

Verkeer omzeilen in Secure Web Appliance

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verschillende soorten bypass](#)

[SWA-procedures omzeilen op implementatietype](#)

[Verkeer omzeilen bij expliciete implementatie](#)

[Configuratie PAC-bestand](#)

[Browserconfiguratie \(Microsoft Edge, Internet Explorer, Google Chrome\)](#)

[Browserconfiguratie \(Mozilla FireFox\)](#)

[Browserconfiguratie \(Apple Safari\)](#)

[Configuratie groepsbeleid](#)

[Verkeer omzeilen in transparante implementatie](#)

[SWA-bypassinstelling](#)

[Het verkeer omleiden van de WCCP/PBR-router](#)

[Pass Through configureren en verkeer toestaan in SWA](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de stappen beschreven voor het omzeilen van verkeer in Secure Web Appliance (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SWA-beheer.
- Basisprotocollen voor netwerken en proxy's

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.

Verschillende soorten bypass

In SWA zijn er drie verschillende concepten van het omzeilen van verkeer van het bereik van de SWA die afhankelijk is van uw Proxy-implementatie (expliciete of transparante implementatie), of van het worden geanalyseerd en gescand door de SWA. Hier volgt een kort overzicht van deze drie concepten:

- Bypass: een instelling die voorkomt dat verkeer de SWA bereikt, waardoor het gebruik van de netwerkinterfacekaart (NIC) wordt verlaagd en er geen sessie tussen de gebruiker en het toestel nodig is.
- Doorgeven: deze configuratie voorkomt dat de SWA HTTPS-verkeer decodeert. Desondanks blijft de SWA twee afzonderlijke sessies faciliteren: één tussen de client en de SWA en een tweede tussen de SWA en de webserver.
- Toestaan: een instelling in het toegangsbeleid waarbij HTTP of gedecodeerd verkeer de inspectie door interne SWA-engines overslaat, zoals AMP, Sophos, WebRoot en het toepassingsfilter. In dit geval zijn er nog steeds twee sessies in gebruik in de SWA.

Type	Applies to	Transparent Deployment	Explicit Deployment	Configuration Path	Logging	Number of Sessions	Description
Bypass from SWA	HTTPS & HTTP			GUI > Web Security Manager > Bypass Settings	Bypasslogs	1	SWA routes the traffic to configured gateway (Layer 3 redirection)
Bypass from WCCP Router	HTTPS & HTTP			WCCP Router	No Logs on SWA	0	Traffic Redirects to the Gateway from Router
Bypass from PAC	HTTPS & HTTP			From the PAC file	No Logs on SWA	0	Requests are not sent to the proxy.
Bypass from Browser	HTTPS & HTTP			From the Browser or Group Policy	No Logs on SWA	0	Requests are not sent to the proxy.
Pass Through	HTTPS & HTTP			GUI > Web Security Manager > Decryption Policy	Accesslogs	2	SWA does not decrypt the traffic and sends the same ClientHello to the web server.
Allow	Decrypted Traffic & HTTP			GUI > Web Security Manager > Access Policy	Accesslogs	2	SWA does not Scan the traffic with its scanning engines, such as AMP, Sophos, WebRoot, AVC and ...

Afbeelding - Vergelijkingstabel

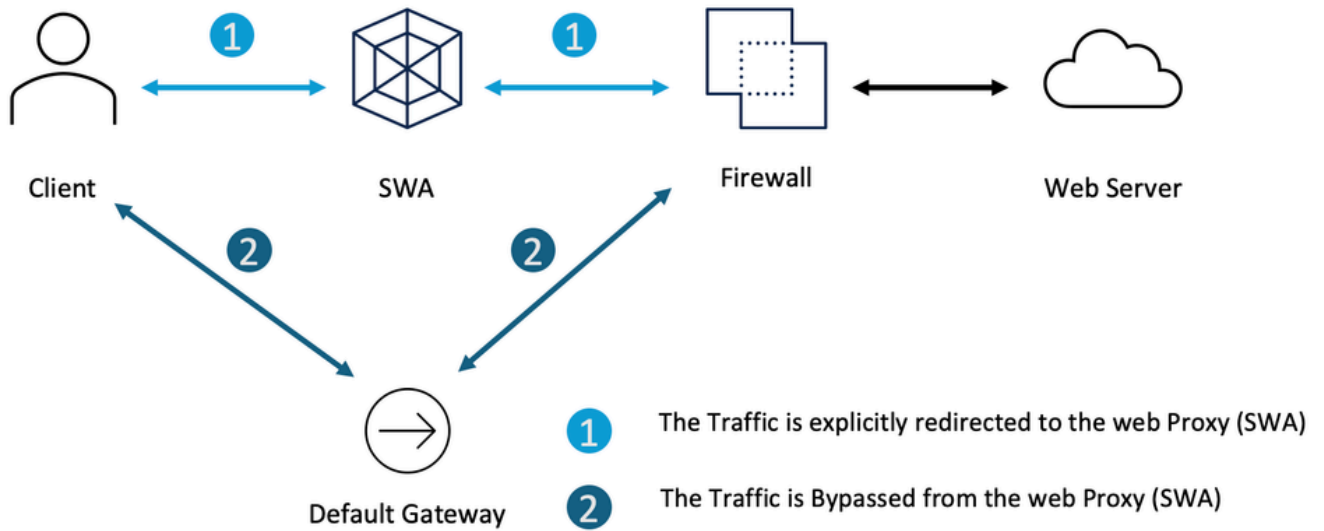
SWA-procedures omzeilen op implementatietype

