Konfigurieren der sicheren Webappliance zum Zulassen des Gastzugriffs

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Szenario - Überblick

Konfigurationsschritte

- Schritt 1: Identifikationsprofil erstellen
- Schritt 2: (Optional) Erstellen Sie benutzerdefinierte URL-Kategorien für zulässige und gesperrte URLs
- Schritt 3: Entschlüsselungsrichtlinie für verwaltete Geräte erstellen
- Schritt 4: Entschlüsselungsrichtlinie für nicht verwaltete Geräte erstellen
- Schritt 5: Erstellen einer Zugriffsrichtlinie für verwaltete Geräte
- Schritt 6: Erstellen einer Zugriffsrichtlinie für nicht verwaltete Geräte
- Schritt 7: (Optional) Erstellen einer Cisco Datensicherheitsrichtlinie für verwaltete Geräte
- Schritt 8: (Optional) Erstellen einer Cisco Datensicherheitsrichtlinie für nicht verwaltete Geräte
- Schritt 9: Speichern der Änderungen

Zugehörige Informationen

Einleitung

In diesem Dokument werden die Schritte beschrieben, mit denen Benutzer, die das Entschlüsselungszertifikat nicht installiert haben, über die Secure Web Appliance (SWA) auf das Internet zugreifen können.

Voraussetzungen

Anforderungen

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

- Installierte physische oder virtuelle SWA.
- Lizenz aktiviert oder installiert.
- Der Setup-Assistent ist abgeschlossen.
- Administrator-Zugriff 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.

Szenario - Überblick

Dieser Artikel behandelt ein Szenario der Netzwerkzugriffskontrolle innerhalb des Wi-Fi-Subnetzes 10.10.10.0/24. Die Umgebung besteht aus zwei unterschiedlichen Benutzergruppen, die unterschiedliche Sicherheits- und Zugriffsrichtlinien erfordern:

- Verwaltete Geräte: Firmeneigene Laptops, die vollständig authentifiziert sind und auf denen das SWA-Entschlüsselungszertifikat installiert ist Diese Geräte sind vertrauenswürdig und unterliegen in der Regel den Standard-Zugriffsrichtlinien des Unternehmens.
- Nicht verwaltete Geräte/Gastgeräte: Private Laptops und Mobilgeräte ohne Authentifizierung ohne SWA-Entschlüsselungszertifikat

Ziel:
Ziel des Unternehmens ist die Implementierung restriktiver Web-Zugriffsrichtlinien für nicht verwaltete Geräte, die deren Verbindung auf einen bestimmten Teil der zulässigen URLs beschränken und gleichzeitig sicherstellen, dass die Unternehmensressourcen geschützt bleiben.

Anmerkung: Da das Entschlüsselungszertifikat auf den nicht verwalteten Geräten nicht vertrauenswürdig ist, können Sie den HTTPS-Datenverkehr nicht entschlüsseln, und die Aktion muss auf "Pass Through" (Weiterleiten) festgelegt werden.

Konfigurationsschritte

Schritt 1: Erstellen eines Identifikationsprofils	Schritt 1.1: Navigieren Sie in der SWA-GUI zum Web Security Manager, und wählen Sie Identification Profile aus. Schritt 1.2: Klicken Sie auf Identifikationsprofil hinzufügen. Schritt 1.3. Definieren eines Namens für das Profil. Schritt 1.4 (Optional) Definieren Sie die Beschreibung. Schritt 1.5. Wählen Sie Benutzer in Identifizierung und Authentifizierung authentifizieren. Schritt 1.6. Wählen Sie den Active Directory-Bereich

aus Bereich oder Sequenz auswählen.

Schritt 1.7. Wählen Sie unter Select a Scheme (Schema auswählen) die gewünschten Authentifizierungsprotokolle aus.

Tipp: Wählen Sie in der Liste Schema auswählen nicht die Option Standardauthentifizierung aus.

Schritt 1.8. Aktivieren Sie das Kontrollkästchen für Support Guest-Berechtigungen.

Schritt 1.9. (Optional) Abhängig von Ihrem Design können Sie das Surrogat aktivieren, indem Sie dieselben Surrogateinstellungen auf explizite Weiterleitungsanforderungen anwenden.

