Verkeer omzeilen in Secure Web Appliance

Inhoud

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 bereiken 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

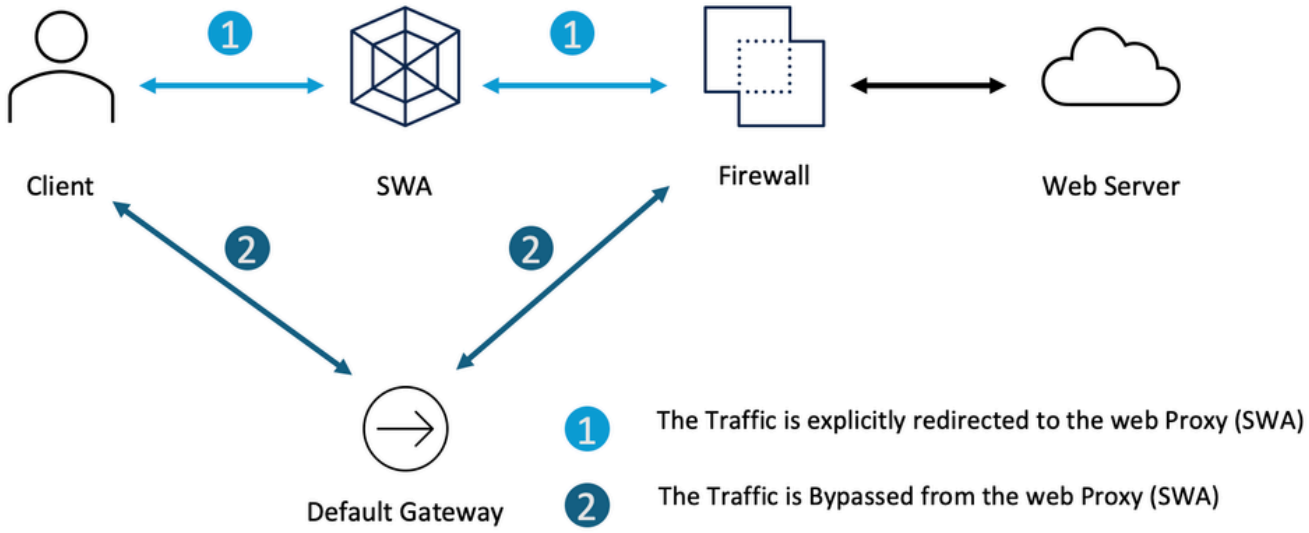
SWA-procedures omzeilen op implementatietype

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).



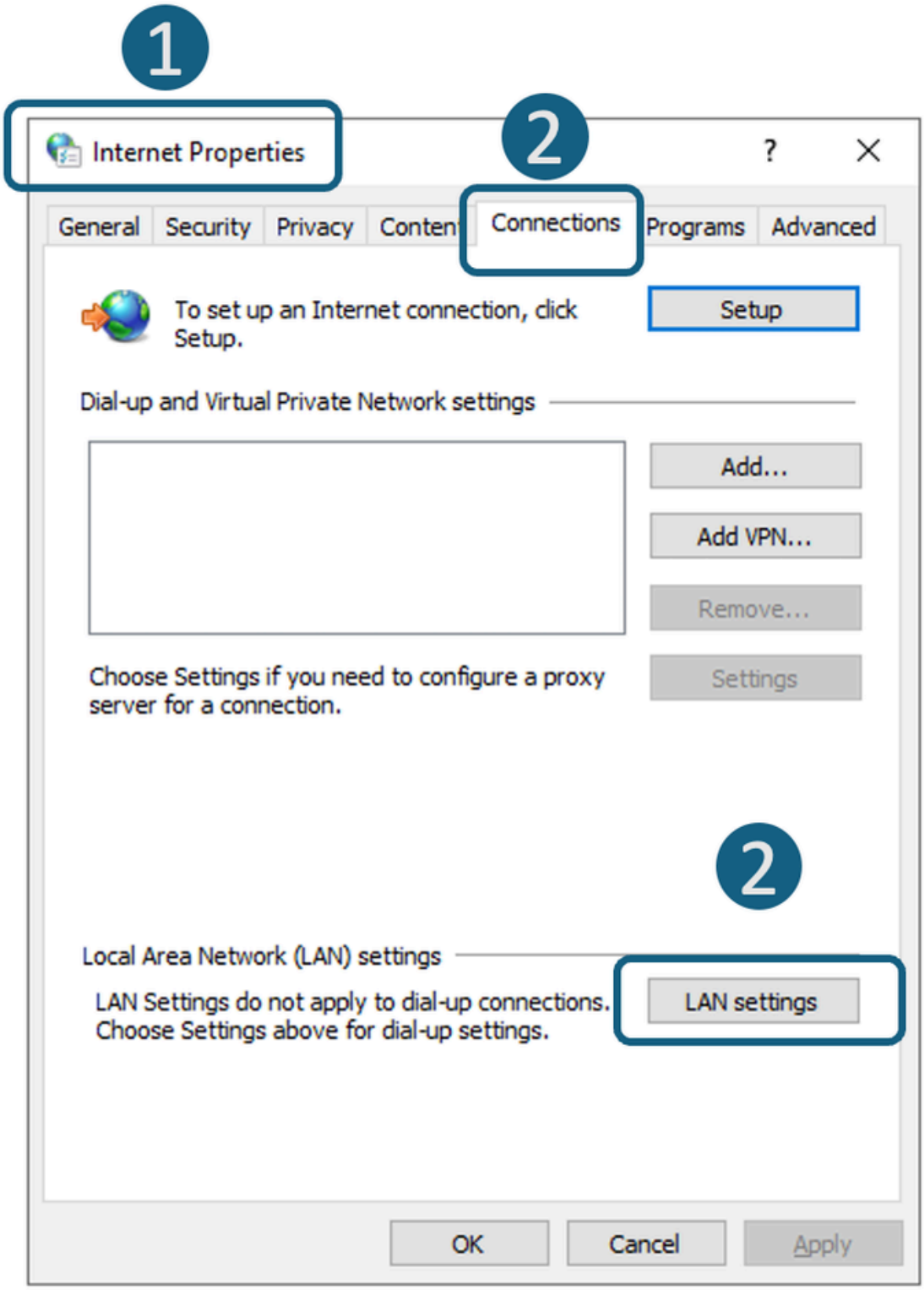
Afbeelding - Omzeilen van het verkeer in expliciete implementatie

