Umgehung des Datenverkehrs in einer sicheren Web-Appliance

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Verschiedene Arten von Umgehungen
- SWA-Umgehungsverfahren nach Bereitstellungstyp
  - Datenverkehr bei expliziter Bereitstellung umgehen
    - Konfiguration der PAC-Datei
    - Browserkonfiguration (Microsoft Edge, Internet Explorer, Google Chrome)
    - Browserkonfiguration (Mozilla FireFox)
    - Browserkonfiguration (Apple Safari)
    - Gruppenrichtlinienkonfiguration
  - Datenverkehr in transparenterBereitstellung umgehen
    - SWA-Umgehungseinstellung
    - Umleitung des Datenverkehrs vom WCCP/PBR-Router
- Konfigurieren von Passthrough und Zulassen von Datenverkehr in SWA
- Zugehörige Informationen

Einleitung

In diesem Dokument werden die Schritte zur Umgehung des Datenverkehrs in der Secure Web Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SWA-Verwaltung.
- Grundlegende Netzwerk- und Proxy-Protokolle

Cisco empfiehlt die Installation der folgenden Tools:

- Physisches oder virtuelles SWA
- Administratorzugriff auf die grafische Benutzeroberfläche (GUI) von SWA

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Verschiedene Arten von Umgehungen

In SWA gibt es drei verschiedene Konzepte zur Umgehung eines Datenverkehrs, der den SWA nicht erreicht, was von Ihrer Proxy-Bereitstellung (Explicit oder Transparent Deployment) abhängt, oder von der Analyse und dem Scannen durch den SWA. Im Folgenden finden Sie einen Überblick über diese drei Konzepte:

- Umgehung: Eine Einstellung, die verhindert, dass Datenverkehr die SWA erreicht. Dadurch wird die Auslastung der Netzwerkschnittstellenkarten (NIC) reduziert und eine Sitzung zwischen Benutzer und Gerät wird überflüssig.
- Durchstellen: Diese Konfiguration verhindert, dass der SWA HTTPS-Datenverkehr entschlüsselt. Dennoch werden im SWA weiterhin zwei getrennte Sitzungen angeboten: eine zwischen dem Client und dem SWA und eine zweite zwischen dem SWA und dem Webserver.
- Zulassen: Eine Einstellung in der Zugriffsrichtlinie, bei der HTTP- oder entschlüsselter Datenverkehr die Prüfung durch interne SWA-Engines wie AMP, Sophos, WebRoot und den Anwendungsfilter überspringt. In diesem Fall werden in der SWA noch zwei Sitzungen verwendet.

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 ...

Bild - Vergleichsdiagramm

SWA-Umgehungsverfahren nach Bereitstellungstyp

Bypass-Verfahren unterscheiden sich je nach Proxybereitstellungsmodell. Im Folgenden finden Sie eine kurze Übersicht über die einzelnen Typen:

- Explizite Bereitstellung: Clients werden manuell konfiguriert, um den Datenverkehr an den Proxy weiterzuleiten.
- Transparente Bereitstellung: Die Netzwerkinfrastruktur leitet den Datenverkehr automatisch zum Proxy um, sodass keine Konfiguration auf Client-Seite erforderlich ist.

Datenverkehr bei expliziter Bereitstellung umgehen

Um den Datenverkehr in der expliziten Bereitstellung zu umgehen, müssen Sie den Client so konfigurieren, dass die Webanforderung für die gewünschten URLs nicht an den SWA weitergeleitet wird. Wie in diesem Netzwerkdiagramm dargestellt, wird ein Teil des Datenverkehrs direkt an die Firewall oder das Standard-Gateway weitergeleitet, um das SWA zu umgehen (Pfad 2).

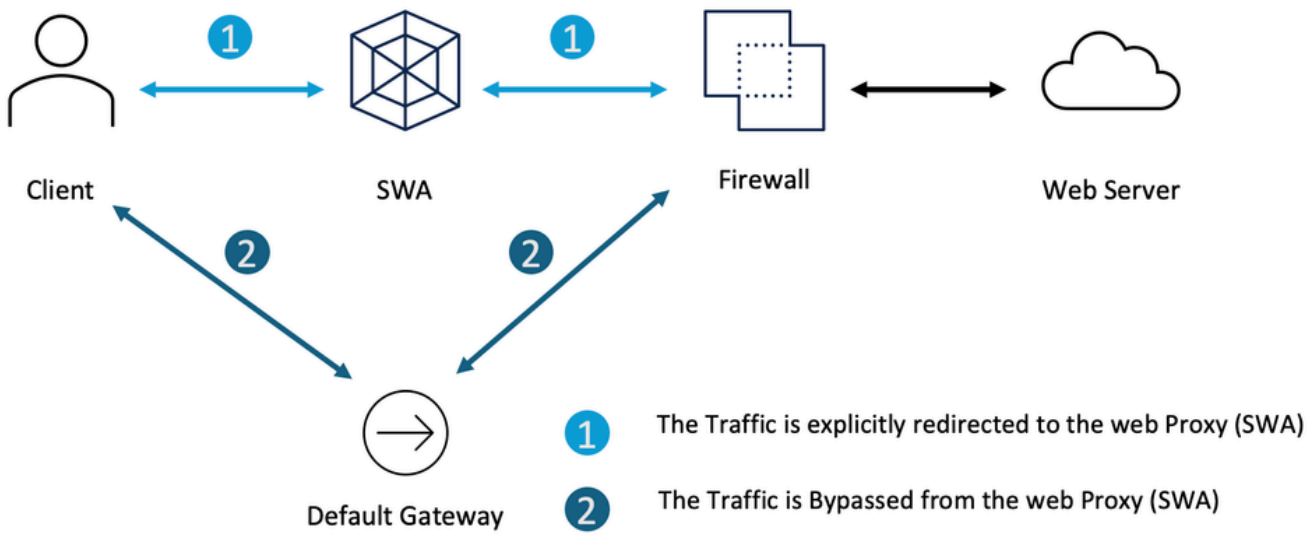


Image - Umgehung des Datenverkehrs bei expliziter Bereitstellung

Abhängig von Ihrer expliziten Proxy-Bereitstellung können Sie einige URLs ausnehmen, die an die SWA umgeleitet werden sollen.

