingen te blokkeren](#)
[Bloktoepassingen op basis van gebruikersagent Strings](#)
[Bloktoepassingen gebaseerd op toepassingszichtbaarheidscontroles](#)
[bloktoepassingen op basis van MIME-type](#)
[URL-categorieën in toegangsbeleid blokkeren](#)
[HTTP-configuratie van poorten beperken in toegangsbeleid](#)
[Bloktoegang voor specifieke IP-adressen](#)
[Hoe te vinden welke gebruikersagent of MIME een toepassing gebruikt](#)
[Referentie](#)
[Lijst van gebruikersagenten](#)
[Lijst van MIME-typen](#)

Inleiding

Dit document beschrijft verschillende methoden om onbekende toepassingen op Cisco Secure Web Appliance te blokkeren.

Methoden om onbekende toepassingen te blokkeren

U kunt één van deze methoden alleen of in combinatie gebruiken.

> **Opmerking:** Deze Kennis Base artikel verwijst naar software die niet onderhouden of ondersteund wordt door Cisco. Deze informatie wordt ter beschikking gesteld als hoffelijkheid voor uw gemak. Voor verdere assistentie kunt u contact opnemen met de verkoper van de software.

Bloktoepassingen op basis van gebruikersagent Strings

De eerste verdediging is om de koorden van Gebruiker Agent te gebruiken om onbekende toepassingen te blokkeren.

- Voeg de gebruikersagent toe onder **Web Security Manager** > **Access Policies** > **Protocols and User Agents** kolom <voor het vereiste toegangsbeleid>.
- Voeg de string van de gebruikersagent toe onder het kopje **Block Custom User Agents** (één per lijn).

> **Opmerking:** U kunt de links gebruiken die onder Referentie zijn meegeleverd, om naar gebruikersagents te zoeken.

Bloktoepassingen gebaseerd op toepassingszichtbaarheidscontroles

Als Application Visibility and Control (AVC) ingeschakeld is (onder **GUI > Security Services > Web Reputation and Anti-Malware**), kunt u de toegang blokkeren op basis van toepassingstypen zoals proxy's, bestanddelen, internethulpprogramma's enzovoort. Dit kan onder **Web Security Manager > Access Policies > Applications** kolom <voor het vereiste toegangsbeleid>.

bloktoepassingen op basis van MIME-type

Als de gebruikersagent niet bestaat, kunt u proberen het MIME-type (Multipurpose Internet Mail ExUitbreidingen) toe te voegen:

- MIME-typen toevoegen onder **Web Security Manager** > **Web Access Policies** > **Objects** kolom <voor het vereiste toegangsbeleid>.
- Voeg het object/MIME-type toe in het **Block Custom MIME Types** deel (één per lijn). Bijvoorbeeld om bitTorrent-toepassingen te blokkeren, dient u application/x-bittorrent.

  Opmerking: U kunt de links gebruiken die onder Referentie zijn meegeleverd om naar MIME-typen te zoeken.

URL-categorieën in toegangsbeleid blokkeren

Zorg ervoor dat categorieën zoals filterpreventie, illegale activiteiten, illegale downloads, enzovoort worden geblokkeerd in het toegangsbeleid. Als sommige toepassingen bekende URL's of IP-adressen voor hun verbindingen gebruiken, dan kunt u hun gekoppelde vooraf gedefinieerde URL-categorieën blokkeren of ze in een geblokkeerde aangepaste URL-categorie configureren met hun IP-adres, Full Qualified Domain Name (FQDN) of een regex dat overeenkomt met de domeinen. Dit kan onder **Web Security Manager > Access Policies > URL Categories** kolom.

HTTP-configuratie van poorten beperken in toegangsbeleid

Sommige toepassingen kunnen de HTTP CONNECT-methode gebruiken om verbinding te maken met verschillende poorten. Laat alleen bekende poorten of de specifieke poorten toe die in uw omgeving nodig zijn in de HTTP CONNECT-gebieden voor poortconfiguratie:

- HTTP CONNECT kan worden geconfigureerd onder **Web Security Manager** > **Access Policies** > **Protocols and User Agents** kolom <voor het vereiste toegangsbeleid>.
- Toevoegen toegestane poorten onder **HTTP CONNECT Ports**.

Bloktoegang voor specifieke IP-adressen

Voor toepassingen waar u alleen weet van bestemming IP adressen die worden benaderd, kunt u de functie L4 Traffic Monitor gebruiken om de toegang voor die specifieke IP-adressen te blokkeren. U kunt de bestemmings-IP's toevoegen onder **Web Security Manager > L4 Traffic Monitor > Additional Suspected Malware Addresses**.

Hoe te vinden welke gebruikersagent of MIME een toepassing gebruikt

Als u niet weet welke gebruikersagent of MIME-type door bepaalde toepassingen wordt gebruikt, kunt u een van deze stappen uitvoeren om deze informatie te vinden:

- Start een pakketvastlegging met WireShark (Etheral) op de client en filter voor 'http'-protocol.
- Start de opname op Secure Web Appliance (onder) **Support and Help** > **Packet Capture**), gefilterd op het IP-adres van de klant.

Referentie

> **Opmerking:** De hier genoemde externe websites zijn slechts ter referentie vermeld. De verbindingen en de inhoud worden niet door Cisco gecontroleerd en zijn onderhevig aan verandering.

Lijst van gebruikersagenten

User Agent String.com (bij User agentstring.com)

Lijst van MIME-typen

- Vaak voorkomende MIME-typen (op mozilla.org)
- MIME-typen: Volledige lijst van MIME-typen (op w3cub.com)
- De volledige lijst van MIME-typen (op site.com)