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

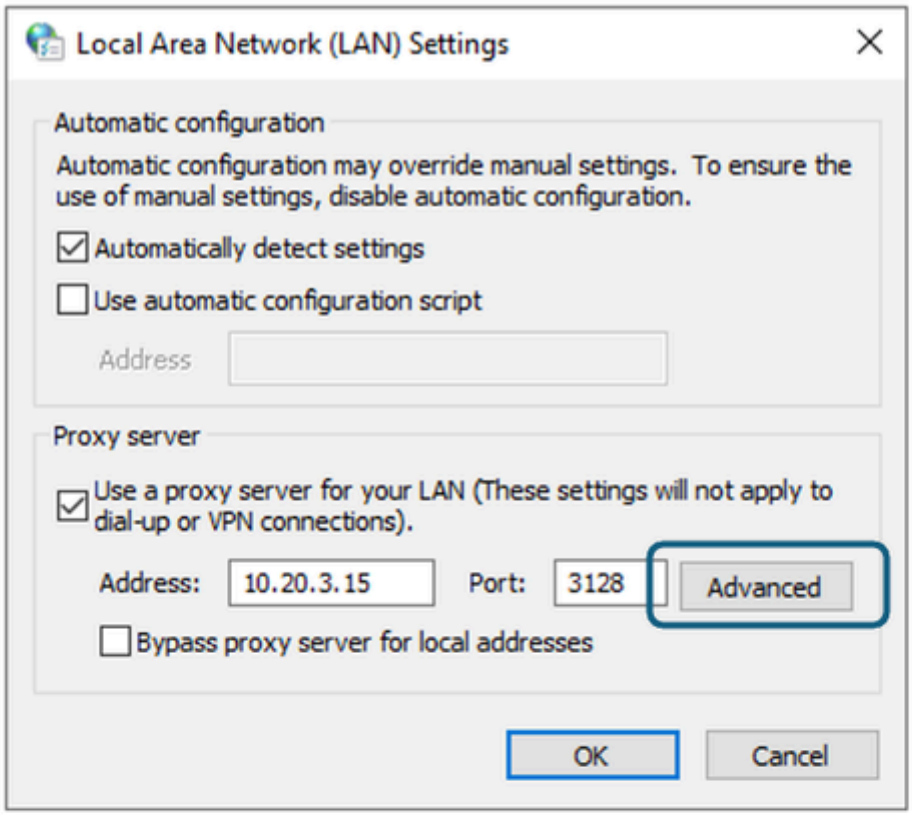
Expliciete proxyconfiguratie	Stappen om URL's uit te sluiten van het bereiken van de SWA

Configuratie PAC-bestand	Afhankelijk van hoe u uw PAC-bestand hebt geconfigureerd, kunt u de uitzonderingenlijst definiëren en de actie instellen op DIRECT.
	