Explizite Proxykonfiguration	Schritte, um URLs vom Erreichen des SWA auszuschließen

Konfiguration der PAC-Datei	Je nachdem, wie Sie die PAC-Datei konfiguriert haben, können Sie die Ausnahmeliste definieren und die Aktion auf DIRECT festlegen.
	
	Nachfolgend finden Sie einige Beispiele, wie die private IP-Adresse vom Server umgangen werden kann.
	
	`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";`
	
	Dieses Beispiel umgeht die SWA-Umleitung des Datenverkehrs zu www.
	
	`if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";`
	
	In diesem Beispiel werden alle Subdomänen von cisco.com daran gehinc SWA-Domäne

	`if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";` Anmerkung: Da es sich bei der PAC-Datei nicht um ein Produkt von handelt, werden die Informationen zu einem späteren Zeitpunkt bere Wenden Sie sich für weitere Unterstützung an den Softwareanbieter
Browserkonfiguration (Microsoft Edge, Internet Explorer, Google Chrome)	Schritt 1. Geben Sie im Startmenü "Internetoptionen" ein und drücken Sie Eingabetaste. Schritt 2: Navigieren Sie zur Registerkarte Connections (Verbindungen), klicken Sie auf LAN Settings (LAN-Einstellungen) Schritt 3: Klicken Sie auf "Erweitert" Schritt 4: Definieren Sie die gewünschten URLs im Abschnitt "Ausnahme