Bypass-procedures zijn afhankelijk van uw model voor proxy-implementatie. Hier is een kort overzicht van elk type:

- Expliciete implementatie: clients worden handmatig geconfigureerd om verkeer naar de proxy te leiden.
- Transparante implementatie: netwerkinfrastructuur leidt automatisch verkeer om naar de proxy, zonder configuratie aan de clientzijde.

Verkeer omzeilen bij expliciete implementatie


Als u het verkeer in de expliciete implementatie wilt omzeilen, moet u de client configureren om het webverzoek voor de gewenste URL's niet door te sturen naar de SWA. Zoals in dit netwerkdiagram wordt weergegeven, gaat een deel van het verkeer rechtstreeks naar de firewall of de standaardgateway om de SWA te omzeilen (pad nummer 2).

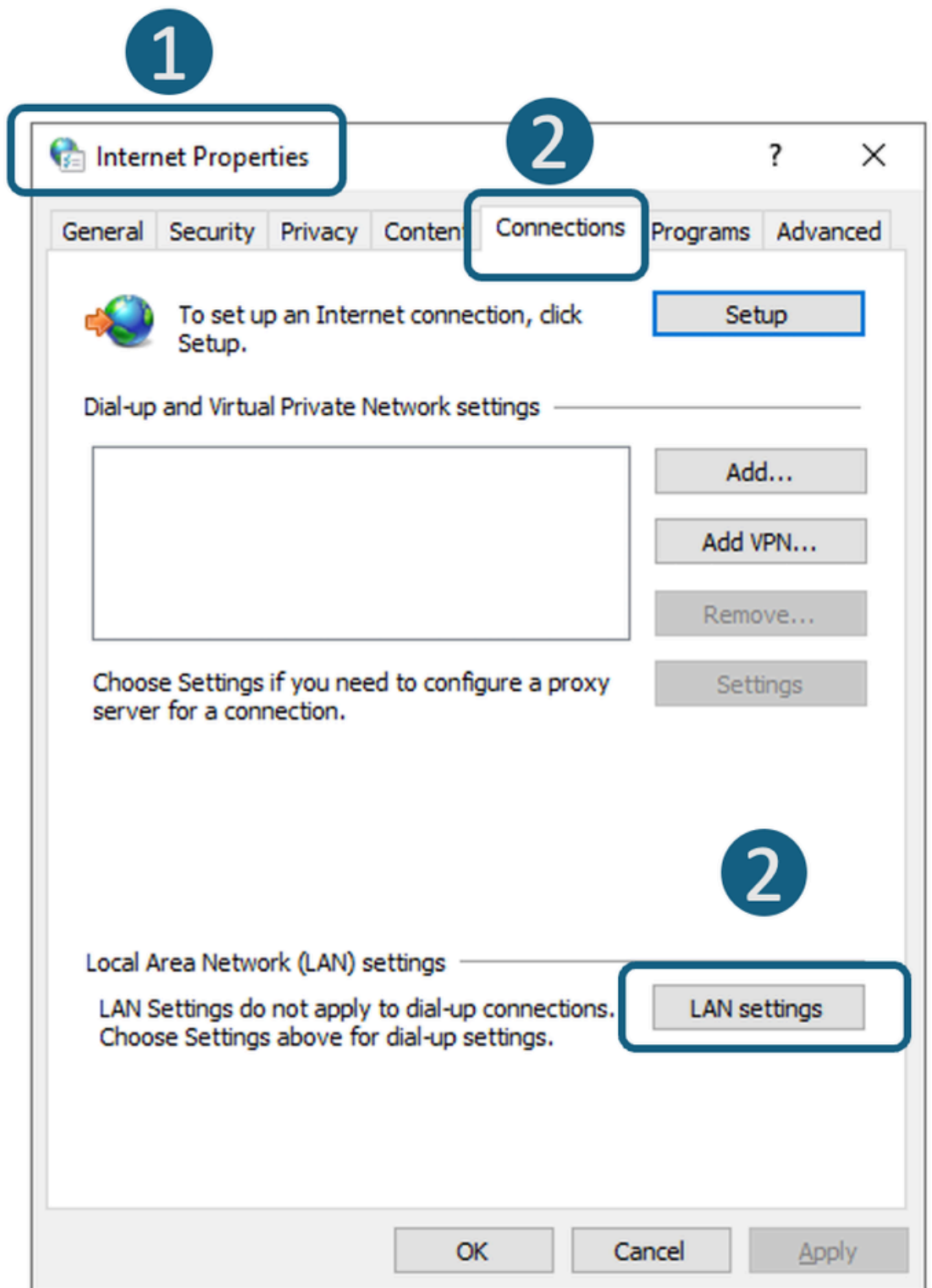


Afbeelding - Omzeilen van het verkeer in expliciete implementatie

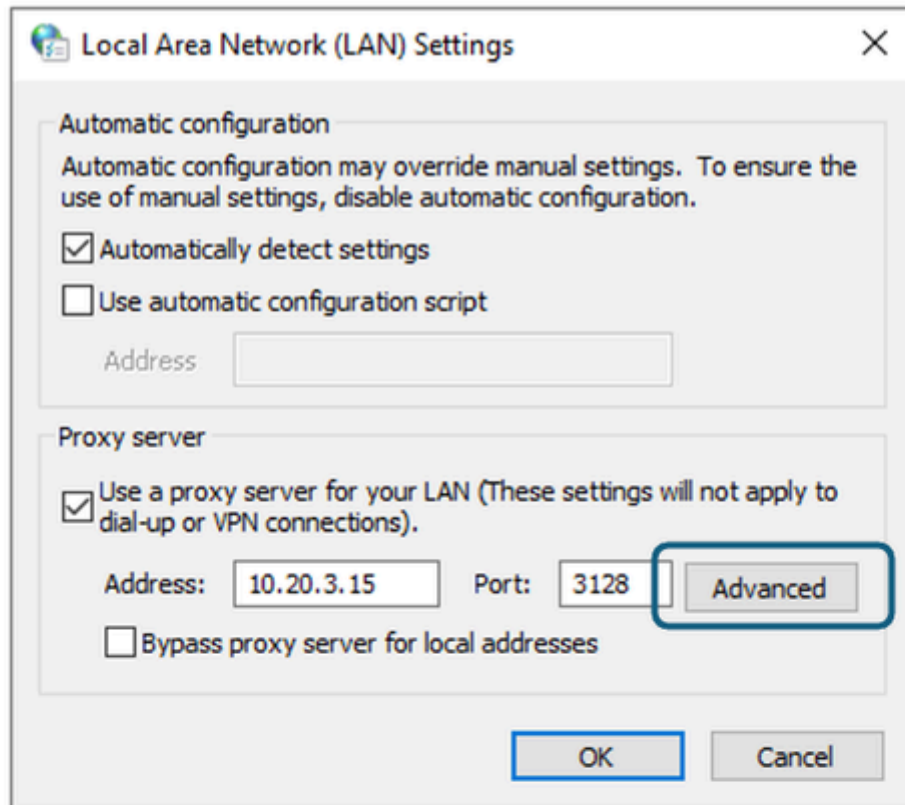
Afhankelijk van uw expliciete proxy-implementatie, kunt u sommige URL's vrijstellen om naar de SWA te worden omgeleid.

<p>Expliciete proxyconfiguratie</p>	<p>Stappen om URL's uit te sluiten van het bereik van de SWA</p>
<p>Configuratie PAC-bestand</p>	<p>Afhankelijk van hoe u uw PAC-bestand hebt geconfigureerd, kunt u de uitzonderingslijst definiëren en de actie instellen op DIRECT.</p> <p>Hier zijn enkele voorbeelden om het privé-IP-adres te omzeilen en de SWA te bereiken</p> <pre>var resolved_ip = dnsResolve(host); if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") isInNet(resolved_ip, "127.0.0.0", "255.255.255.0")) return "DIRECT";</pre> <p>Dit is een voorbeeld van het omzeilen van het verkeer naar www.cisco.com van het omleiden van de SWA</p> <pre>if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";</pre> <p>In dit voorbeeld worden alle subdomeinen van cisco.com omzeild door de SWA om</p>