	Hier zijn enkele voorbeelden om het privé-IP-adres te omzeilen en de SWA te bereiken
	
	`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";`
	
	Dit is een voorbeeld van het omzeilen van het verkeer naar www.cisco.com van het omleiden van de SWA
	
	`if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";`
	
	In dit voorbeeld worden alle subdomeinen van cisco.com omzeild door de SWA om

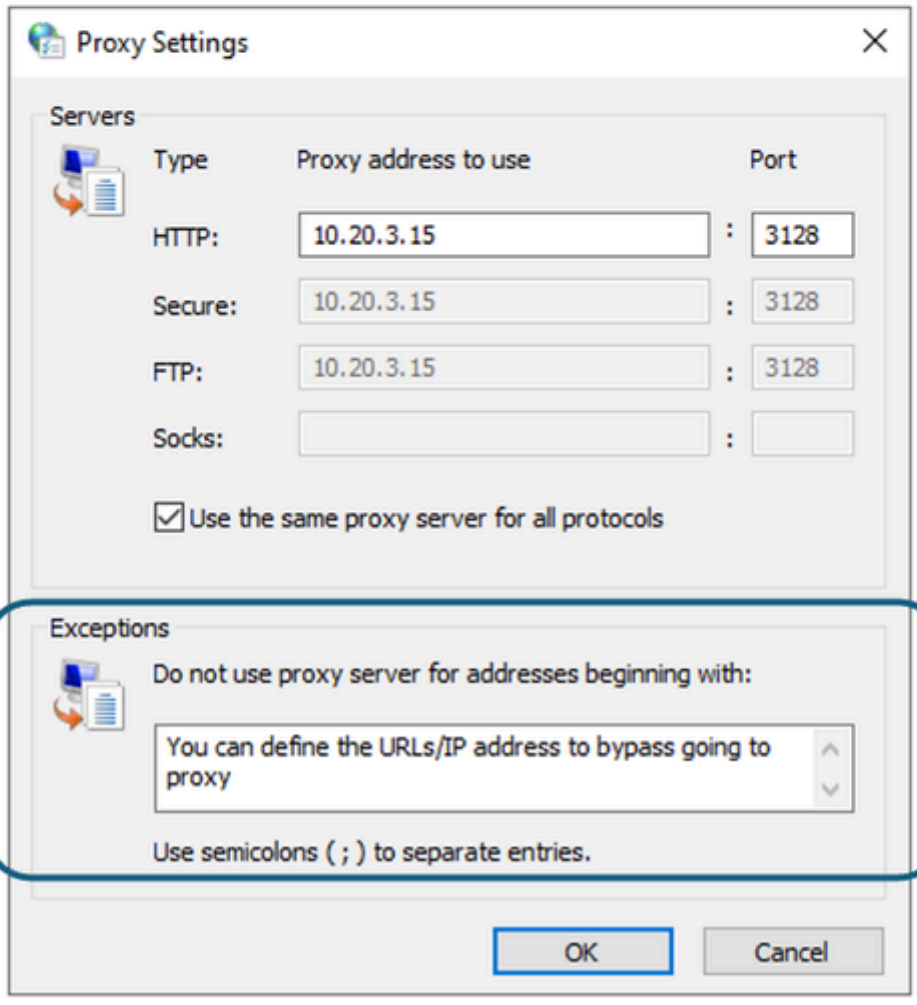
	te leiden `if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";` Opmerking: Aangezien het PAC-bestand geen Cisco-product is, wordt de informatie met het oog op uw gemak verstrekt. Voor verdere hulp kunt u contact opnemen met de softwareleverancier.
Browserconfiguratie (Microsoft Edge, Internet Explorer,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