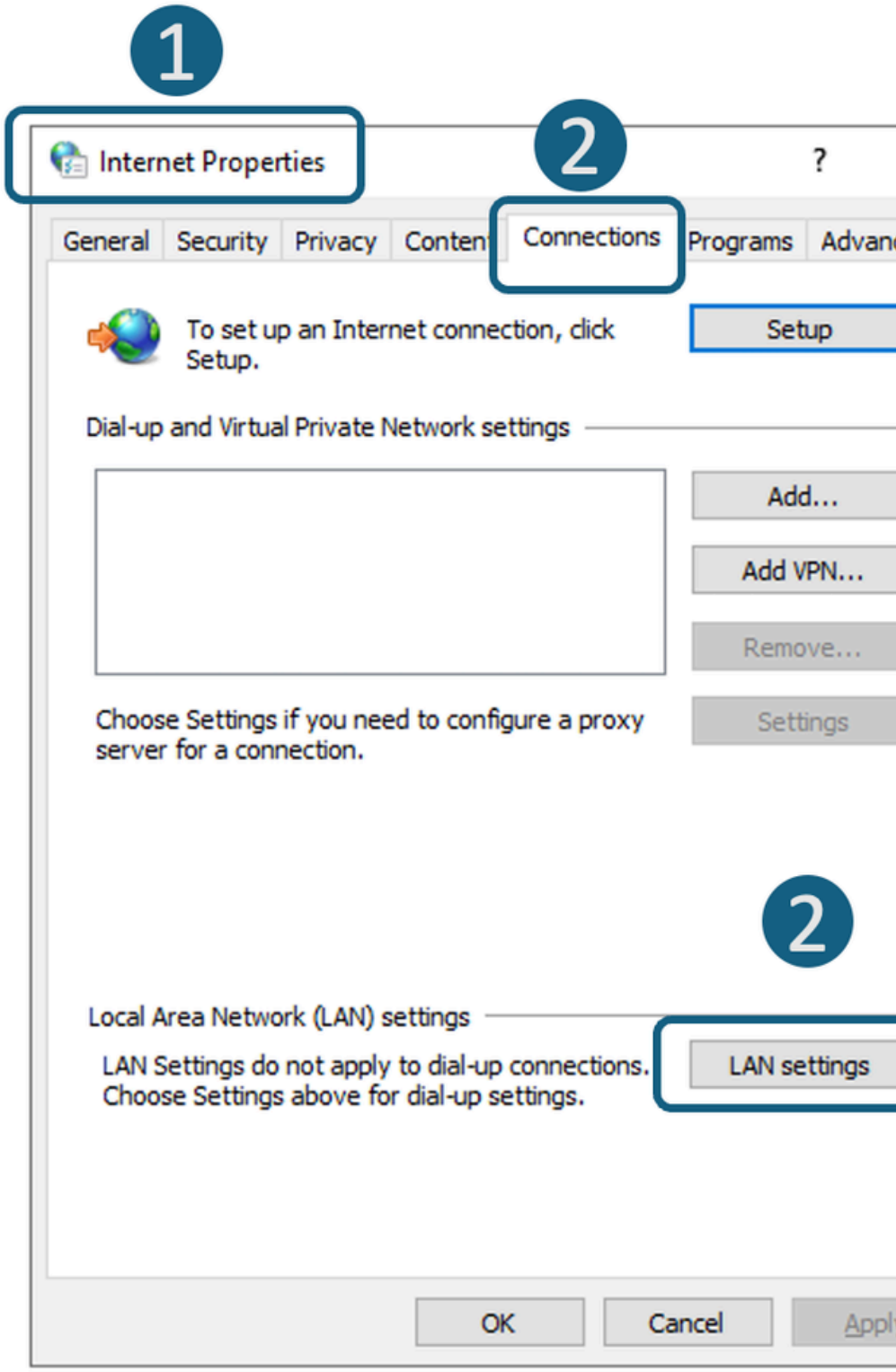


Bild - Navigieren zu LAN-Einstellungen

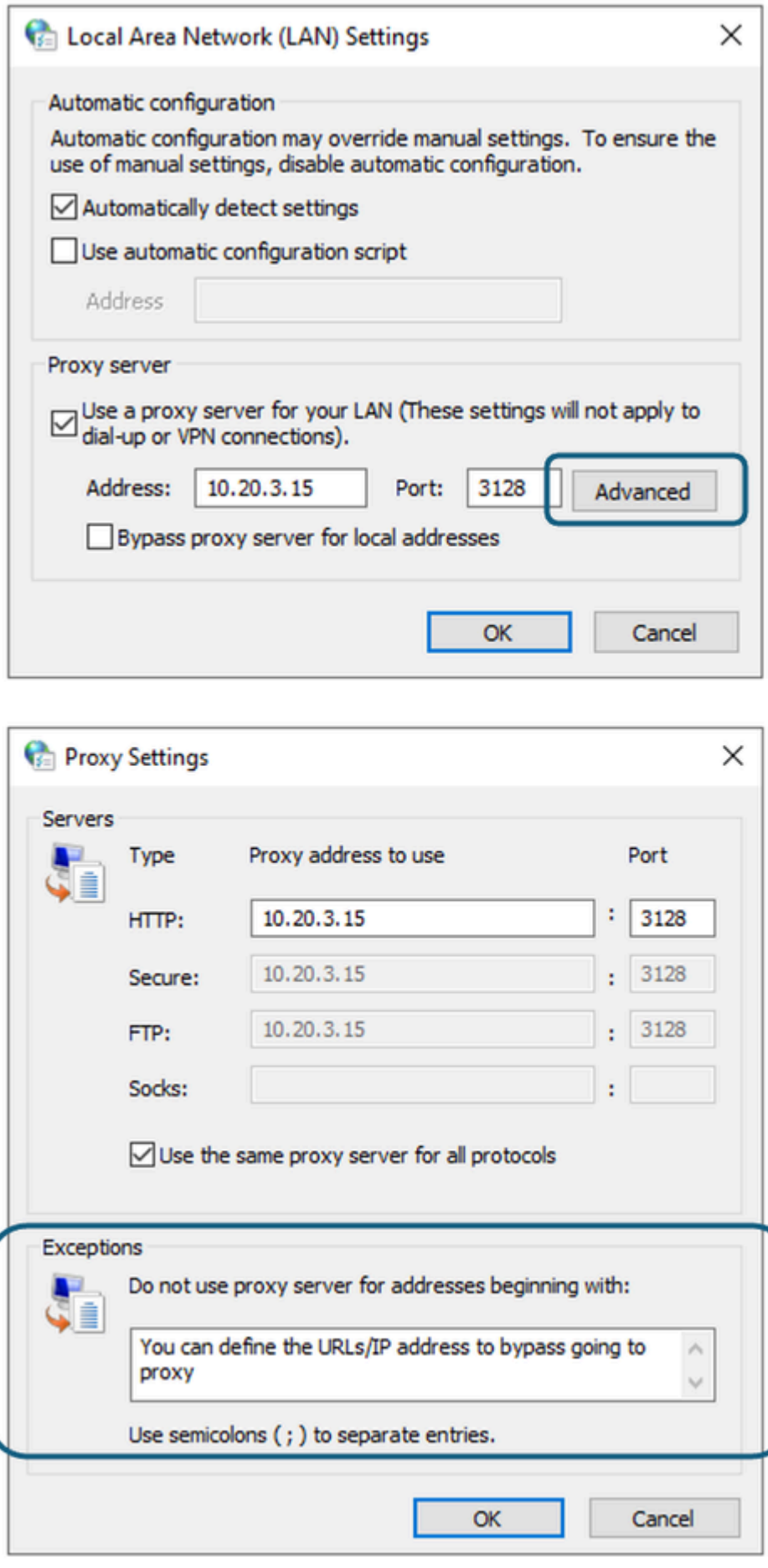
