Konfiguration einer Bereichsanforderung für Microsoft Update-Datenverkehr in SWA

Inhalt

Einleitung

In diesem Dokument werden die Schritte beschrieben, die ausgeführt werden, damit der Datenverkehr von Microsoft Updates die Bereichsanforderung in einer sicheren Webappliance (SWA) verwenden kann.

Voraussetzungen

Anforderungen

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

- SWA-Verwaltung.

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.

Bereichsanforderung

Eine Bereichsanforderung ist eine Funktion des HTTP-Protokolls, die es einem Client (wie einem Webbrowser oder einem Download-Manager) ermöglicht, nur einen bestimmten Teil einer Datei von einem Server anzufordern, anstatt die gesamte Datei auf einmal herunterzuladen. Dies ist insbesondere für die Wiederaufnahme unterbrochener Downloads, das Streaming von Medien oder den effizienten Zugriff auf große Dateien nützlich. Der Client gibt den gewünschten Bytebereich im Range-Header der HTTP-Anforderung an, und der Server antwortet mit einem 206-Statuscode für partiellen Inhalt, wenn er Bereichsanforderungen unterstützt und nur das angeforderte Segment der Datei bereitstellt.

Dieser Mechanismus verbessert die Leistung und das Anwendererlebnis in mehreren Szenarien. Beim Video-Streaming beispielsweise ermöglichen Bereichsanforderungen den Playern, nur die Segmente abzurufen, die für die Wiedergabe benötigt werden. Dadurch wird die Bandbreitennutzung reduziert und die Reaktionsfähigkeit verbessert. Ebenso verwenden Download-Manager Range-Anfragen, um eine Datei in Blöcke aufzuteilen und parallel herunterzuladen, wodurch der Prozess beschleunigt wird. Range-Anfragen spielen auch eine Schlüsselrolle bei Caching- und Proxy-Systemen, da sie teilweise Updates ermöglichen und redundante Datenübertragungen reduzieren.

Bereichsanforderung in der Proxyumgebung

In einer Proxy-Umgebung spielen Range Requests eine entscheidende Rolle bei der Optimierung der Bandbreitennutzung und der Verbesserung der Effizienz bei der Bereitstellung von Inhalten. Wenn Bereichsanforderungen aktiviert sind, kann der Proxyserver nur die erforderlichen Byte-Segmente vom Ursprungsserver abrufen und sie lokal zwischenspeichern. Dadurch können Clients einen Teil des Inhalts anfordern, z. B. bestimmte Segmente eines Videos oder eine große Datei, und diesen schnell aus dem Proxy-Cache erhalten, falls verfügbar. Sie ermöglicht auch parallele Downloads und Wiederaufnahmefunktionen, die besonders in Umgebungen mit begrenzter Bandbreite oder hoher Latenz von Vorteil sind.

Wenn Bereichsanforderungen jedoch deaktiviert sind, muss der Proxy die gesamte Datei vom Ursprungsserver abrufen, auch wenn der Client nur einen kleinen Teil benötigt. Dies führt zu unnötigem Datentransfer, erhöhter Auslastung sowohl der Proxy- als auch der Ursprungsserver sowie langsameren Reaktionszeiten für Clients. Außerdem werden effiziente Caching-Strategien verhindert, da der Proxy keinen Teil des Inhalts speichern oder bereitstellen kann. In Streaming-Szenarien kann dies zu Pufferverzögerungen oder einer Beeinträchtigung der

Benutzerfreundlichkeit führen. Die Deaktivierung von Bereichsanfragen kann aus Sicherheits- oder Richtliniengründen erfolgen, geht jedoch oft zulasten von Leistung und Flexibilität.

Stellen Sie sich beispielsweise ein Szenario vor, in dem 10 Benutzer versuchen, jeweils 1 MB von einer 100-MB-Datei über einen Proxyserver herunterzuladen.

Bereichsanforderungen deaktiviert:

Wenn Bereichsanforderungen deaktiviert sind, kann der Proxy nicht nur das 1-MB-Segment abrufen, das jeder Benutzer benötigt. Stattdessen muss die gesamte 100-MB-Datei für jede Anforderung vom Ursprungsserver heruntergeladen werden. Daraus ergeben sich:

Gesamtdatenverkehr vom Ursprung zum Proxy: 10 × 100 MB = 1.000 MB (1 GB)

Nur 10 MB dieser Daten werden tatsächlich von den Clients verwendet.

Die verbleibenden 990 MB werden verschwendet, was zu einer ineffizienten Bandbreitennutzung und einer höheren Auslastung der Proxy- und Ursprungsserver führt.