Afbeelding - Navigeer naar LAN-instellingen

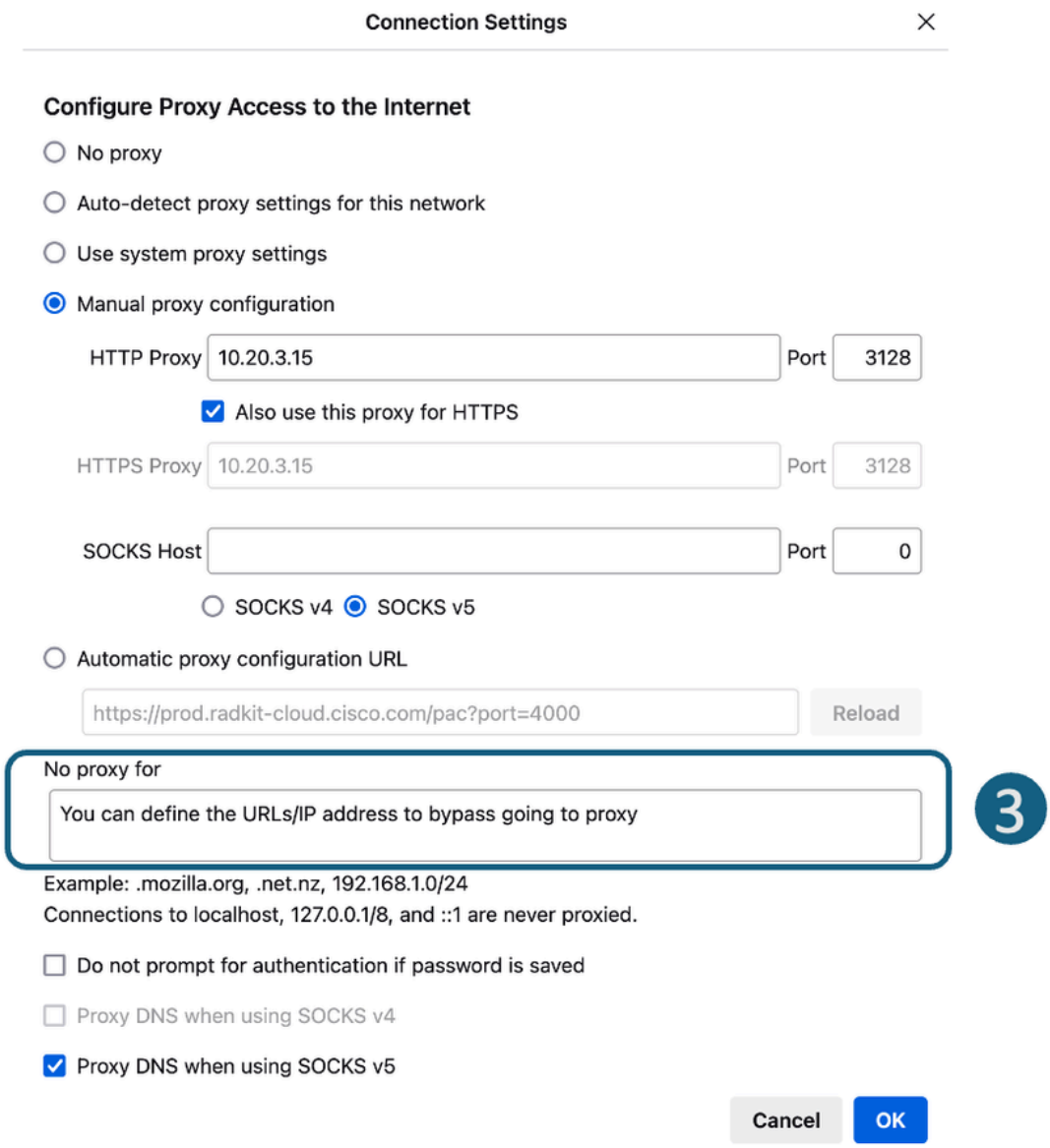


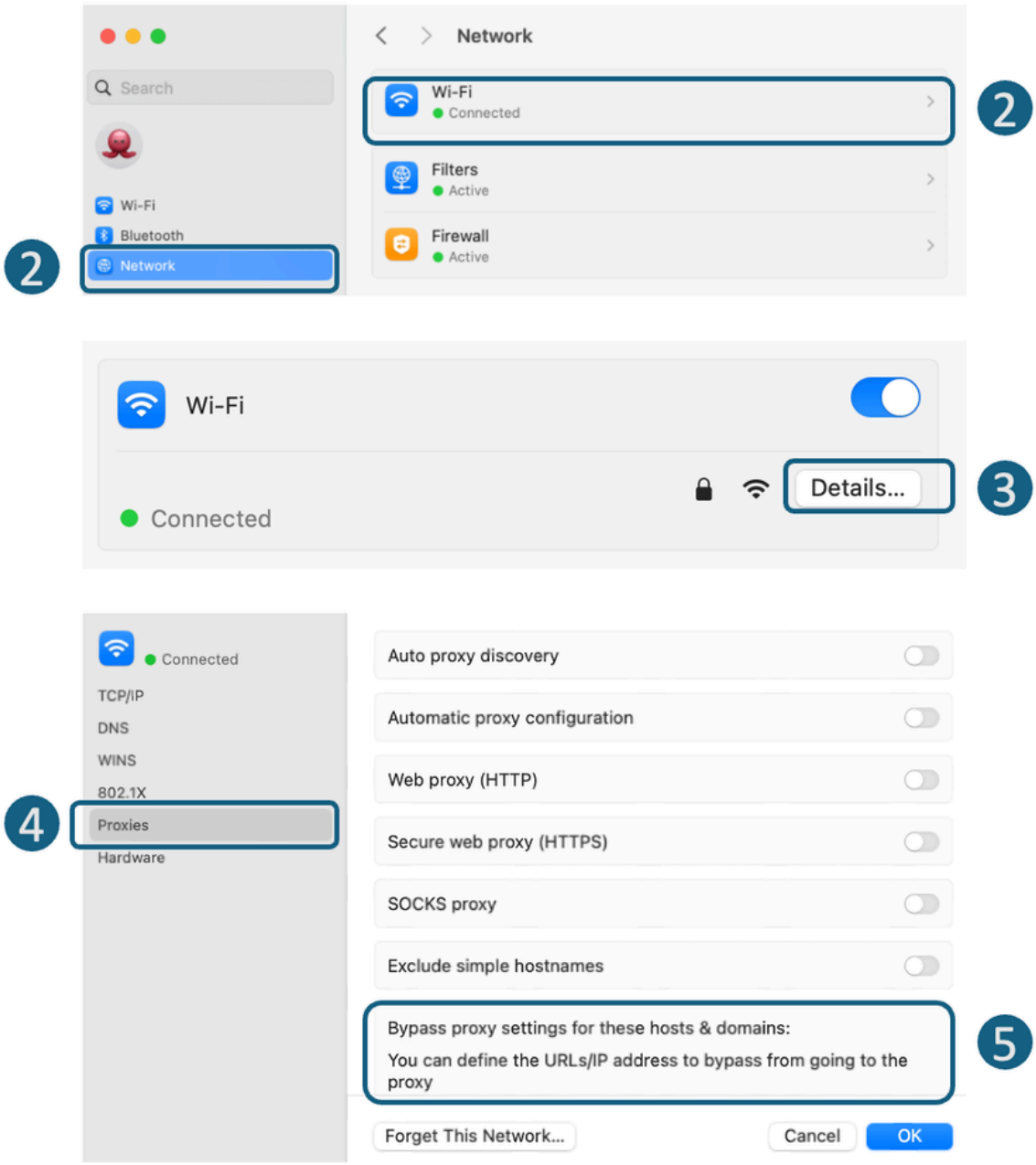