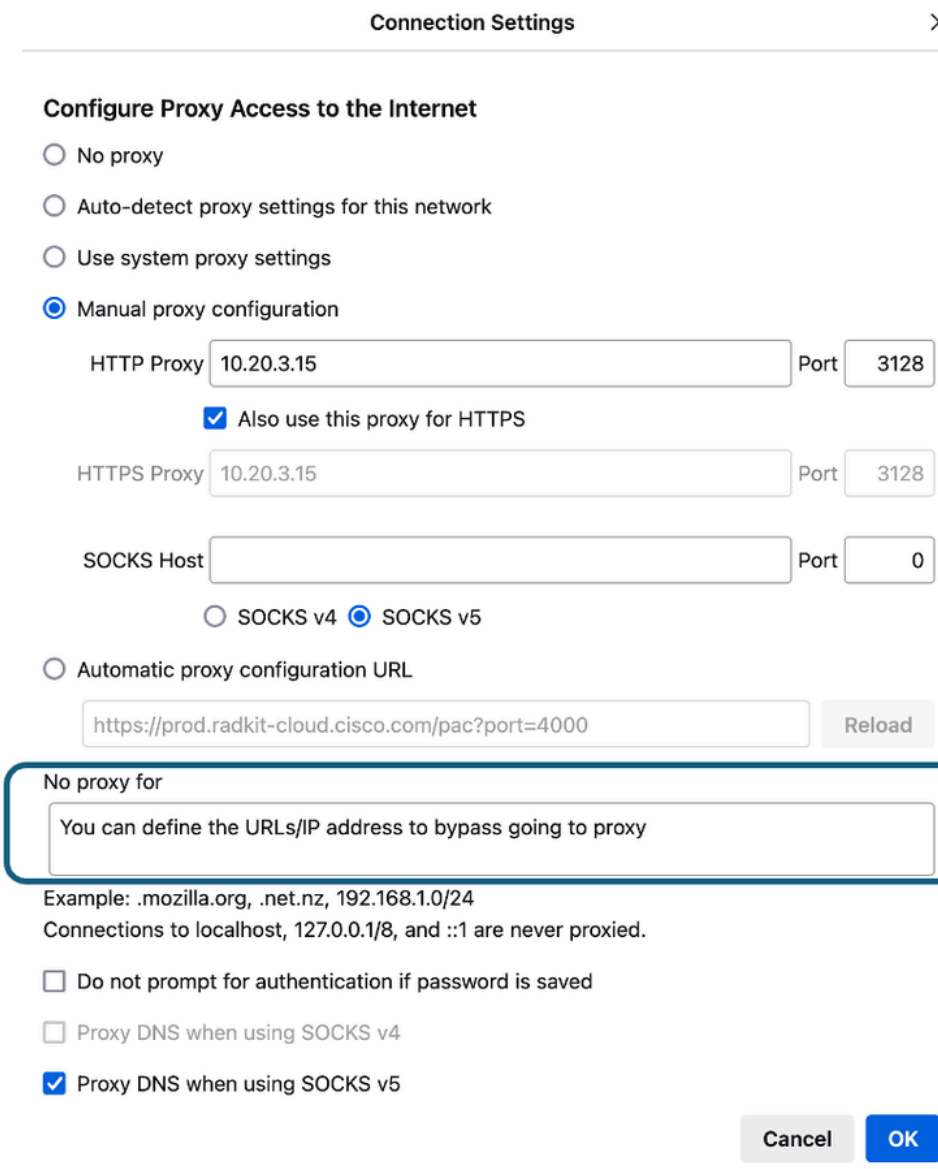
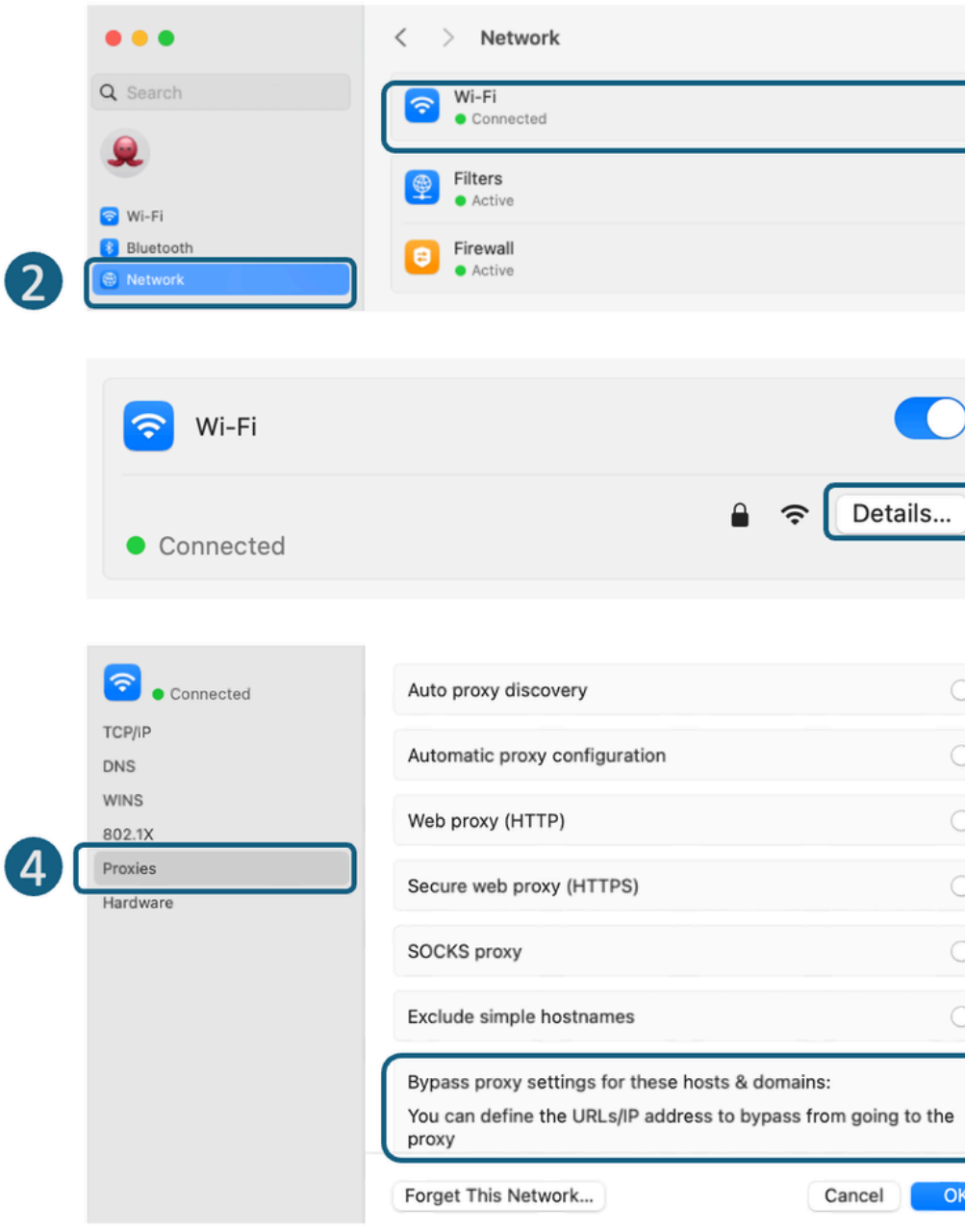