Aktivierte Bereichsanforderungen:

Bei aktivierten Bereichsanforderungen ruft der Proxy nur die angeforderte Größe von 1 MB pro Benutzer ab:

Gesamtdatenverkehr vom Ursprung zum Proxy: 10 × 1 MB = 10 MB

Der Proxy kann diese Segmente zwischenspeichern und bei Bedarf an andere Benutzer weitergeben.

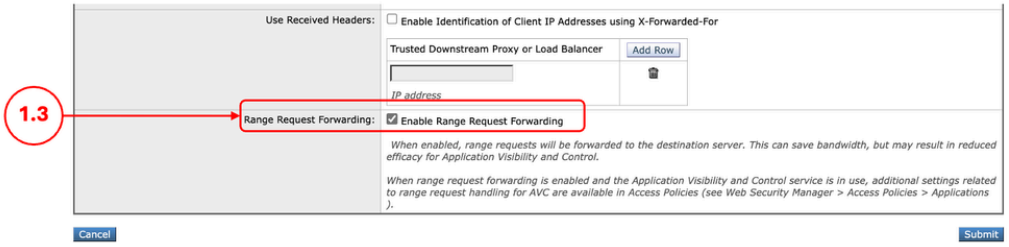
Das Ergebnis: 90 Mal weniger Datenverkehr, schnellere Reaktionszeiten und eine deutlich bessere Ressourcenauslastung.

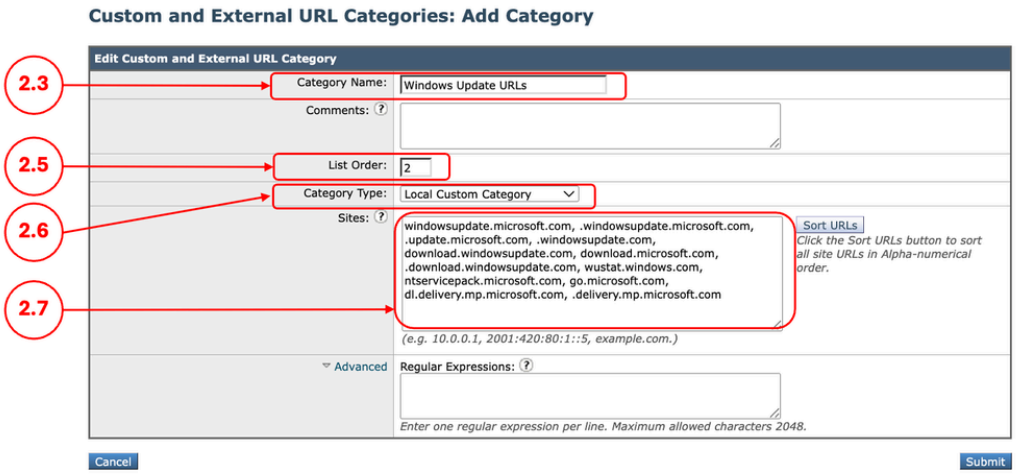
Aktivieren der Bereichsanforderung für Microsoft Updates

Obwohl Range Requests die Performance steigern, behindern sie das Scannen von Sicherheitsdaten und die Durchsetzung von Richtlinien in SWA-Umgebungen, da diese Systeme nicht in der Lage sind, partielle Inhalte vollständig zu überprüfen. In diesem Artikel wird die Verwendung von Bereichsanforderungen ausschließlich auf den Datenverkehr von Microsoft Update beschränkt.