3



4

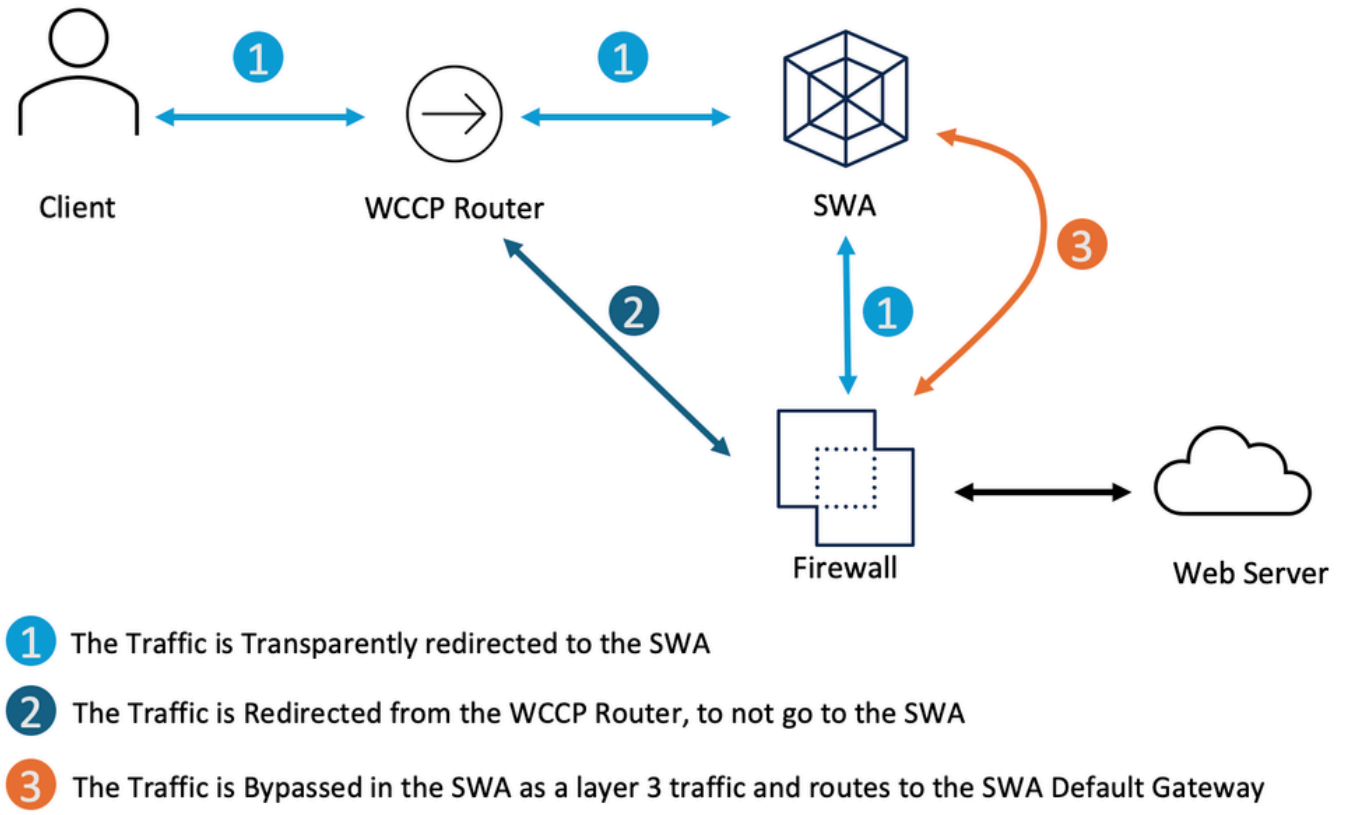
Afbeelding - De uitzonderingen definiëren