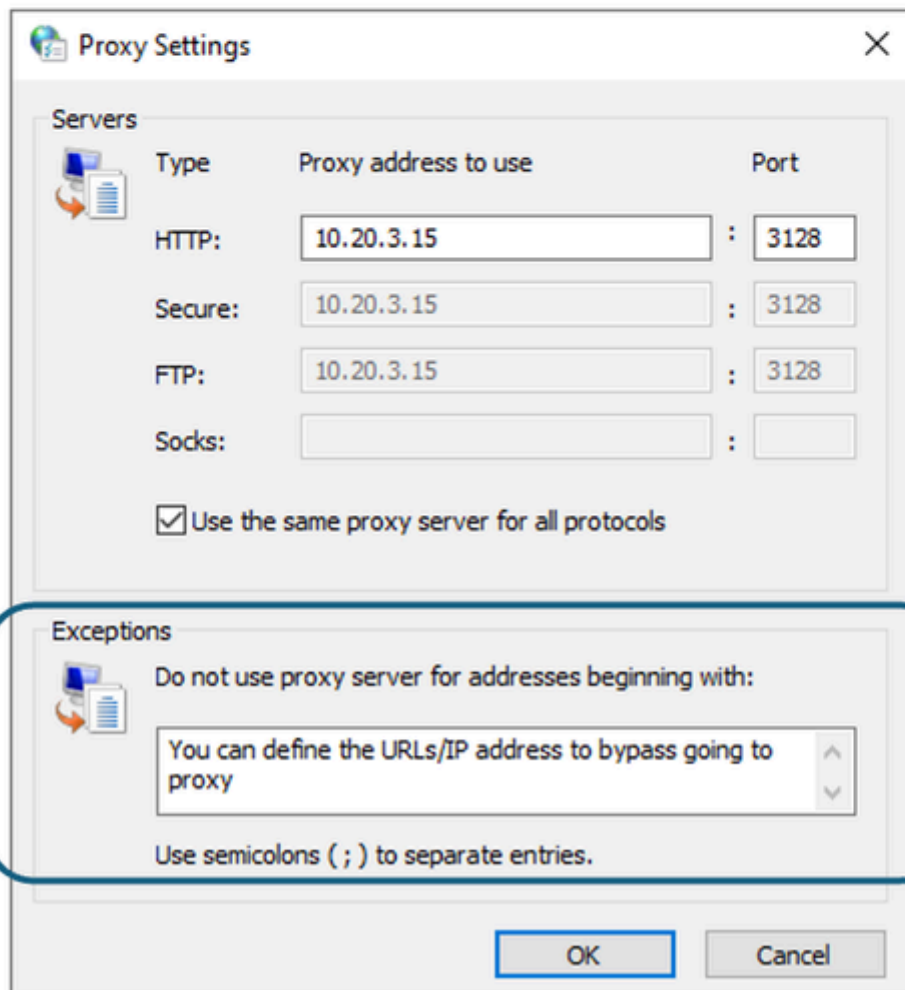
	<p>te leiden</p> <pre>if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";</pre> <hr/> <p> Opmerking: Aangezien het PAC-bestand geen Cisco-product is, wordt de informatie met het oog op uw gemak verstrekt. Voor verdere hulp kunt u contact opnemen met de softwareleverancier.</p> <hr/>
Browserconfiguratie (Microsoft Edge, Internet Explorer, Google Chrome)	<p>Stap 1. Typ in het menu Start "Internetopties" en druk op ENTER</p> <p>Stap 2. Navigeer naar het tabblad Verbindingen en klik op LAN-instellingen</p> <p>Stap 3. Klik op de geavanceerde</p> <p>Stap 4. Definieer uw gewenste URL's in het gedeelte Uitzonderingen.</p>



Afbeelding - Navigeer naar LAN-instellingen



3



4

Browserconfiguratie
(Mozilla FireFox)

Stap 1. Klik in de rechterbovenhoek op het menu met drie balken en selecteer Instellingen.

Stap 2. Typ in de zoekbalk proxy.

Stap 3. Definieer uw gewenste URL's in de sectie Geen proxy voor.