Vorsicht: Da Sie den Datenverkehr nicht entschlüsseln können, wählen Sie in der transparenten Bereitstellung nicht Persistent Cookie oder Session Cookie.

Schritt 1.10. Definieren Sie das Subnetz der IP-Adresse in, definieren Sie Mitglieder nach Subnetz.

Schritt 1.11: Senden und bestätigen Sie die Änderungen.

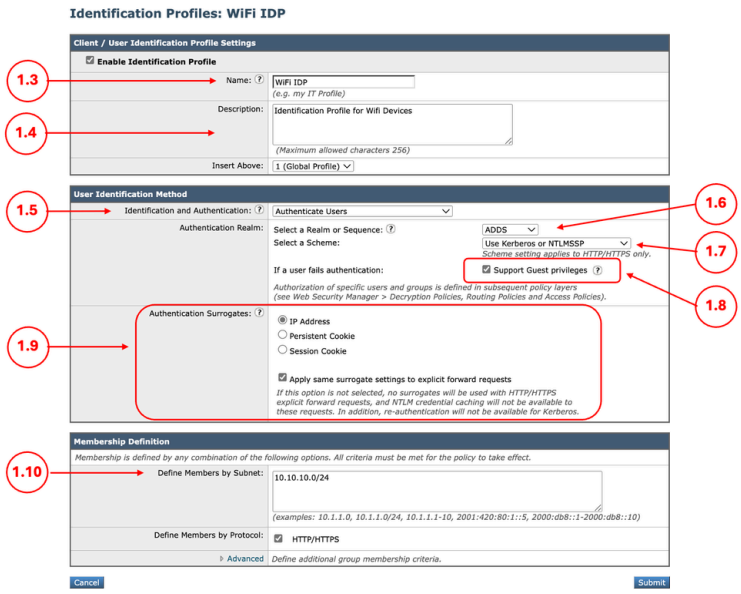
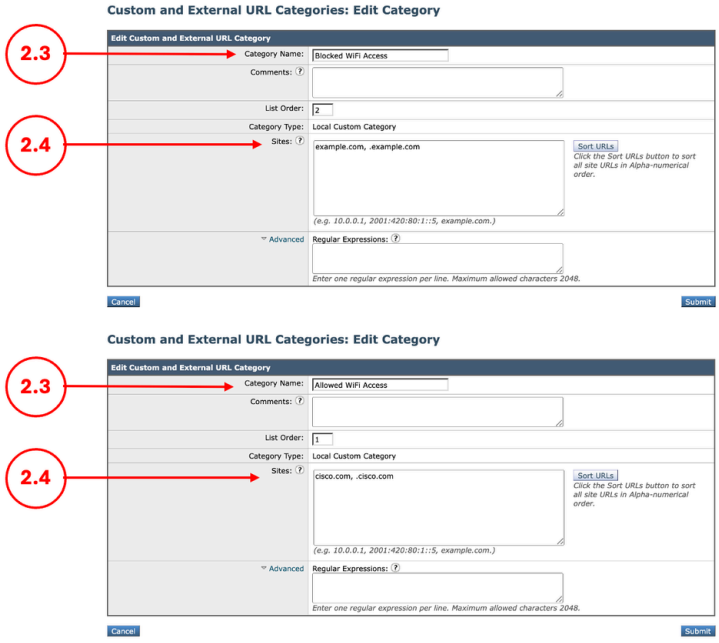