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.  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.

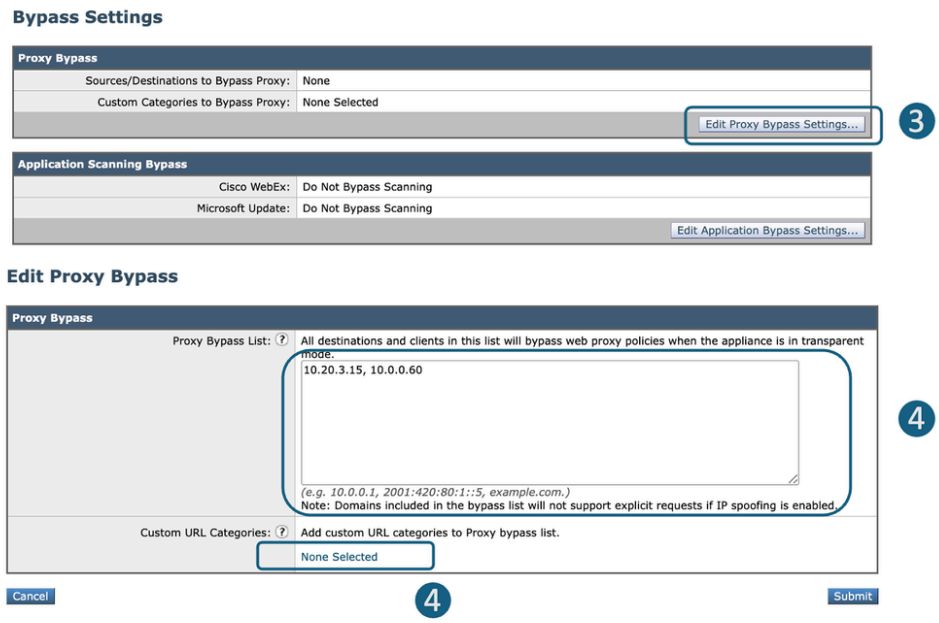
Verkeer omzeilen in transparante implementatie

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.



Afbeelding - Het verkeer omzeilen in transparante implementatie

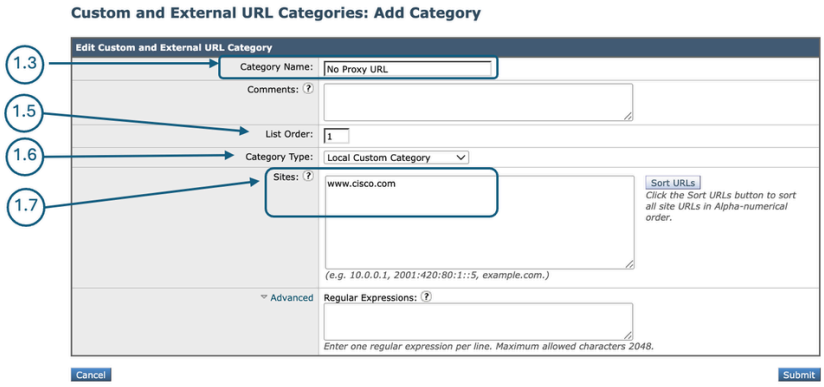
Transparante proxyimplementatie van verkeer omzeilen	Stappen om het verkeer te omzeilen van het bereiken van de SWA
SWA-bypassinstelling	Stap 1. Kies Web Security Manager vanuit de GUI. Stap 2. Selecteer Instellingen omzeilen. Stap 3. Klik op Proxy Bypass-instellingen bewerken. Stap 4. U kunt de URL,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