Connection Settings

Configure Proxy Access to the Internet

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

Manual proxy configuration

HTTP Proxy Port

Also use this proxy for HTTPS

HTTPS Proxy Port

SOCKS Host Port

SOCKS v4 SOCKS v5

Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

Do not prompt for authentication if password is saved

Proxy DNS when using SOCKS v4

Proxy DNS when using SOCKS v5

Afbeelding - Definieer de uitzonderingen in Fire Fox

Browserconfiguratie
(Apple Safari)

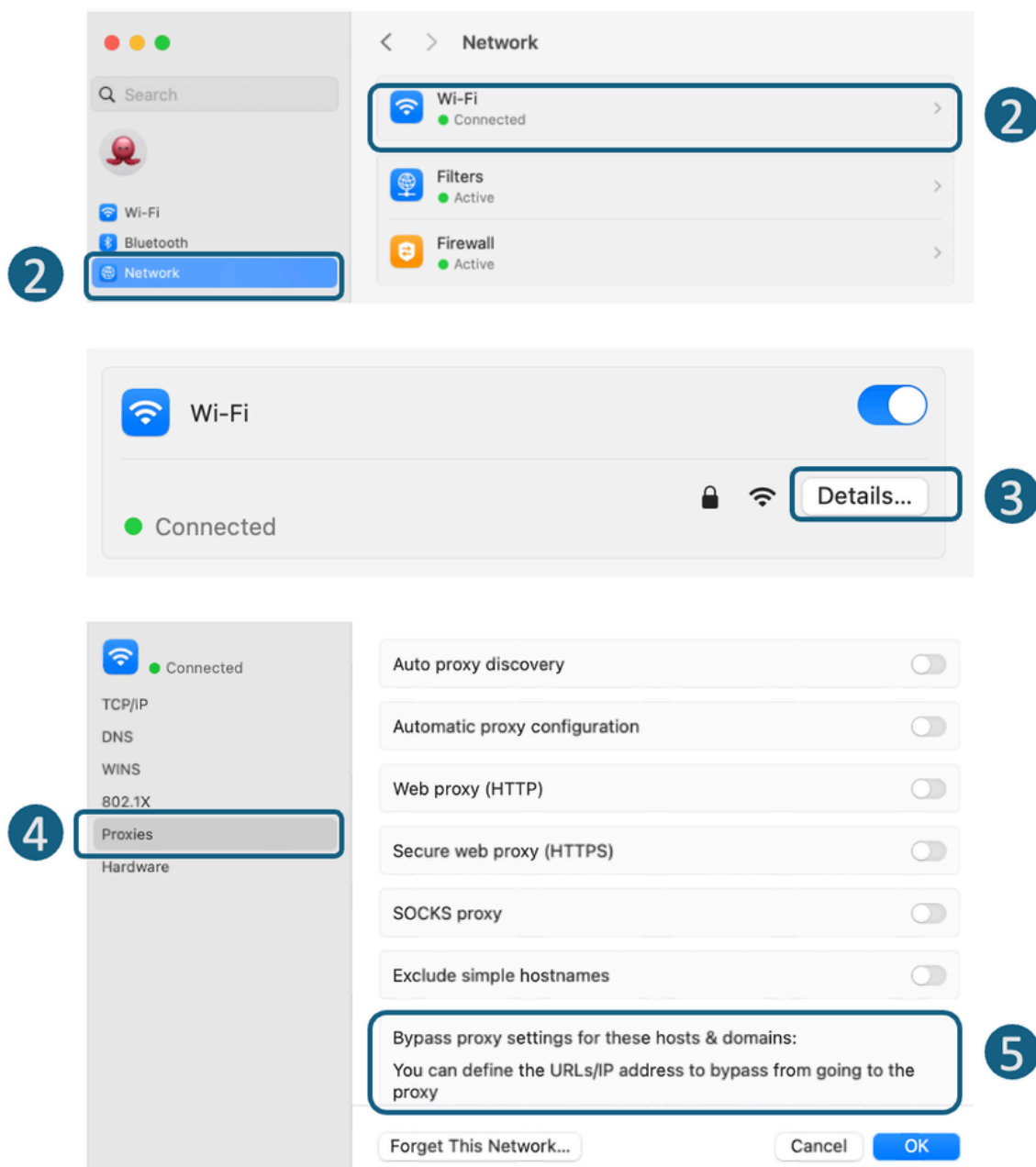
Stap 1. Klik in de linkerbovenhoek op het Apple-pictogram en kies Systeeminstellingen.

Stap 2. Navigeer in het linkerdeelvenster naar Netwerk en selecteer de netwerkinterface die u gebruikt om toegang te krijgen tot internet.

Stap 3. Klik op de details.

Stap 4. Selecteer in het linkerdeelvenster Proxies.

Stap 5. Definieer uw gewenste URL's in het gedeelte Proxy-instellingen omzeilen.