Bild - Identifikationsprofil definieren

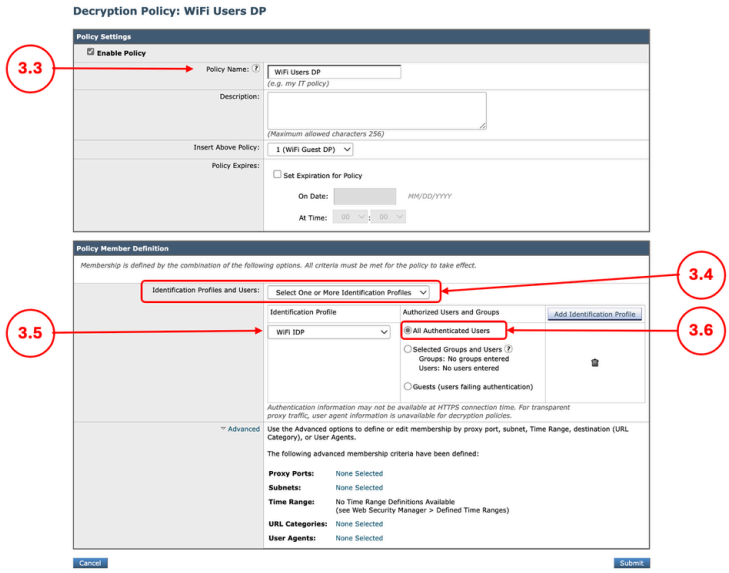
Schritt 2: (Optional) Erstellen Sie benutzerdefinierte URL-Kategorien für zulässige und gesperrte URLs	Schritt 2.1.Navigieren Sie in der GUI zuWeb Security Manager, und wählen Sie Benutzerdefinierte und externe URL-Kategorien aus. Schritt 2.2.Klicken Sie auf Kategorie hinzufügen, um eine neue benutzerdefinierte URL-Kategorie zu erstellen. Schritt 2.3.EnterName für die neue Kategorie. Schritt 2.4.Definieren Sie die Domain und/oder Subdomains der Websites, die Sie den Zugriff blockieren möchten. Schritt 2.5.Senden Sie die Änderungen. Schritt 2.6. Führen Sie die gleichen Schritte aus, um eine URL-Kategorie für die Website zu erstellen, auf die Sie den Zugriff zulassen.  Bild: Benutzerdefinierte URL-Kategorie definieren
Schritt 3: Entschlüsselungsrichtlinie für verwaltete Geräte erstellen	Schritt 3.1. Navigieren Sie in der GUI zuWeb Security Manager, und wählen Sie Entschlüsselungsrichtlinien aus. Schritt 3.2: Klicken Sie auf Richtlinie hinzufügen. Schritt 3.3.EnterName für die neue Richtlinie. Schritt 3.4: Wählen Sie mindestens ein

Identifikationsprofil aus dem Dropdown-Menü Identifikationsprofile und Benutzer aus.

Schritt 3.5.Wählen Sie das in Schritt 1 erstellte Identifikationsprofil aus.

Schritt 3.6. Wählen Sie Alle authentifizierten Benutzer aus.

Schritt 3.7: Klicken Sie auf Senden.



Entschlüsselungsrichtlinie für verwaltete Geräte erstellen

Schritt 3.8. Klicken Sie auf der Seite Entschlüsselungsrichtlinien auf den Link von URL-Filterung für die neue Richtlinie.

Schritt 3.9. (Optional) Sie können jede benutzerdefinierte URL-Kategorie hinzufügen, indem Sie auf Benutzerdefinierte Kategorien auswählen klicken und In Richtlinie einschließen vor den Kategorienamen wählen.

Schritt 3.10: Konfigurieren Sie die Aktion für jede benutzerdefinierte und externe URL-Kategoriefilterung und vordefinierte URL-Kategoriefilterung.

Schritt 3.11: Klicken Sie auf Senden

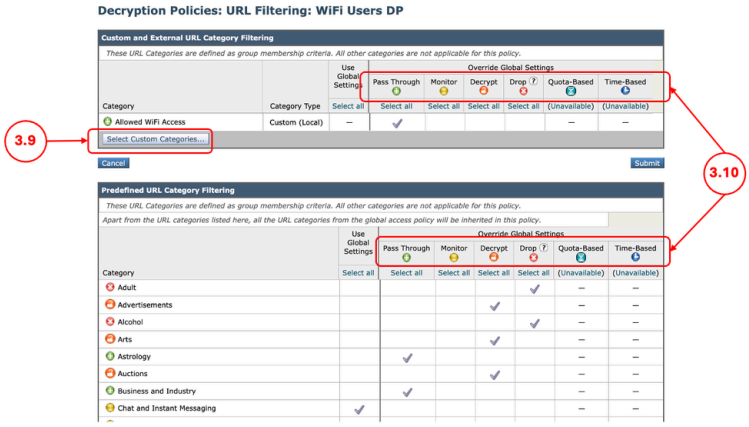


Image: Aktion für Entschlüsselungsrichtlinie konfigurieren

Schritt 4: Entschlüsselungsrichtlinie für nicht verwaltete Geräte erstellen

Schritt 4.1. Navigieren Sie in der GUI zuWeb Security Manager, und wählen Sie Entschlüsselungsrichtlinien aus.