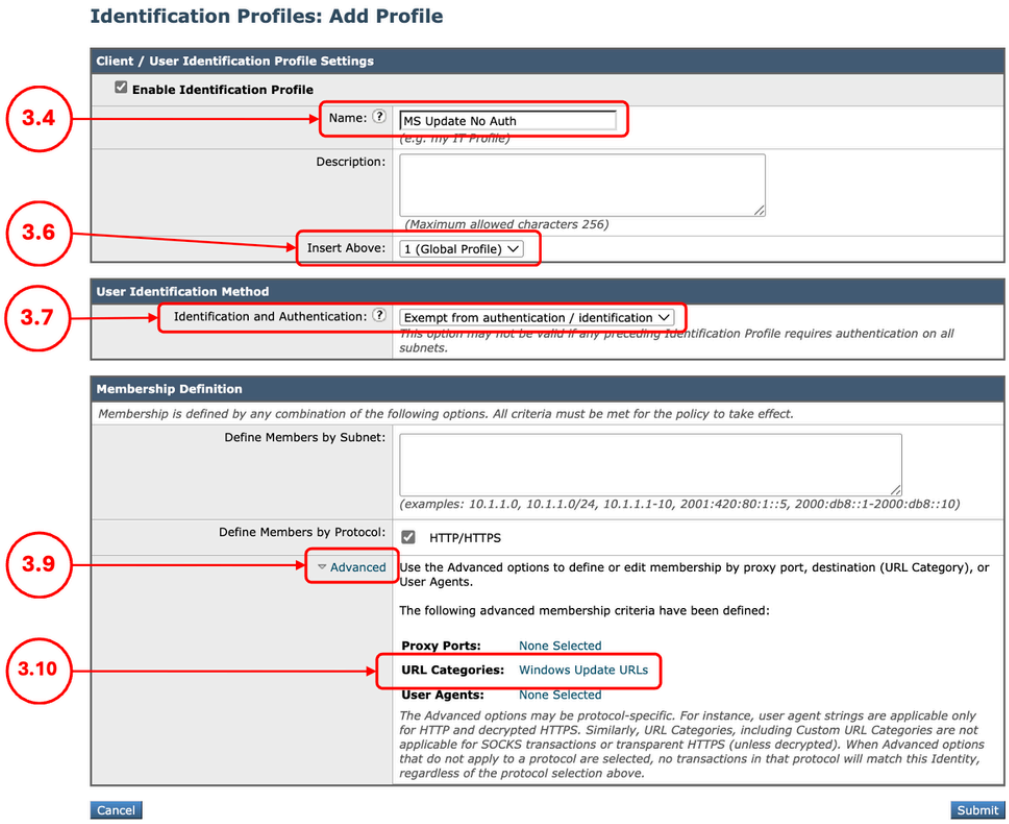
⚠ Vorsicht: Die Aktivierung der Weiterleitung von Bereichsanfragen kann die richtlinienbasierte AVC-Effizienz (Application Visibility and Control) beeinträchtigen und die Sicherheit beeinträchtigen.

Schritte zum Aktivieren der Bereichsanforderung nur für Microsoft Updates

Schritt 1: Aktivieren Sie die Bereichsanforderung	Schritt 1.1. Klicken Sie in der GUI auf Sicherheitsdienste, und wählen Sie Webproxy aus. Schritt 1.2: Klicken Sie auf Einstellungen bearbeiten. Schritt 1.3. Aktivieren Sie das Kontrollkästchen Enable Range Request Forwarding. Schritt 1.4: Klicken Sie auf Senden.  Bild - Bereichsanforderungsweiterleitung aktivieren
Schritt 2: Erstellen einer benutzerdefinierten URL-Kategorie für Microsoft Updates-URLs	Schritt 2.1.Wählen Sie aus der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Benutzerdefinierte und externe URL-Kategorien. Schritt 2.2.Klicken Sie aufKategorie hinzufügen,um eine benutzerdefinierte URL-Kategorie hinzuzufügen. Schritt 2.3.Zuweisen eines eindeutigen Kategorienamens. Schritt 2.4. (Optional) Beschreibung hinzufügen. Schritt 2.5. Wählen Sie aus der Listenreihenfolge die erste Kategorie für die Positionierung am oberen Rand aus. Schritt 2.6. Wählen Sie aus der Dropdown-Liste Kategorie Typ die Option Lokale benutzerdefinierte Kategorie aus. Schritt 2.7. Fügen Sie im Abschnitt Sites Microsoft Updates-URLs hinzu. Tipp: Über diesen Link können Sie die Liste der Microsoft-Updates überprüfen: Schritt 2 - WSUS konfigurieren | Microsoft - Lernen Vorsicht: Kopieren/Einfügen der URLs wie in Microsoft-Dokumenten; Formatieren Sie sie richtig als SWA-Format. Weitere Informationen finden Sie unter: Benutzerdefinierte URL-Kategorien in Secure Web Appliance konfigurieren - Cisco

	Hier ein Beispiel:
	
	`http://windowsupdate.microsoft.com ===> windowsupdate.microsoft.com`
	`http://*.windowsupdate.microsoft.com ===> .windowsupdate.microsoft.com`
	
	Schritt 2.8: Klicken Sie auf Senden.
	