Bild: Definieren der Ausnahmen

Browserkonfiguration (Mozilla FireFox)	Schritt 1. Klicken Sie in der rechten oberen Ecke auf das Menü mit den d Leisten, und wählen Sie Einstellungen. Schritt 2. Geben Sie in die Suchleiste proxy ein. Schritt 3: Definieren Sie Ihre gewünschten URLs im Abschnitt Kein Proxy  Bild - Definieren Sie die Ausnahmen in Fire Fox
Browserkonfiguration (Apple Safari)	Schritt 1. Klicken Sie in der oberen linken Ecke auf das Apple-Symbol, ur Sie Systemeinstellungen aus. Schritt 2: Navigieren Sie im linken Bereich zu Netzwerk, und wählen Sie Netzwerkschnittstelle aus, über die Sie auf das Internet zugreifen.

	Schritt 3. Klicken Sie auf die Details. Schritt 4. Wählen Sie im linken Bereich Proxies aus. Schritt 5. Definieren Sie Ihre gewünschten URLs im Abschnitt Proxy-Eins umgehen.  Bild - Definieren Sie die Ausnahmen in Fire Fox
Gruppenrichtlinienkonfiguration	Je nachdem, wie Sie die Gruppenrichtlinie zum Übertragen der Proxyeins konfiguriert haben, können Sie die Ausnahmeliste definieren.

Datenverkehr bei transparenter Bereitstellung umgehen

In einer transparenten Bereitstellung können Sie den Datenverkehr entweder mithilfe der WCCP-Router- oder der SWA-Umgehungseinstellungen umgehen. Die SWA-Umgehung agiert auf Layer 3 und leitet den Datenverkehr an das Standard-Gateway weiter. Die Appliance wird dabei vollständig umgangen. Die Verarbeitung und Erstellung separater Sitzungen ist somit nicht möglich.

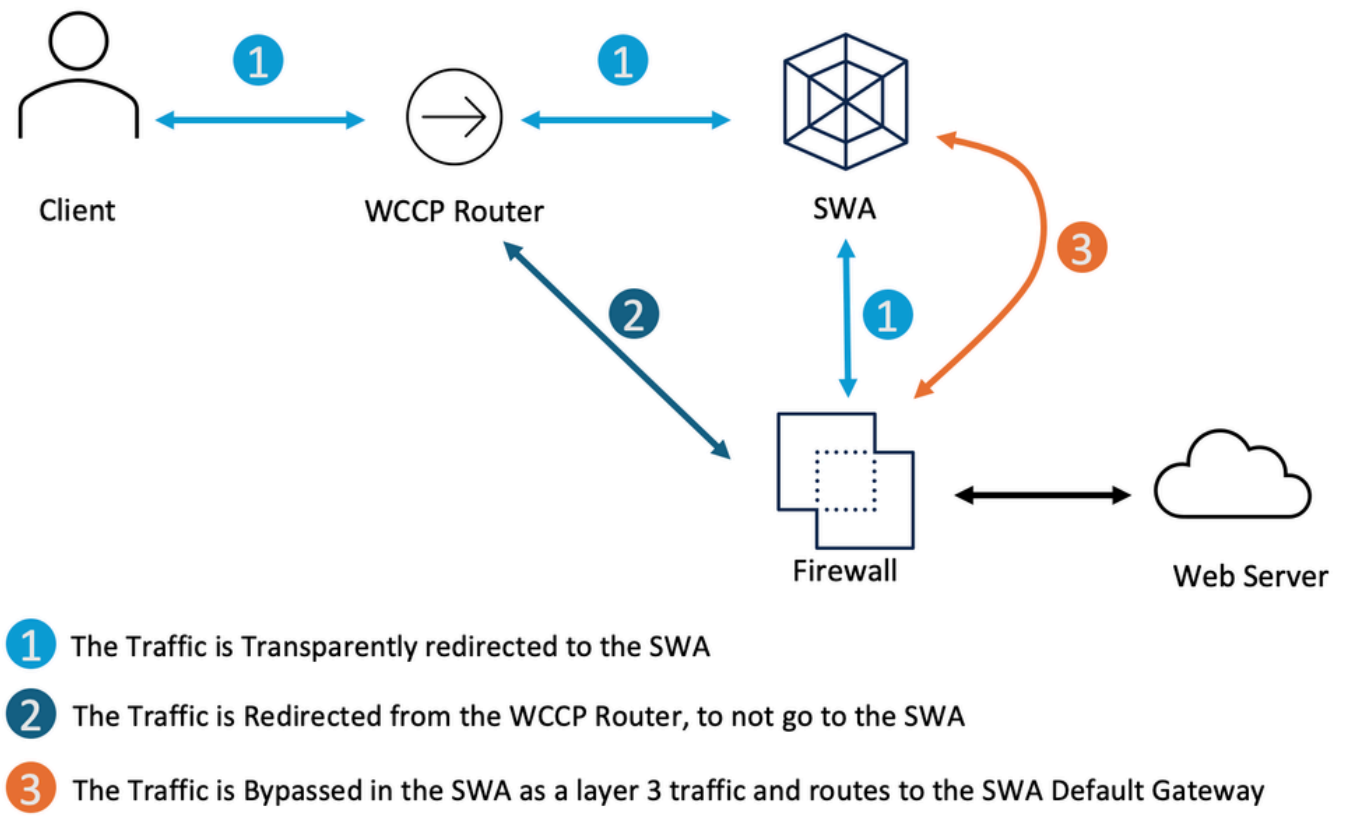
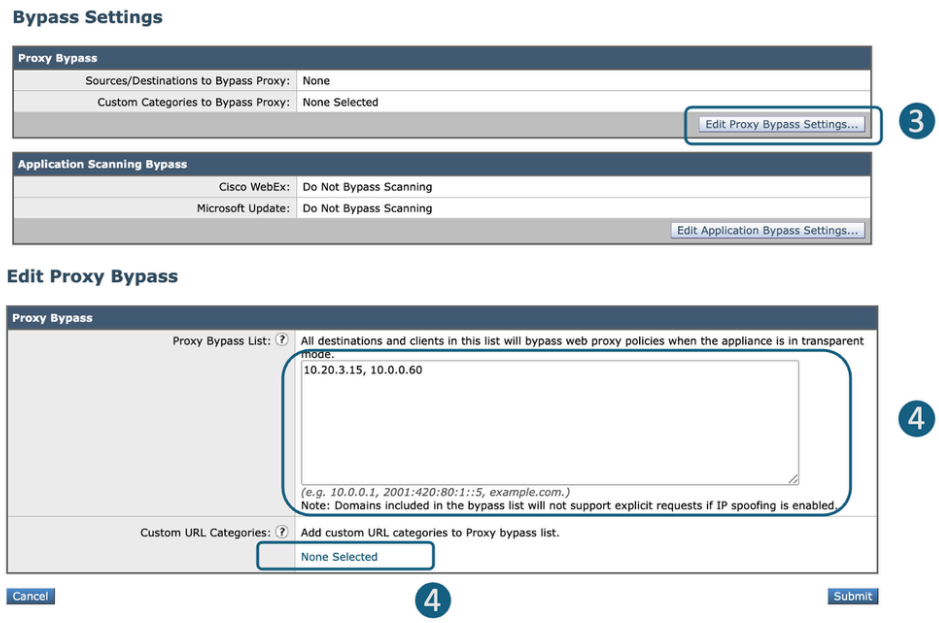