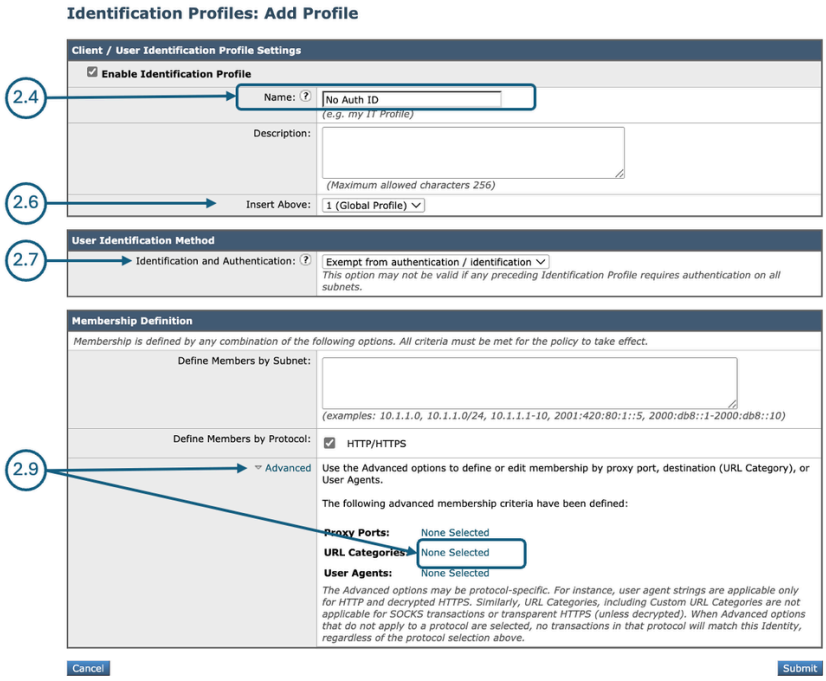
	 Afbeelding - Instellingen voor bypass configureren Tip: verkeer dat met deze instellingen wordt omzeild, wordt niet aangemeld in de accesslogs en kan worden bekeken in de bypass_logs.
Het verkeer omleiden van de WCCP/PBR-router	U kunt het IP-adres van de bron of bestemming configureren in uw WCCP of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

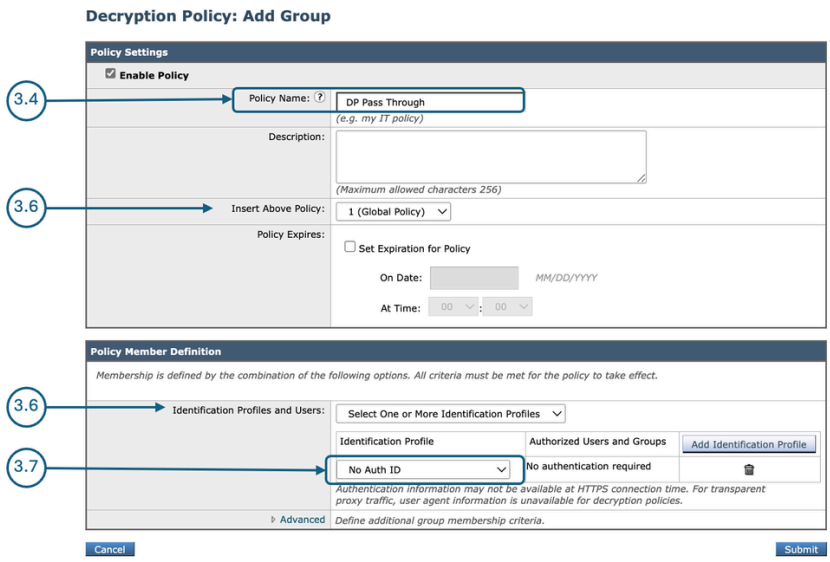
Pass Through configureren en verkeer toestaan in SWA

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
Stap 1. Maak een aangepaste URL-rubriek voor de URL's.	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.