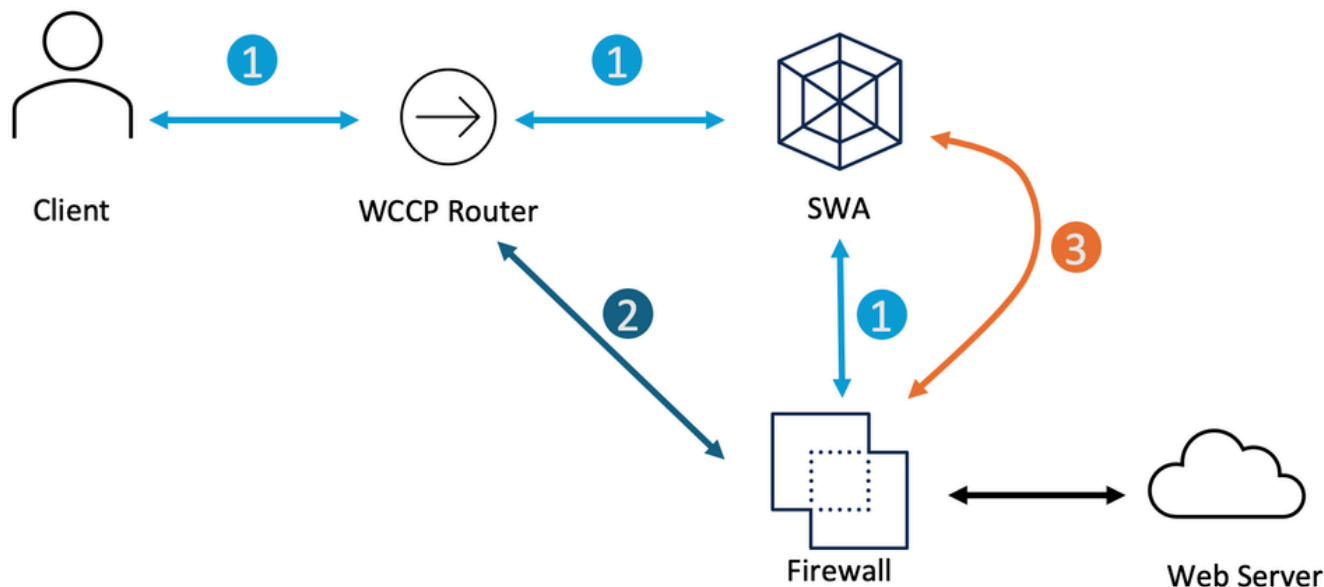
Afbeelding - Definieer de uitzonderingen in Fire Fox

Configuratie
groepsbeleid

Afhankelijk van hoe u het groepsbeleid hebt geconfigureerd om de proxy-instellingen te pushen, kunt u de uitzonderingenlijst definiëren.

Verkeer omzeilen in transparante implementatie

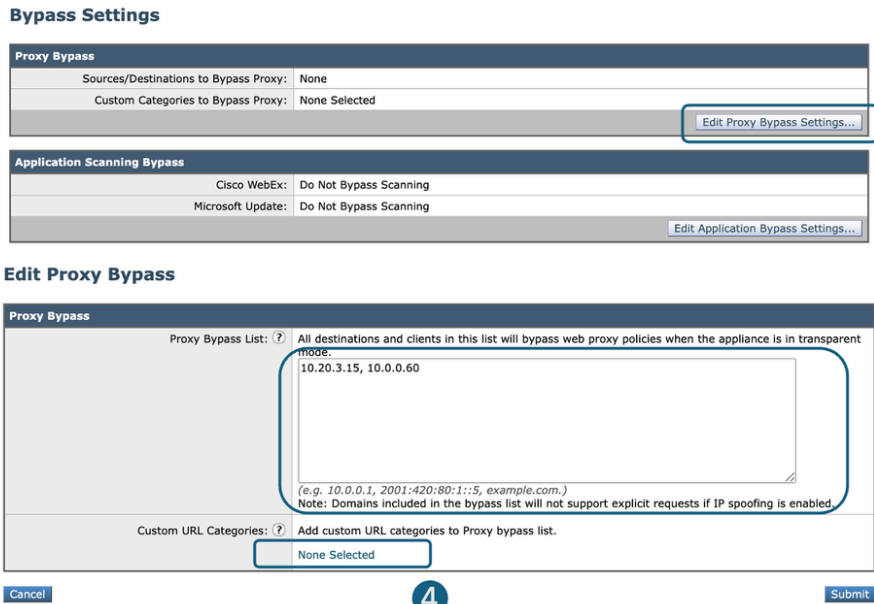

U kunt verkeer in een transparante implementatie omzeilen met behulp van de WCCP-router of SWA Bypass-instellingen. SWA Bypass werkt op Layer 3, routeert het verkeer naar de standaardgateway en omzeilt het toestel volledig, waardoor de verwerking en het maken van afzonderlijke sessies wordt voorkomen.