Image - Umgehung des Datenverkehrs bei transparenter Bereitstellung

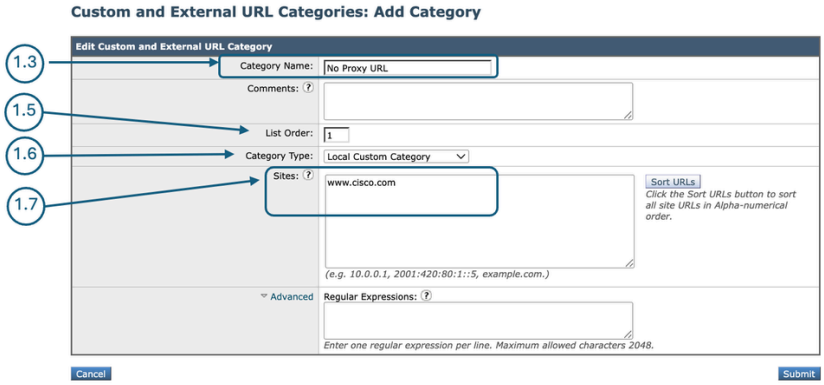
Datenverkehr umgehen Transparente Proxy-Bereitstellung	Schritte zum Umgehen des Datenverkehrs vom SWA
SWA-Umgehungseinstellung	Schritt 1. Wählen Sie in der GUI Web Security Manager aus. Schritt 2: Wählen Sie Bypass Settings aus. Schritt 3: Klicken Sie auf Einstellungen für die Proxyumgehung bearbeiten. Schritt 4. Sie können die URL, die IP-Adresse oder eine benutzerdefinierte URL-Kategorie zur Liste hinzufügen. Schritt 5: Senden und bestätigen Sie die Änderungen.

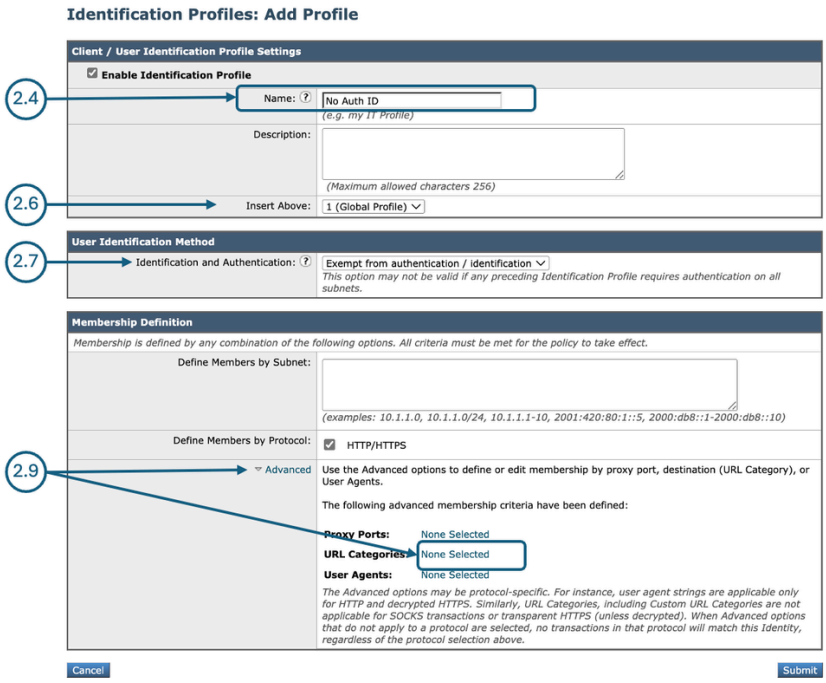
	 Bild - Konfigurieren der Umgehungseinstellungen Tipp: Datenverkehr, der mit diesen Einstellungen umgangen wird, wird nicht in den Zugriffsprotokollen protokolliert und kann in Bypass_Logs angezeigt werden.
Umleitung des Datenverkehrs vom WCCP/PBR-Router	Sie können die Quell- oder Ziel-IP-Adresse in Ihrem WCCP oder richtlinienbasierten Router (Policy Based Router, PBR) so konfigurieren, dass einige Datenströme nicht an den SWA umgeleitet werden.

Konfigurieren von Passthrough und Zulassen von Datenverkehr in SWA

Wenn der Datenverkehr die SWA erreicht und Sie aufgrund der Datenschutzbedenken die Last für die SWA auf reduzieren möchten, dass der Datenverkehr für einige URLs nicht von der SWA überprüft werden soll, gehen Sie wie folgt vor.