Schritt 4.2: Klicken Sie auf Richtlinie hinzufügen.

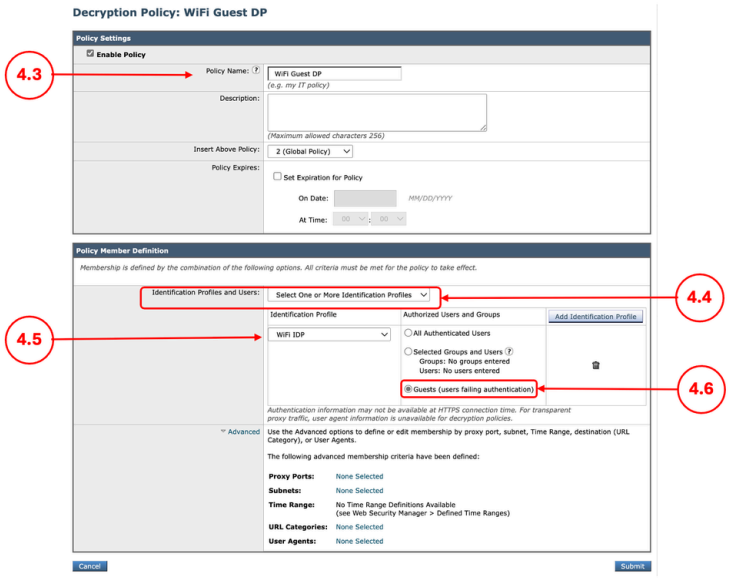
Schritt 4.3.EnterName für die neue Richtlinie.

Schritt 4.4: Wählen Sie mindestens ein Identifikationsprofil aus dem Dropdown-Menü Identifikationsprofile und Benutzer aus.

Schritt 4.5.Wählen Sie das in Schritt 1 erstellte Identifikationsprofil aus.

Schritt 4.6. Wählen Sie Gäste (Benutzer, die nicht authentifiziert werden konnten).

Schritt 4.7: Klicken Sie auf Senden.



Entschlüsselungsrichtlinie für nicht verwaltete Geräte erstellen

Schritt 4.8. Klicken Sie auf der Seite Entschlüsselungsrichtlinien auf den Link von URL-Filterung für die neue Richtlinie.

Schritt 4.9. (Optional) Sie können jede benutzerdefinierte URL-Kategorie hinzufügen, indem Sie auf Benutzerdefinierte Kategorien auswählen klicken und In Richtlinie einschließen vor den Kategorienamen wählen.

Schritt 4.10: Konfigurieren Sie die Aktion für jede benutzerdefinierte und externe URL-Kategoriefilterung und vordefinierte URL-Kategoriefilterung.

Anmerkung: Verwenden Sie nicht Entschlüsseln als Aktion, da das SWA-Entschlüsselungszertifikat auf den nicht verwalteten Geräten nicht vertrauenswürdig ist.