	 
	Bild - Erstellen einer benutzerdefinierten URL-Kategorie

Schritt 3. (Optional) Erstellen Sie ein Identifizierungsprofil, um den Datenverkehr von Microsoft Updates von der Authentifizierung auszunehmen Anmerkung: Mit dieser Aktion wird die Authentifizierungslast für den Datenverkehr zu Microsoft Updates auf dem SWA reduziert.	Schritt 3.1.Wählen Sie aus der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Identifikationsprofile. Schritt 3.2.Klicken Sie auf Profil hinzufügen, um ein Profil hinzuzufügen. Schritt 3.3.Stellen Sie sicher, dass das Kontrollkästchen Identifikationsprofil aktivieren aktiviert ist. Schritt 3.4.Zuweisen eines eindeutigen profileName. Schritt 3.5. (Optional) Beschreibung hinzufügen. Schritt 3.6.Wählen Sie aus der Dropdown-Liste Einfügen aus, wo dieses Profil in der Tabelle angezeigt werden soll. Schritt 3.7. Wählen Sie im Abschnitt User Identification Methoddie Option Exempt from authentication/identification (Von Authentifizierung/Identifizierung ausnehmen) aus. Schritt 3.8.Geben Sie im Feld Member nach Subnetz definieren, wenn Sie den Microsoft-Datenverkehr für bestimmte Benutzer passieren möchten, die entsprechenden IP-Adressen oder Subnetze ein, oder lassen Sie dieses Feld leer, um alle IP-Adressen einzuschließen. Schritt 3.9. Wählen Sie im Abschnitt Erweitert die Option Benutzerdefinierte URL-Kategorien aus. Schritt 3.10. Fügen Sie die benutzerdefinierte URL-Kategorie hinzu, die

	für Microsoft-Updates erstellt wurde. Schritt 3.11. Klicken Sie auf Fertig. Schritt 3.12. Klicken Sie auf Senden.  Bild - Identifikationsprofil erstellen
Schritt 4: (Optional) Erstellen Sie eine Entschlüsselungsrichtlinie, um den Datenverkehr von Microsoft Updates weiterzuleiten. Anmerkung: Microsoft Updates verwendet HTTP, und der HTTPS-Datenverkehr dient zum Push der Updates-Links. Mit dieser Aktion wird die Entschlüsselungslast für die SWA verringert.	Schritt 4.1.Wählen Sie aus der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Entschlüsselungsrichtlinie. Schritt 4.2. Klicken Sie auf Add Policy, um eine Entschlüsselungsrichtlinie hinzuzufügen. Schritt 4.3: Zuweisen eines eindeutigen PolicyName. Schritt 4.4. (Optional) Beschreibung hinzufügen. Schritt 4.5.Wählen Sie aus der Dropdown-Liste Insert Above Policydie erste Richtlinie aus. Schritt 4.6.Wählen Sie unterIdentifikationsprofile und Benutzer die Option Wählen Sie ein oder mehrere Identifikationsprofile aus. Schritt 4.7: Wählen Sie das Identifikationsprofil, das Sie in Schritt 3 erstellt haben, und fahren Sie mit Schritt 4.11 fort. Schritt 4.8. Wenn Sie kein ID-Profil für Windows Updates erstellt haben, wählen Sie im Abschnitt Erweitert die Option Benutzerdefinierte URL-

Kategorien aus.

Schritt 4.9. Fügen Sie die benutzerdefinierte URL-Kategorie hinzu, die in Schritt 2 für Microsoft-Updates erstellt wurde.

Schritt 4.10. Klicken Sie auf Fertig.

Schritt 4.11: Klicken Sie auf Senden.