Schritte	Schritte
Schritt 1: Erstellen einer benutzerdefinierten URL-Kategorie für die URLs	Schritt 1.1.Wählen Sie aus der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Benutzerdefinierte und externe URL-Kategorien. Schritt 1.2.Klicken Sie aufKategorie hinzufügen,um eine

	benutzerdefinierte URL-Kategorie hinzuzufügen. Schritt 1.3.Zuweisen eines eindeutigen Kategorienamens. Schritt 1.4. (Optional) Beschreibung hinzufügen. Schritt 1.5. Wählen Sie aus der Listenreihenfolge die erste Kategorie für die Positionierung an der Spitze aus. Schritt 1.6. Wählen Sie aus der Dropdown-Liste Kategorie Typ die Option Lokale benutzerdefinierte Kategorie aus. Schritt 1.7. Fügen Sie gewünschte URLs im Abschnitt Sites hinzu. Schritt 1.8: Senden.  Bild - Erstellen einer benutzerdefinierten URL-Kategorie
Schritt 2: Erstellen eines Identifikationsprofils, um den Datenverkehr von der Authentifizierung auszunehmen	Schritt 2.1.Wählen Sie aus der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Identifikationsprofile. Schritt 2.2.Klicken Sie auf Profil hinzufügen, um ein Profil hinzuzufügen. Schritt 2.3.Verwenden Sie das Kontrollkästchen Identifikationsprofil aktivieren, um dieses Profil zu aktivieren oder es schnell zu deaktivieren, ohne es zu löschen. Schritt 2.4.Zuweisen eines eindeutigen profileName. Schritt 2.5. (Optional) Beschreibung hinzufügen. Schritt 2.6.Wählen Sie aus der Dropdown-Liste Einfügen aus, wo dieses Profil in der Tabelle angezeigt werden soll. Schritt 2.7. Wählen Sie im Abschnitt User Identification Methoddie Option Exempt from authentication/identification (Von Authentifizierung/Identifizierung ausnehmen) aus. Schritt 2.8.Lassen Sie dieses Feld im Feld Mitglieder nach Subnetz definieren leer, um alle Client-IP-Adressen einzuschließen, es sei denn, Sie möchten den Datenverkehr

	für eine bestimmte IP-Adresse weiterleiten. Schritt 2.9. Wählen Sie im Abschnitt Erweitert die Option Benutzerdefinierte URL-Kategorien aus.  Bild - Identifikationsprofil hinzufügen Schritt 2.10: Fügen Sie die benutzerdefinierte URL-Kategorie hinzu, die in Schritt 1 erstellt wurde. Schritt 2.11. Klicken Sie auf Fertig. Schritt 2.12: Senden.
Schritt 3: Erstellen einer Entschlüsselungsrichtlinie zum Weiterleiten des Datenverkehrs	Schritt 3.1.Wählen Sie aus der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Entschlüsselungsrichtlinie. Schritt 3.2. Klicken Sie auf Add Policy, um eine Entschlüsselungsrichtlinie hinzuzufügen. Schritt 3.3.Aktivieren Sie die Richtlinie über das Kontrollkästchen Enable Policy (Richtlinie aktivieren). Schritt 3.4: Zuweisen eines eindeutigen PolicyName. Schritt 3.5. (Optional) Beschreibung hinzufügen. Schritt 3.6.Wählen Sie aus der Dropdown-Liste "Insert Above Policyd" (Über Richtlinie einfügen) die erste Richtlinie aus. Schritt 3.7.Wählen Sie aus den Identifikationsprofilen und

Benutzern das Identifikationsprofil aus, das Sie in Schritt 2 erstellt haben.

Schritt 3.8: Senden.

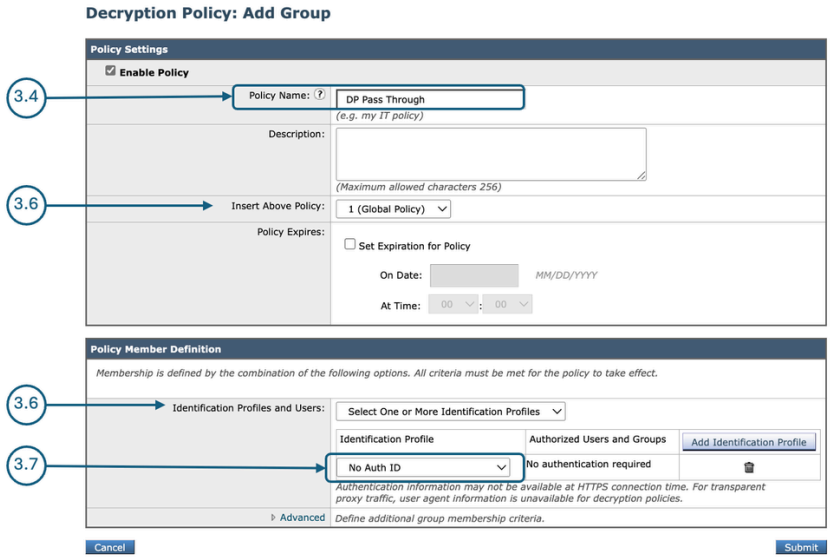


Bild - Entschlüsselungsrichtlinie erstellen

Schritt 3.9.Klicken Sie auf der Seite Entschlüsselungsrichtlinien unter URL-Filterung auf den Link, der dieser neuen Entschlüsselungsrichtlinie zugeordnet ist.

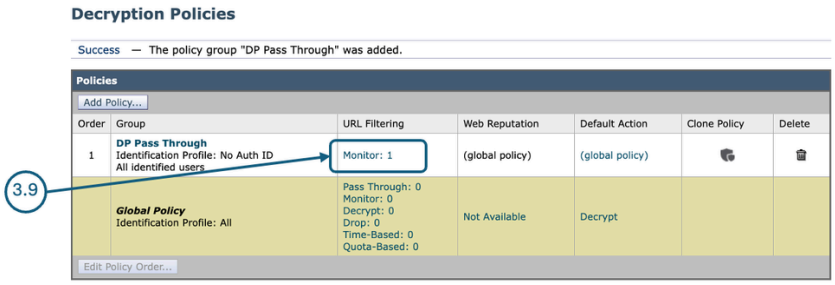


Bild - URL-Filterung auswählen

Schritt 3.10.SelectPassThrough die Aktion für die in Schritt 1 erstellte URL-Kategorie.