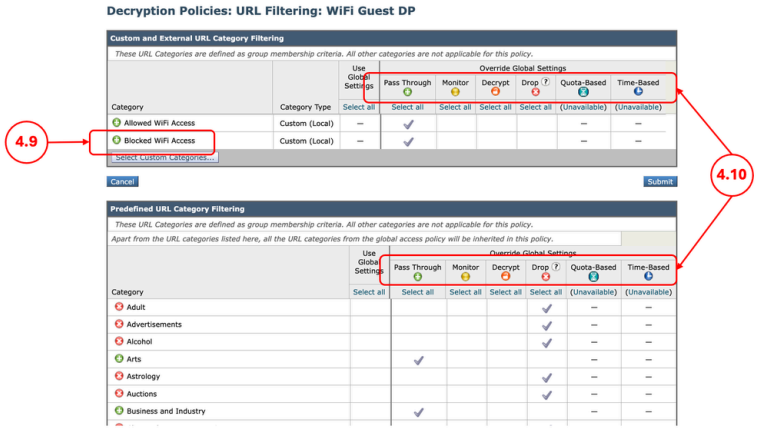
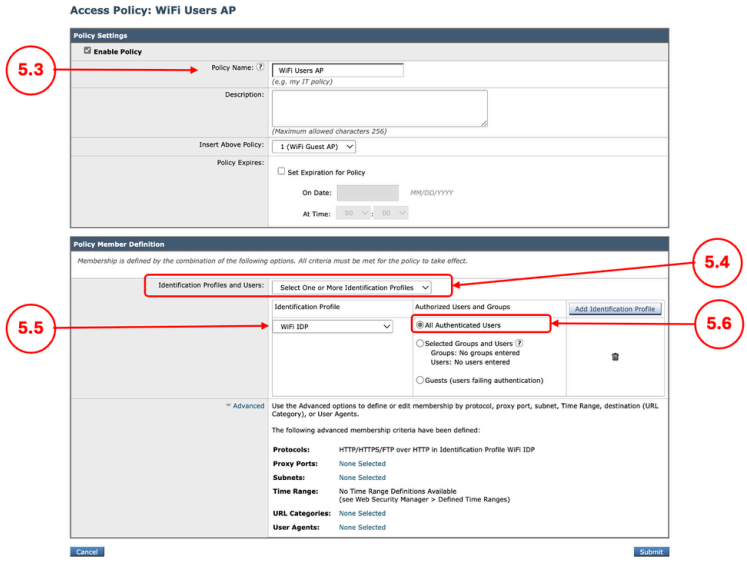


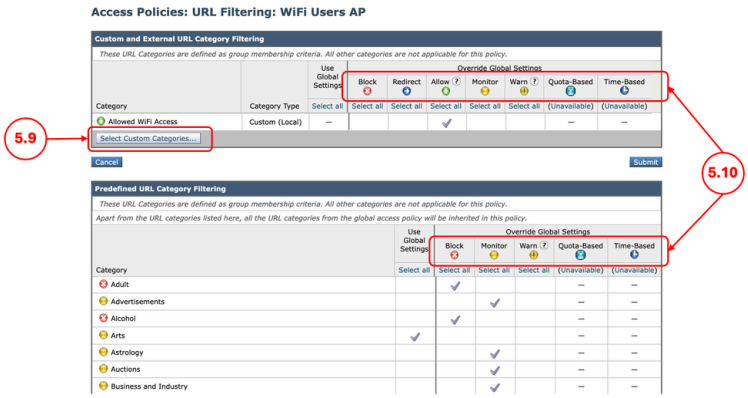
Image - Entschlüsselungsaktion für nicht verwaltete Geräte

Schritt 4.11. Blättern Sie im Abschnitt Nicht kategorisierte URLs nach unten, und wählen Sie die gewünschte Aktion aus.

Bild - Nicht kategorisierte URLs

Tipp: Aus sicherheitstechnischer Sicht ist es am

	besten, die Aktion auf Drop festzulegen. Falls eine URL Zugriff benötigt, können Sie sie in der benutzerdefinierten URL-Kategorie hinzufügen, die der Richtlinie zugewiesen ist. Schritt 4.12: Klicken Sie auf Senden
Schritt 5: Erstellen einer Zugriffsrichtlinie für verwaltete Geräte	Schritt 5.1. Navigieren Sie in der GUI zuWeb Security Manager, und wählen SieZugriffsrichtlinien. Schritt 5.2: Klicken Sie auf Richtlinie hinzufügen. Schritt 5.3.EnterName für die neue Richtlinie. Schritt 5.4: Wählen Sie mindestens ein Identifikationsprofil aus dem Dropdown-Menü Identifikationsprofile und Benutzer aus. Schritt 5.5.Wählen Sie das in Schritt 1 erstellte Identifikationsprofil aus. Schritt 5.6. Wählen Sie Alle authentifizierten Benutzer aus. Schritt 5.7: Klicken Sie auf Senden.  Image - Zugriffsrichtlinie für verwaltete Geräte Schritt 5.8. Klicken Sie auf der Seite Access Policies (Zugriffsrichtlinien) auf den Link von URL Filtering (URL-Filterung) für die neue Richtlinie. Schritt 5.9. (Optional) Sie können jede