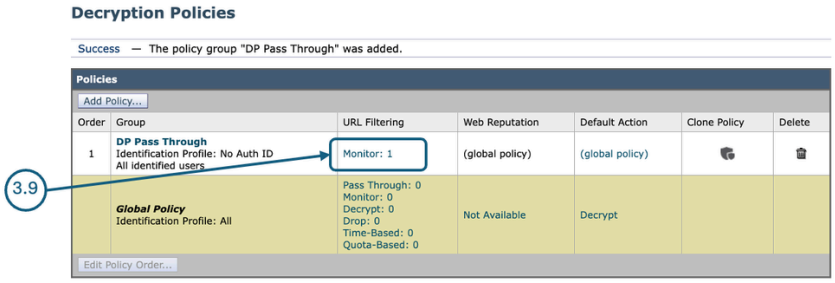
	Stap 1.4. (Optioneel) Beschrijving toevoegen. Stap 1.5. Kies in Lijstvolgorde de eerste categorie die u bovenaan wilt plaatsen. Stap 1.6. Kies in de vervolgkeuzelijst Categorie de optie Lokale aangepaste rubriek. Stap 1.7. Voeg gewenste URL's toe in de sectie Sites. Stap 1.8. Verzenden.  Afbeelding - 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.

	 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.



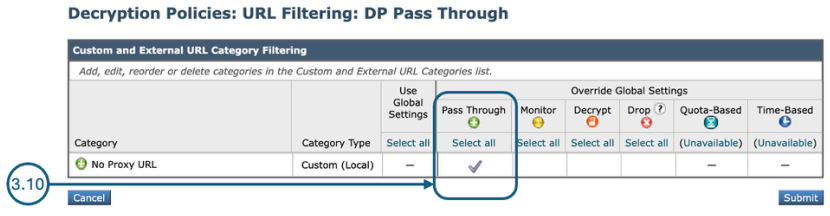
Afbeelding - Een decoderingsbeleid maken

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



Afbeelding - URL-filtering selecteren

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



Afbeelding - De actie instellen om door te gaan

Stap 3.11. Verzenden.

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

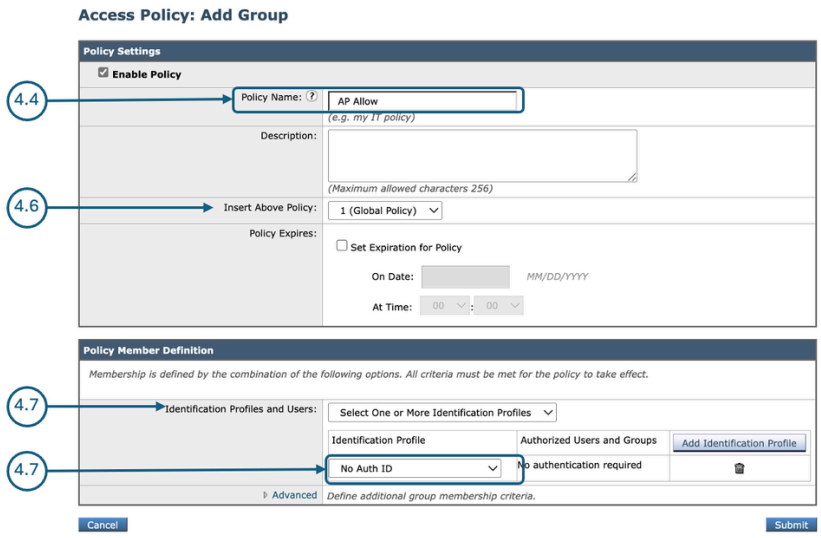
Stap 4.1.Kies Web Security Manager vanuit GUI en klik opAccess Policy.

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.

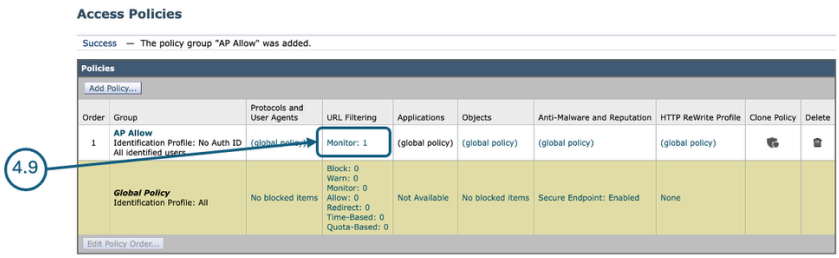
Stap 4.7.Kies in het gedeelte Identificatieprofielen en gebruikers het identificatieprofiel dat u in stap 2 hebt gemaakt.

Stap 4.8. Verzenden.



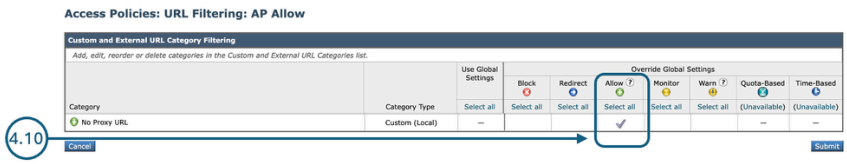
Afbeelding - Toegangsbeleid maken

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



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.



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.