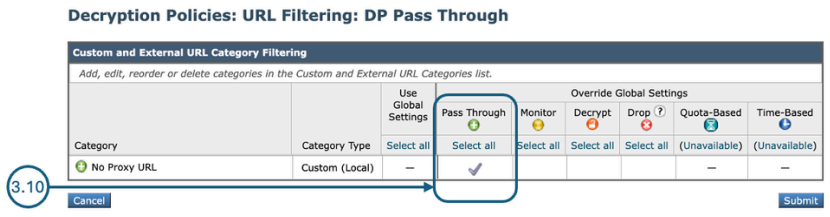
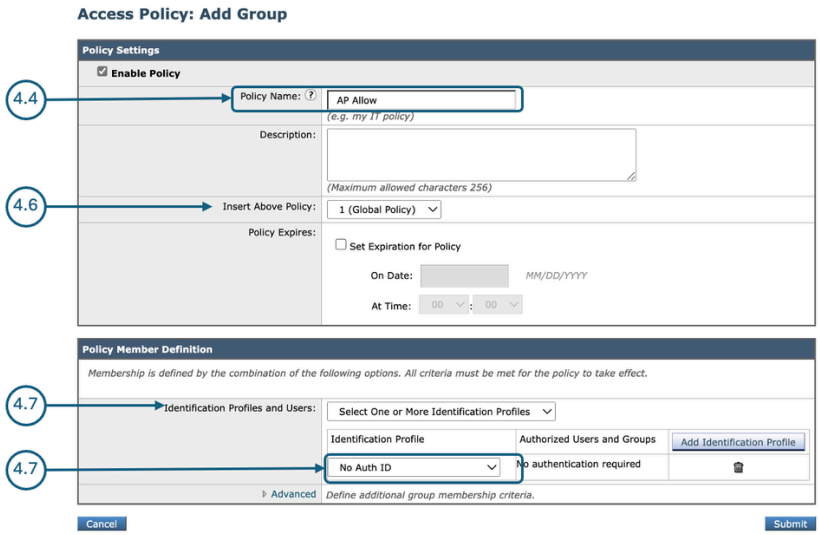


Bild: Festlegen der durchzuführenden Aktion

	Schritt 3.11: Senden.
Schritt 4: Erstellen einer Zugriffsrichtlinie, um Microsoft Updates-Datenverkehr zuzulassen	Schritt 4.1.Wählen Sie in der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Zugriffsrichtlinie. Schritt 4.2. Klicken Sie auf Add Policy, um eine Zugriffsrichtlinie hinzuzufügen. Schritt 4.3.Aktivieren Sie die Richtlinie über das Kontrollkästchen Enable Policy (Richtlinie aktivieren). Schritt 4.4: Zuweisen eines eindeutigen PolicyName. Schritt 4.5. (Optional) Beschreibung hinzufügen. Schritt 4.6.Wählen Sie aus der Dropdown-Liste "Insert Above Policyd" (Über Richtlinie einfügen) die erste Richtlinie aus. Schritt 4.7.Wählen Sie aus den Identifikationsprofilen und Benutzern das Identifikationsprofil aus, das Sie in Schritt 2 erstellt haben. Schritt 4.8: Senden.  Bild: Erstellen einer Zugriffsrichtlinie Schritt 4.9. Klicken Sie auf der Seite Zugriffsrichtlinien unter URL-Filterung auf den Link, der dieser neuen Zugriffsrichtlinie zugeordnet ist.

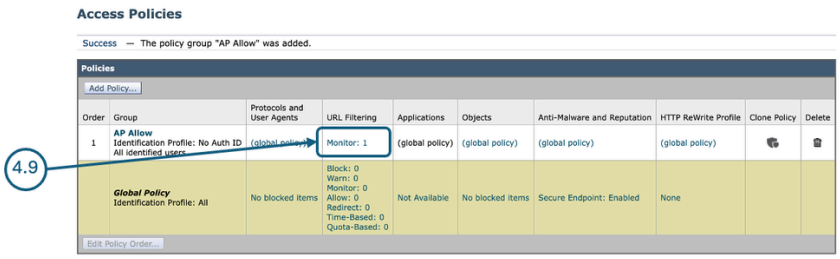


Bild - URL-Filterung auswählen

Schritt 4.10.Wählen Sie die Aktion für die benutzerdefinierte URL-Kategorie aus, die für die in Schritt 1 erstellte URL-Kategorie erstellt wurde.

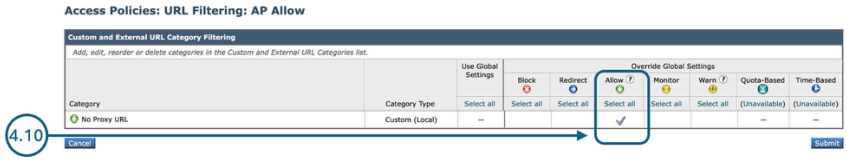


Bild: Festlegen der Aktion auf Zulassen

Schritt 4.11: Senden.

Schritt 4.12: Änderungen bestätigen.

Zugehörige Informationen

- Umgehen des Datenverkehrs von Microsoft Updates in einer sicheren Web-Appliance
- Umgehung der Authentifizierung in einer sicheren Web-Appliance - Cisco
- Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Web Appliance - GD(Allgemeine Bereitstellung) - Endbenutzer für Richtlinienanwendung klassifizieren [Cisco Secure Web Appliance] - Cisco
- Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco
- Wie kann Office 365-Datenverkehr auf der Cisco Web Security Appliance (WSA) von der Authentifizierung und Entschlüsselung ausgenommen werden - Cisco
- Best Practices für sichere Web-Appliances - Cisco
- Blockieren von Datenverkehr in einer sicheren Web-Appliance
- Upload-Verkehr in sicherer Web-Appliance blockieren
- Download ausführbarer Dateien in SWA blockieren

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.