- 1** The Traffic is Transparently redirected to the SWA
- 2** The Traffic is Redirected from the WCCP Router, to not go to the SWA
- 3** The Traffic is Bypassed in the SWA as a layer 3 traffic and routes to the SWA Default Gateway

Afbeelding - Het verkeer omzeilen in transparante implementatie

<p>Transparante proxyimplementatie van verkeer omzeilen</p>	<p>Stappen om het verkeer te omzeilen van het bereik van de SWA</p>
<p>SWA-bypassinstelling</p>	<p>Stap 1. Kies Web Security Manager vanuit de GUI.</p> <p>Stap 2. Selecteer Instellingen omzeilen.</p> <p>Stap 3. Klik op Proxy Bypass-instellingen bewerken.</p> <p>Stap 4. U kunt de URL, het IP-adres of een aangepaste URL-categorie aan de lijst toevoegen.</p> <p>Stap 5. Verzenden en vastleggen van de wijzigingen.</p>

	 <p>Afbeelding - Instellingen voor bypass configureren</p> <p> Tip: verkeer dat met deze instellingen wordt omzeild, wordt niet aangemeld in de accesslogs en kan worden bekeken in de bypass_logs.</p>
<p>Het verkeer omleiden van de WCCP/PBR-router</p>	<p>U kunt het IP-adres van de bron of bestemming configureren in uw WCCP of PBR (Policy Based Router) om bepaalde verkeer niet naar de SWA om te leiden.</p>

Pass Through configureren en verkeer toestaan in SWA

Als het verkeer de SWA raakt en om de belasting op de SWA te verminderen vanwege de privacyproblemen, wilt u niet dat het verkeer voor sommige URL's wordt geïnspecteerd door de SWA, gebruikt u deze stappen.

Stappen	Stappen
<p>Stap 1. Maak een aangepaste URL-rubriek voor de URL's.</p>	<p>Stap 1.1. Kies Web Security Manager van GUI en klik op Aangepaste en Externe URL-categorieën. Stap 1.2. Klik op Categorie toevoegen om een aangepaste URL-rubriek toe te voegen. Stap 1.3. Een unieke categorienaam toewijzen.</p>

Stap 1.4. (Optioneel) Beschrijving toevoegen.

Stap 1.5. Kies in Lijstvolgorde de eerste categorie die u bovenaan wilt plaatsen.

Stap 1.6. Kies in de vervolgkeuzelijst Categorie de optie Lokale aangepaste rubriek.

Stap 1.7. Voeg gewenste URL's toe in de sectie Sites.

Stap 1.8. Verzenden.

Custom and External URL Categories: Add Category

1.3 → Category Name: No Proxy URL

1.5 → List Order: 1

1.6 → Category Type: Local Custom Category

1.7 → Sites: www.cisco.com

Sort URLs
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

Advanced Regular Expressions: ?

Enter one regular expression per line. Maximum allowed characters 2048.

Cancel Submit

Afbeelding - Een aangepaste URL-rubriek maken

Stap 2. Maak een identificatieprofiel om verkeer uit te sluiten van verificatie.

Stap 2.1. Kies Web Security Manager van GUI en klik op Identificatieprofielen.

Stap 2.2. Klik op Profiel toevoegen om een profiel toe te voegen.

Stap 2.3. Gebruik het selectievakje Identificatieprofiel inschakelen om dit profiel in te schakelen of snel uit te schakelen zonder het te verwijderen.

Stap 2.4. Een unieke profielnaam toewijzen.

Stap 2.5. (Optioneel) Beschrijving toevoegen.

Stap 2.6. Kies in de vervolgkeuzelijst Invoegen hierboven waar dit profiel in de tabel moet worden weergegeven.

Stap 2.7. In het gedeelte Gebruikersidentificatiemethoden kiest u Vrijstellen van verificatie/identificatie.

Stap 2.8. In de Leden definiëren op subnet, laat dit veld leeg om alle client IP-adres op te nemen, tenzij u wilt passeren door het verkeer voor een bepaald IP-adres.

Stap 2.9. Kies in de sectie Geavanceerd de optie Aangepaste URL-categorieën.

Identification Profiles: Add Profile

Afbeelding - Identificatieprofiel toevoegen

Stap 2.10. Voeg de aangepaste URL-categorie toe die is gemaakt in stap 1.

Stap 2.11. Klik op Gereed.

Stap 2.12. Verzenden.