	benutzerdefinierte URL-Kategorie hinzufügen, indem Sie auf Benutzerdefinierte Kategorien auswählen klicken und In Richtlinie einschließen vor den Kategorienamen wählen. Schritt 5.10: Konfigurieren Sie die Aktion für jede benutzerdefinierte und externe URL-Kategoriefilterung und vordefinierte URL-Kategoriefilterung.  Bild - URL-Filterung für Zugriffsrichtlinien für verwaltete Geräte Schritt 5.11: Klicken Sie auf Senden.
Schritt 6: Erstellen einer Zugriffsrichtlinie für nicht verwaltete Geräte	Schritt 6.1. Navigieren Sie in der GUI zuWeb Security Manager, und wählen SieZugriffsrichtlinien. Schritt 6.2: Klicken Sie auf Richtlinie hinzufügen. Schritt 6.3.EnterName für die neue Richtlinie. Schritt 6.4: Wählen Sie mindestens ein Identifikationsprofil aus dem Dropdown-Menü Identifikationsprofile und Benutzer aus. Schritt 6.5.Wählen Sie das in Schritt 1 erstellte Identifikationsprofil aus. Schritt 6.6. Wählen Sie Gäste (Benutzer, die nicht authentifiziert werden konnten). Schritt 6.7: Klicken Sie auf Senden.

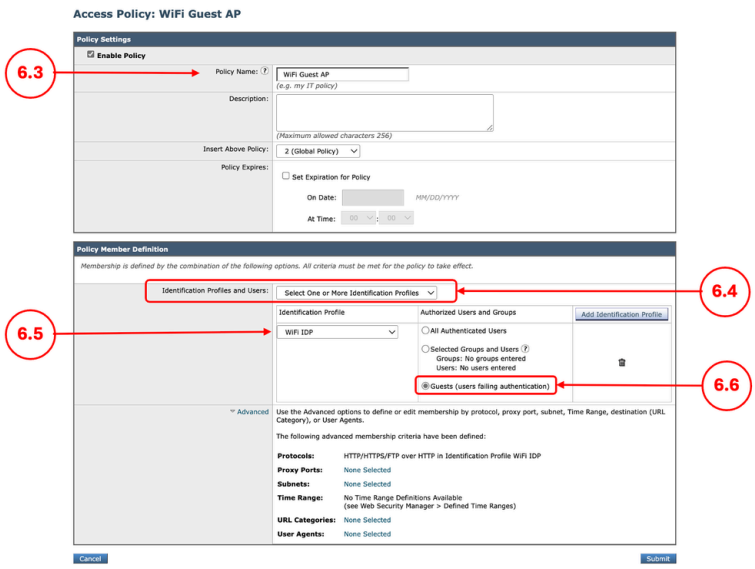


Image - Zugriffsrichtlinie für nicht verwaltete Geräte

Schritt 6.8. Klicken Sie auf der Seite Access Policies (Zugriffsrichtlinien) auf den Link von URL Filtering (URL-Filterung) für die neue Richtlinie.

Schritt 6.9. (Optional) Sie können jede benutzerdefinierte URL-Kategorie hinzufügen, indem Sie auf Benutzerdefinierte Kategorien auswählen klicken und In Richtlinie einschließen vor den Kategorienamen wählen.

Schritt 6.10: Konfigurieren Sie die Aktion für jede benutzerdefinierte und externe URL-Kategoriefilterung und vordefinierte URL-Kategoriefilterung.