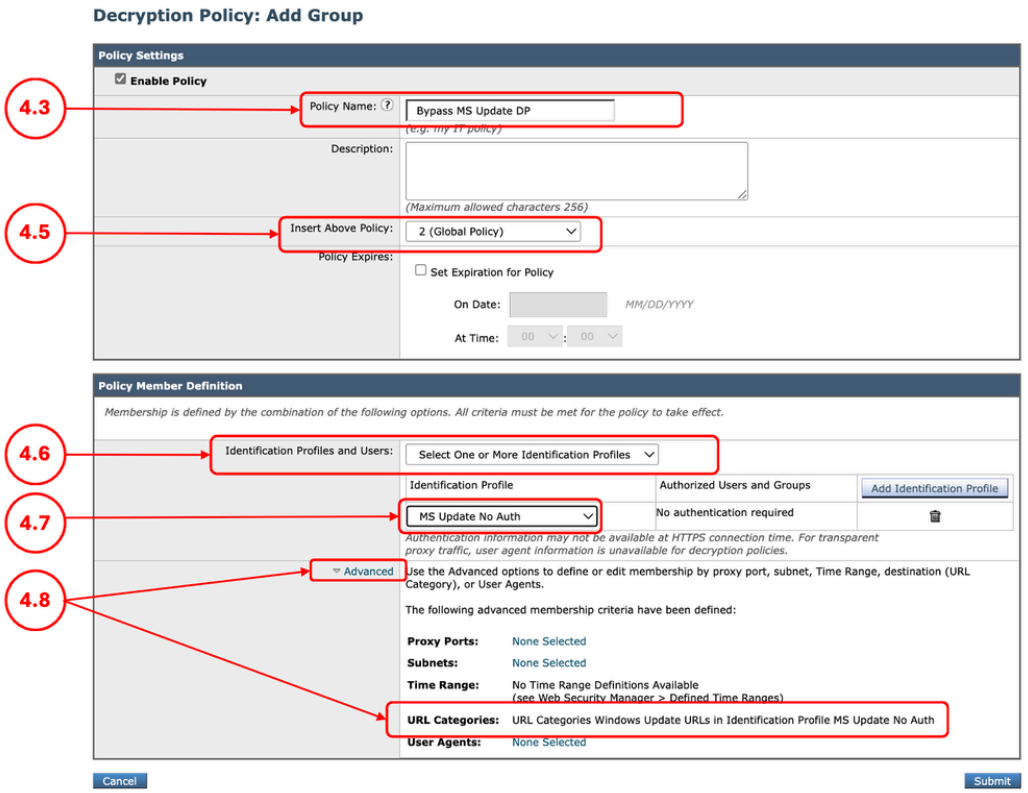
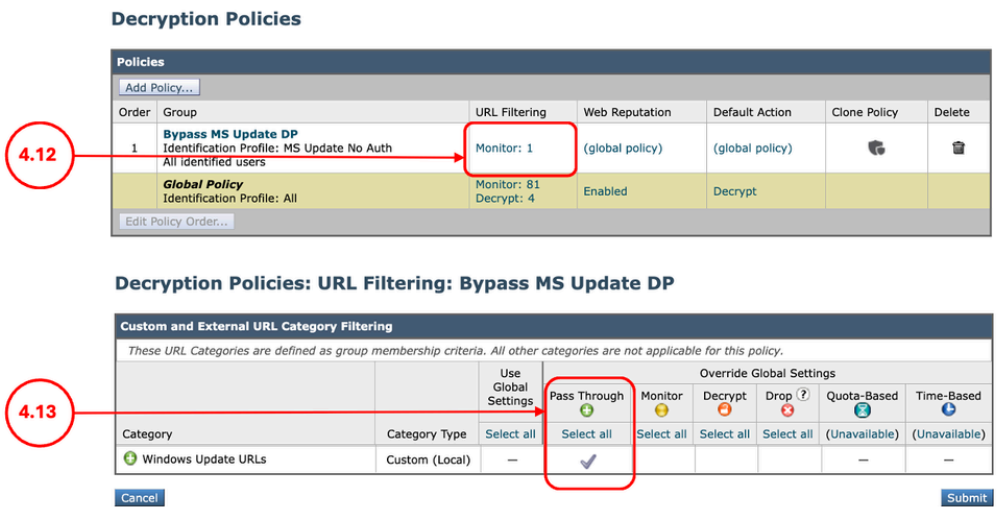


Bild - Entschlüsselungsrichtlinie erstellen

Schritt 4.12.Klicken Sie auf der Seite Entschlüsselungsrichtlinien unter URL-Filterung auf den Link, der dieser neuen Entschlüsselungsrichtlinie zugeordnet ist.

Schritt 4.13.SelectPassThrough die Aktion für die URL-Kategorie von Microsoft Updates.

	 Bild: Festlegen des Action-Passthrough für die URL-Kategorie Schritt 4.12. Klicken Sie auf Senden.
Schritt 5: Erstellen einer Zugriffsrichtlinie zum Zulassen von Bereichsanforderungen für Microsoft Updates-Datenverkehr	Schritt 5.1.Klicken Sie in der GUI aufWebsicherheits-Manager und wählen SieZugriffsrichtlinie. Schritt 5.2. Klicken Sie auf Add Policy, um eine Zugriffsrichtlinie hinzuzufügen. Schritt 5.3: Zuweisen eines eindeutigen PolicyName. Schritt 5.4: (optional) Beschreibung hinzufügen. Schritt 5.5.Wählen Sie aus der Dropdown-Liste "Insert Above Policydie erste Policy" (Richtlinie einfügen) aus. Schritt 5.6.Wählen Sie unterIdentifikationsprofile und Benutzer die Option Wählen Sie ein oder mehrere Identifikationsprofile aus. Schritt 5.7: Wählen Sie das Identifikationsprofil, das Sie in Schritt 3 erstellt haben, und fahren Sie mit Schritt 5.11 fort. Schritt 5.8. Wenn Sie kein ID-Profil für Windows Updates erstellt haben, wählen Sie im Abschnitt Erweitert die Option Benutzerdefinierte URL-Kategorien aus. Schritt 5.9. Fügen Sie die benutzerdefinierte URL-Kategorie hinzu, die in Schritt 2 für Microsoft-Updates erstellt wurde. Schritt 5.10. Klicken Sie auf Fertig. Schritt 5.11: Senden.