Stap 3. Maak een decoderingsbeleid om door het verkeer te gaan.

Stap 3.1. Van GUI, Kies Web Security Manager en klik vervolgens op Decryptie Policy.

Stap 3.2. Klik op Beleid toevoegen om een decoderingsbeleid toe te voegen.

Stap 3.3. Gebruik het selectievakje Beleid inschakelen om dit beleid in te schakelen.

Stap 3.4. Een unieke beleidsnaam toewijzen.

Stap 3.5. (Optioneel) Beschrijving toevoegen.

Stap 3.6. Kies het eerste beleid uit de vervolgkeuzelijst Invoegen boven beleid.

Stap 3.7. Kies in het gedeelte Identificatieprofielen en gebruikers het identificatieprofiel dat u in stap 2 hebt gemaakt.

Stap 3.8. Verzenden.

Decryption Policy: Add Group

Afbeelding - Een decoderingsbeleid maken

Stap 3.9. Op de pagina Decryptiebeleid, onder URL-filtering, klikt u op de link die is gekoppeld aan dit nieuwe Decryptiebeleid.

Decryption Policies

Success — The policy group "DP Pass Through" was added.

Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DP Pass Through Identification Profile: No Auth ID All identified users	Monitor: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Pass Through: 0 Monitor: 0 Decrypt: 0 Drop: 0 Time-Based: 0 Quota-Based: 0	Not Available	Decrypt		

Afbeelding - URL-filtering selecteren

Stap 3.10. Selecteer Doorgeven als de actie voor de URL-categorie die is gemaakt in stap 1.

Decryption Policies: URL Filtering: DP Pass Through

Custom and External URL Category Filtering

Add, edit, reorder or delete categories in the Custom and External URL Categories list.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop ?	Quota-Based	Time-Based
No Proxy URL	Custom (Local)	—	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Afbeelding - De actie instellen om door te gaan

Stap 3.11. Verzenden.

Stap 4. Maak een toegangsbeleid om Microsoft Updates-verkeer toe te staan.

Stap 4.1. Kies Web Security Manager vanuit GUI en klik op Access Policy.

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

Stap 4.3. Gebruik het selectievakje **Beleid inschakelen** om dit beleid in te schakelen.

Stap 4.4. Een unieke beleidsnaam toewijzen.

Stap 4.5. (Optioneel) **Beschrijving** toevoegen.

Stap 4.6. Kies het eerste beleid uit de vervolgkeuzelijst **Invoegen boven beleid**.

Stap 4.7. Kies in het gedeelte **Identificatieprofielen en gebruikers** het identificatieprofiel dat u in stap 2 hebt gemaakt.

Stap 4.8. **Verzenden**.

Access Policy: Add Group

Policy Settings

Enable Policy

Policy Name: (e.g. my IT policy)

Description:

(Maximum allowed characters 256)

Insert Above Policy:

Policy Expires:

Set Expiration for Policy

On Date:

At Time:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Identification Profile:

Authorized Users and Groups:

Afbeelding - Toegangsbeleid maken

Stap 4.9. Op de pagina **Toegangsbeleid**, onder **URL-filtering**, klikt u op de koppeling die is gekoppeld aan dit nieuwe toegangsbeleid.

Access Policies

Success - The policy group "AP Allow" was added.

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP Rewrite Profile	Clone Policy	Delete
1	AP Allow Identification Profile: No Auth ID All identified users	(global policy)	Monitor: 1	(global policy)	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Block: 0 Warn: 0 Monitor: 0 Allow: 0 Redirect: 0 Time-Based: 0 Quota-Based: 0	Not Available	No blocked items	Secure Endpoint: Enabled	None		

Afbeelding - URL-filtering selecteren

Stap 4.10. Selecteer **Toestaan de actie** voor de aangepaste URL-categorie die is gemaakt voor de URL-categorie die is gemaakt bij stap 1.

Custom and External URL Category Filtering		Use Global Settings		Override Global Settings					
Category	Category Type	Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based	
No Proxy URL	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)	

4.10

Afbeelding - Actie toestaan instellen

Stap 4.11. Verzenden.

Stap 4.12. Wijzigen doorvoeren.

Gerelateerde informatie

- [Microsoft Updates-verkeer omzeilen in Secure Web Appliance](#)
- [Verificatie omzeilen in Secure Web Appliance - Cisco](#)
- [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](#)
- [Best practices voor veilige webapparaten gebruiken - Cisco](#)
- [Verkeer blokkeren in Secure Web Appliance](#)
- [Uploadverkeer blokkeren in Secure Web Appliance](#)
- [Executable File Download blokkeren in SWA](#)

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.