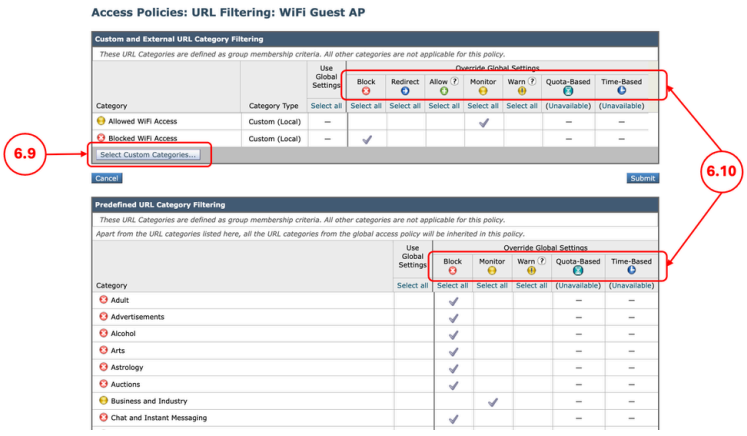


Bild - URL-Filterung für Zugriffsrichtlinien für nicht verwaltete Geräte

Schritt 6.11. Blättern Sie im Abschnitt Nicht kategorisierte URLs nach unten, und wählen Sie die gewünschte Aktion aus.

Bild - Zugriffsrichtlinien Nicht kategorisierte URLs

Tipp: Aus sicherheitstechnischer Sicht ist es am besten, die Aktion auf Blockieren festzulegen. Falls eine URL Zugriff benötigt, können Sie sie der Richtlinie zugewiesenen benutzerdefinierten URL-Kategorie hinzufügen.

Schritt 6.12. Klicken Sie auf Senden

Schritt 7: (Optional) Erstellen einer Cisco Datensicherheitsrichtlinie für verwaltete Geräte

Anmerkung: Wenn Sie den Upload-Datenverkehr nicht nach verwalteten Geräten filtern möchten, können Sie diesen Schritt überspringen.

Schritt 7.1: Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Cisco Data Security.

Schritt 7.2: Klicken Sie auf Richtlinie hinzufügen.

Schritt 7.3.EnterName für die neue Richtlinie.

Schritt 7.4: Wählen Sie mindestens ein Identifikationsprofil aus dem Dropdown-Menü Identifikationsprofile und Benutzer aus.

Schritt 7.5.Wählen Sie das in Schritt 1 erstellte Identifikationsprofil aus.

Schritt 7.6. Wählen Sie Alle authentifizierten Benutzer aus.

Schritt 7.7: Klicken Sie auf Senden.

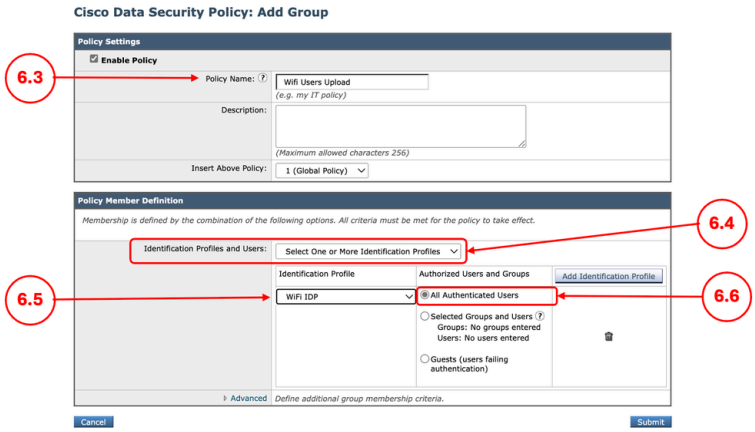


Bild - Cisco Datensicherheitsrichtlinie für verwaltete Geräte

Schritt 7.8: Klicken Sie auf der Seite Cisco Data

	Security Policies (Cisco Datensicherheitsrichtlinien) auf den Link von URL Filtering (URL-Filterung) für die neue Richtlinie. Schritt 7.9. (Optional) Sie können jede benutzerdefinierte URL-Kategorie hinzufügen, indem Sie auf Benutzerdefinierte Kategorien auswählen klicken und In Richtlinie einschließen vor den Kategorienamen wählen. Schritt 7.10: Konfigurieren Sie die Aktion für jede benutzerdefinierte und externe URL-Kategoriefilterung und vordefinierte URL-Kategoriefilterung.  Image - Upload-Aktion für verwaltete Geräte Schritt 7.11: Klicken Sie auf Senden.
Schritt 8: (Optional) Erstellen einer Cisco Datensicherheitsrichtlinie für nicht verwaltete Geräte Anmerkung: Wenn Sie den Upload-Datenverkehr nicht nach nicht verwalteten Geräten filtern möchten, können Sie diesen Schritt überspringen.	Schritt 8.1: Navigieren Sie in der GUI zu Web Security Manager, und wählen Sie Cisco Data Security. Schritt 8.2: Klicken Sie auf Richtlinie hinzufügen. Schritt 8.3.EnterName für die neue Richtlinie. Schritt 8.4: Wählen Sie mindestens ein Identifikationsprofil aus dem Dropdown-Menü Identifikationsprofile und Benutzer aus. Schritt 8.5.Wählen Sie das in Schritt 1 erstellte Identifikationsprofil aus. Schritt 8.6. Wählen Sie Alle authentifizierten Benutzer aus. Schritt 8.7: Klicken Sie auf Senden.