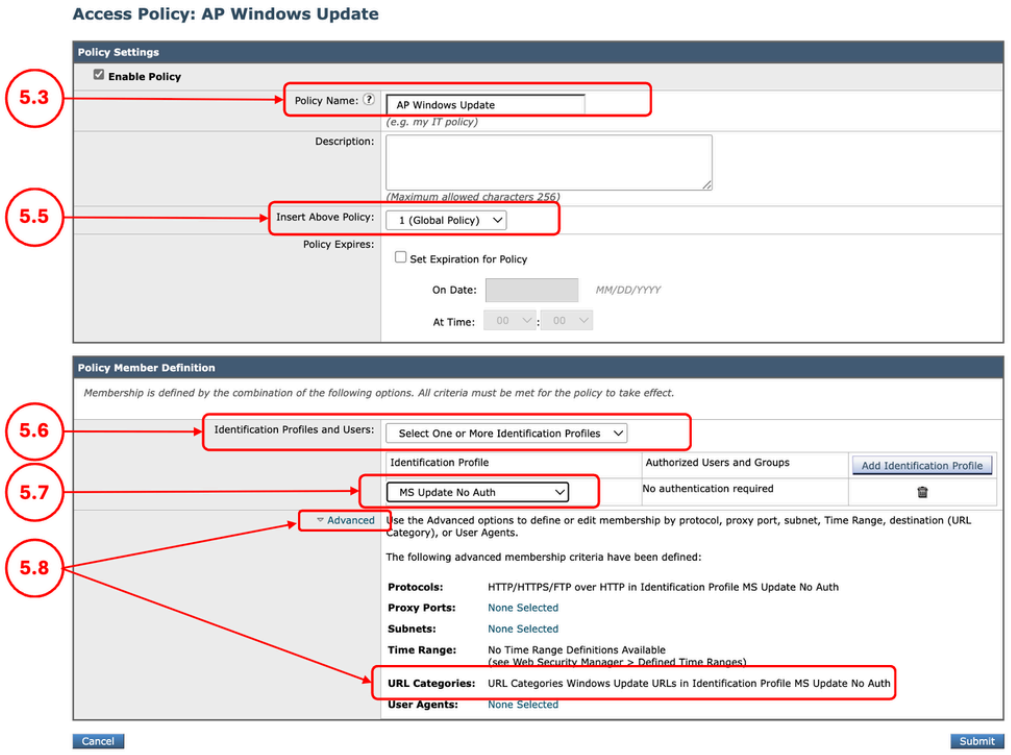


Bild - Erstellen der Zugriffsrichtlinie

Schritt 5.12. Klicken Sie auf der Seite Zugriffsrichtlinien unter URL-Filterung auf den Link, der dieser neuen Zugriffsrichtlinie zugeordnet ist.

Schritt 5.13.Wählen Sie Zulassen als Aktion für die benutzerdefinierte URL-Kategorie aus, die für Microsoft Updates erstellt wurde.

Schritt 5.14: Klicken Sie auf Senden.

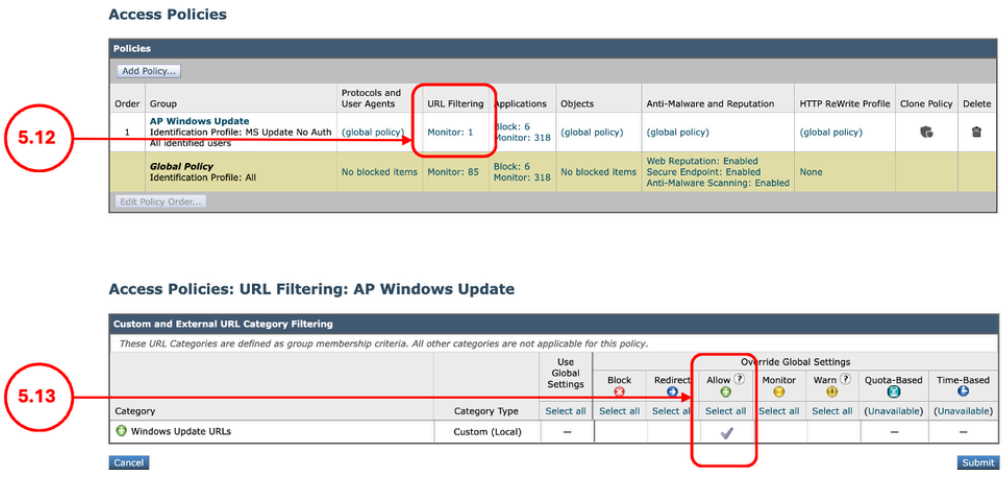


Bild: Festlegen der Aktion Zulassen für die URL-Kategorie

Schritt 5.15. Klicken Sie auf der Seite Zugriffsrichtlinien unter Anwendungen auf den Link, der dieser neuen Zugriffsrichtlinie zugeordnet ist.