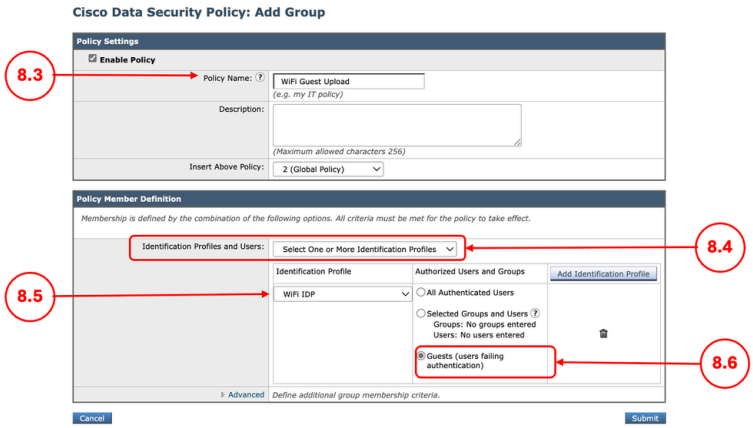


Bild - Cisco Datensicherheitsrichtlinie für nicht verwaltete Geräte

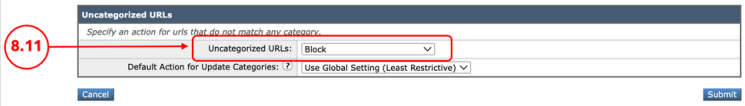
Schritt 8.8: Klicken Sie auf der Seite Cisco Data Security Policies (Cisco Datensicherheitsrichtlinien) auf den Link von URL Filtering (URL-Filterung) für die neue Richtlinie.

Schritt 8.9. (Optional) Sie können jede benutzerdefinierte URL-Kategorie hinzufügen, indem Sie auf Benutzerdefinierte Kategorien auswählen klicken und In Richtlinie einschließen vor den Kategorienamen wählen.

Schritt 8.10: Konfigurieren Sie die Aktion für jede benutzerdefinierte und externe URL-Kategoriefilterung und vordefinierte URL-Kategoriefilterung.

Image - Upload-Aktion für nicht verwaltete Geräte

Schritt 8.11. Blättern Sie im Abschnitt Nicht kategorisierte URLs nach unten, und wählen Sie die gewünschte Aktion aus.

	 Bild - Aktion für nicht kategorisierte URLs hochladen Tipp: Aus sicherheitstechnischer Sicht ist es am besten, die Aktion auf Blockieren festzulegen. Falls eine URL Zugriff benötigt, können Sie sie der Richtlinie zugewiesenen benutzerdefinierten URL-Kategorie hinzufügen. Schritt 8.12: Klicken Sie auf Senden
Schritt 9: Speichern der Änderungen	Schritt 9.1. Bestätigen Sie die Änderungen.

Zugehörige Informationen

- Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Web Appliance - LD (begrenzte Bereitstellung) - Fehlerbehebung...
- Download ausführbarer Dateien in SWA blockieren
- Upload-Verkehr in sicherer Web-Appliance blockieren
- Blockieren von Datenverkehr in einer sicheren Web-Appliance
- Umgehen der Authentifizierung in einer sicheren Web-Appliance
- Konfiguration der Microsoft O365 Tenant-Einschränkung in SWA
- Ersteinrichtung der sicheren Webappliance konfigurieren
- Umgehen des Datenverkehrs von Microsoft Updates in einer sicheren Web-Appliance

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.