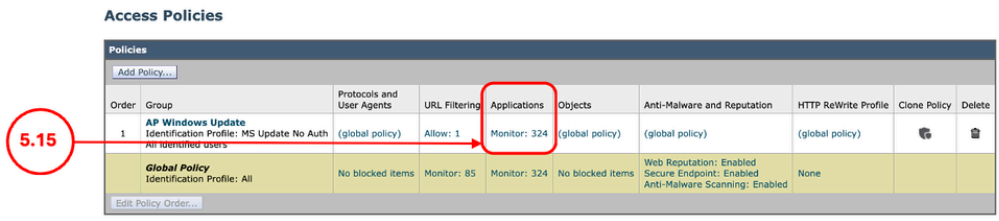


Bild - Anwendungstransparenz und -kontrolle bearbeiten

Schritt 5.16. Wählen Sie unter Anwendungseinstellungen bearbeiten im Abschnitt Benutzerdefinierte Anwendungseinstellungen definieren aus.

Schritt 5.17: Klicken Sie im Abschnitt Anwendungseinstellungen auf Alle bearbeiten für die Anwendung Spiele, und legen Sie die Aktion auf Blockieren fest.

Schritt 5.18. Klicken Sie auf Anwenden.

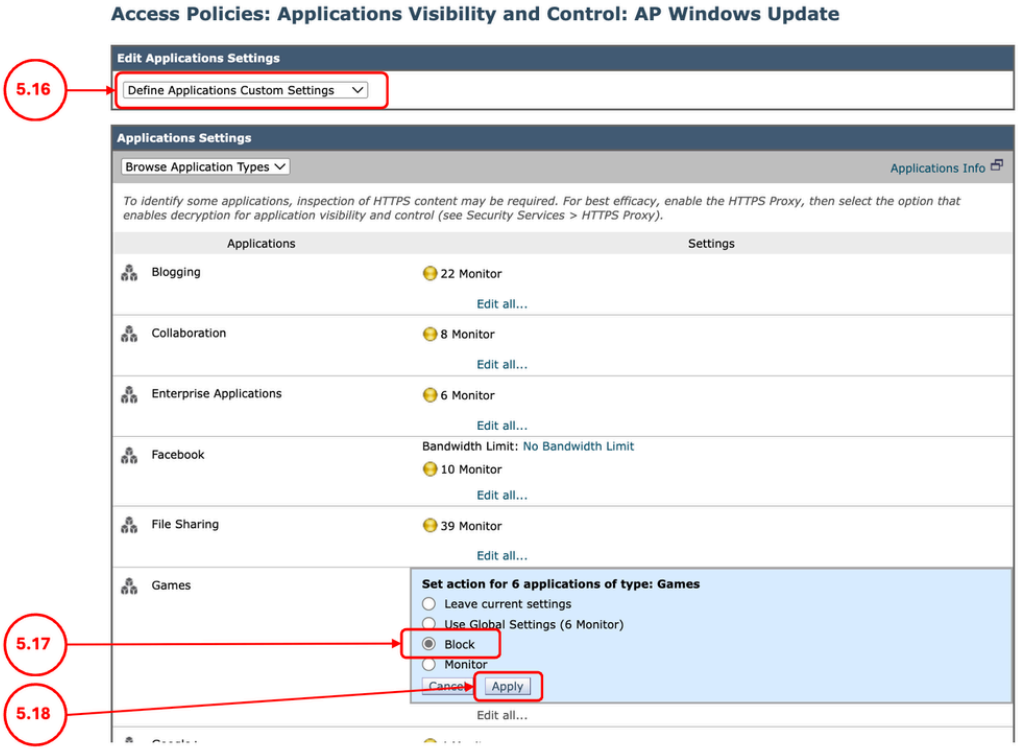


Bild: Eine zu blockierende Anwendungsaktion festlegen

Schritt 5.19. Blättern Sie nach unten zum Abschnitt Bereichsanforderungseinstellungen für Richtlinie, und stellen Sie sicher, dass Bereichsanforderungen weiterleiten ausgewählt ist.

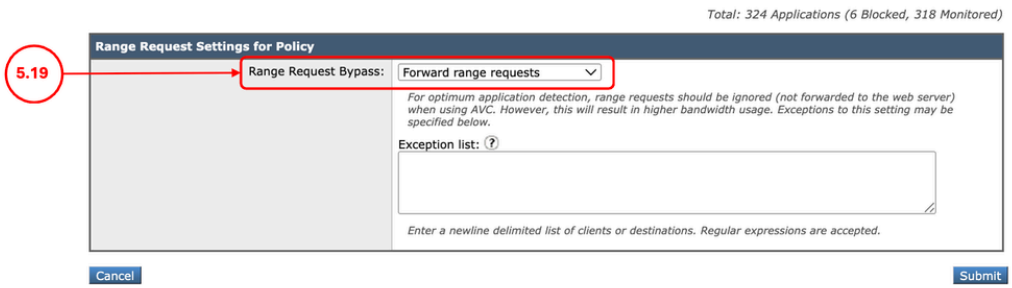


Bild - Bereichsanforderungseinstellungen für Richtlinie

Schritt 5.20: Senden.

Schritt 5.21. Klicken Sie auf der Seite Zugriffsrichtlinien unter Anwendungen auf den Link, der mit der globalen Richtlinie verknüpft ist.

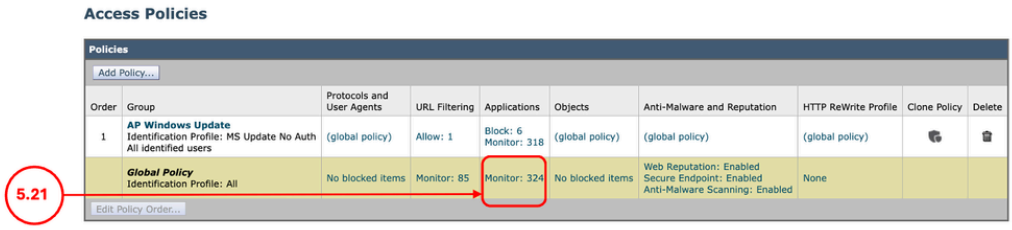


Bild - Standardeinstellungen für die Zugriffsrichtlinie

Schritt 5.22. Blättern Sie nach unten zum Abschnitt Range Request Settings for Policy (Bereichsanforderungseinstellungen für Richtlinie), und stellen Sie sicher, dass Do Not Forward Range Requests (Bereichsanforderungen nicht weiterleiten) ausgewählt ist.

Schritt 5.23: Änderungen bestätigen.

Ändern der Zugriffsprotokolle

Um mehr Transparenz für die Bereichsanforderungen aus den Zugriffsprotokollen zu erhalten, können Sie die folgenden benutzerdefinierten Felder hinzufügen:

[Client-Bereich = %<Bereich:]	Zeigt den vom Client angeforderten Bereich an (Bytes)
[content= %>Inhaltslänge:]	Zeigt die Größe der heruntergeladenen Inhalte an (Byte)

Weitere Informationen zum Hinzufügen eines benutzerdefinierten Felds zu den SWA-Zugriffsprotokollen finden Sie unter diesem Link: Configure Performance Parameter in Access Logs (Leistungsparameter in Zugriffsprotokollen konfigurieren)

Verifizierung

Verwenden Sie diesen CURL-Befehl, um eine Bereichsanforderung an den SWA zu senden:

```
curl -vvvk -H "Pragma: no-cache" -x 10.48.48.181:3128 -H 'Range: bytes=0-100' 'http://catalog.sf.dl.del
```

Aus der Ausgabe der CURL geht hervor, dass die HTTP-Antwort HTTP/1.1 206 ist:

```
> GET http://catalog.sf.dl.delivery.mp.microsoft.com/filestreamingservice/files/f263aa64-f367-42f0-9cad
> Host: catalog.sf.dl.delivery.mp.microsoft.com
> User-Agent: curl/8.7.1
> Accept: */*
> Proxy-Connection: Keep-Alive
> Pragma: no-cache
> Range: bytes=0-100
>
* Request completely sent off
< HTTP/1.1 206 Partial Content
```

Aus den Zugriffsprotokollen können Sie sehen, dass die Aktion TCP_CLIENT_REFRESH_MISS/206 lautet:

```
1773942471.096 14 10.190.0.206 TCP_CLIENT_REFRESH_MISS/206 860 GET http://catalog.sf.dl.delivery.mp.mic
```

Zugehörige Informationen

- 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
- Konfigurieren von Leistungsparametern in Zugriffsprotokollen
- Best Practices für sichere Web-Appliances - Cisco
- Umgehung der Authentifizierung in einer sicheren Web-Appliance - Cisco

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.