Umgehen des Datenverkehrs von Microsoft Updates in einer sicheren Web-Appliance

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Microsoft-Updates

Microsoft-Updates umgehen

- Datenverkehr in SWA umgehen

Schritte zum Durchlaufen von Microsoft Updates

Zugehörige Informationen

Einleitung

In diesem Dokument werden die Schritte zur Umgehung des Datenverkehrs von Microsoft Updates in der sicheren Web-Appliance (SWA) beschrieben.

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.

Microsoft-Updates

Microsoft Updates sind wichtige Patches, Sicherheits-Updates und Funktionsverbesserungen, die Microsoft für seine Betriebssysteme und Softwareanwendungen veröffentlicht. Diese Updates sind für die Aufrechterhaltung der Sicherheit, Stabilität und Leistung von Computern und Netzwerkgeräten von entscheidender Bedeutung. Sie stellen sicher, dass Systeme vor Schwachstellen geschützt sind, Fehler behoben werden und neue Funktionen oder Verbesserungen in die Software integriert werden.

Microsoft Updates können erhebliche Auswirkungen auf Proxy-Server wie Cisco SWA haben. Diese Updates beinhalten oft das Herunterladen großer Dateien oder zahlreicher kleinerer Dateien, die erhebliche Bandbreite und Verarbeitungsressourcen auf dem Proxy beanspruchen können. Dies kann zu Engpässen, einer langsameren Netzwerkleistung und einer höheren Auslastung der Proxy-Infrastruktur führen und sich potenziell auf das allgemeine Benutzererlebnis und andere wichtige Netzwerkvorgänge auswirken.

Das Umgehen des Microsoft Update-Verkehrs vom Proxy kann eine sichere und effektive Möglichkeit sein, diese Herausforderungen zu bewältigen. Da Microsoft Updates von vertrauenswürdigen Microsoft-Servern stammen, kann die Umgehung des Proxys durch diesen Datenverkehr dazu beitragen, die Auslastung des Proxyservers zu reduzieren, ohne die Netzwerksicherheit zu beeinträchtigen. So wird sichergestellt, dass wichtige Updates effizient bereitgestellt werden, während Proxy-Ressourcen für andere Sicherheits- und Content-Filterungsaufgaben erhalten bleiben. Es ist jedoch wichtig, solche Umgehungskonfigurationen sorgfältig zu implementieren, um die Netzwerksicherheit und die Einhaltung der Unternehmensrichtlinien insgesamt zu gewährleisten.

Microsoft-Updates umgehen

Wenn Sie erwägen, den Proxy-Verkehr von Microsoft Updates zu vermeiden, gibt es zwei Hauptansätze

1. Bypass: Hierzu muss das Netzwerk so konfiguriert werden, dass der Datenverkehr so umgeleitet wird, dass er die SWA nicht erreicht.
2. Passthrough: Hierbei wird der SWA so konfiguriert, dass der Datenverkehr von Microsoft Updates weder entschlüsselt noch gescannt wird, sodass er ohne Überprüfung durch den Proxy geleitet werden kann.

Datenverkehr in SWA umgehen

Um den Datenverkehr von Microsoft Updates in mit SWA ausgestatteten Netzwerken zu umgehen, variiert der Ansatz je nach der Einrichtung der Proxy-Bereitstellung:

Bereitstellungstyp	Umgehung des Datenverkehrs

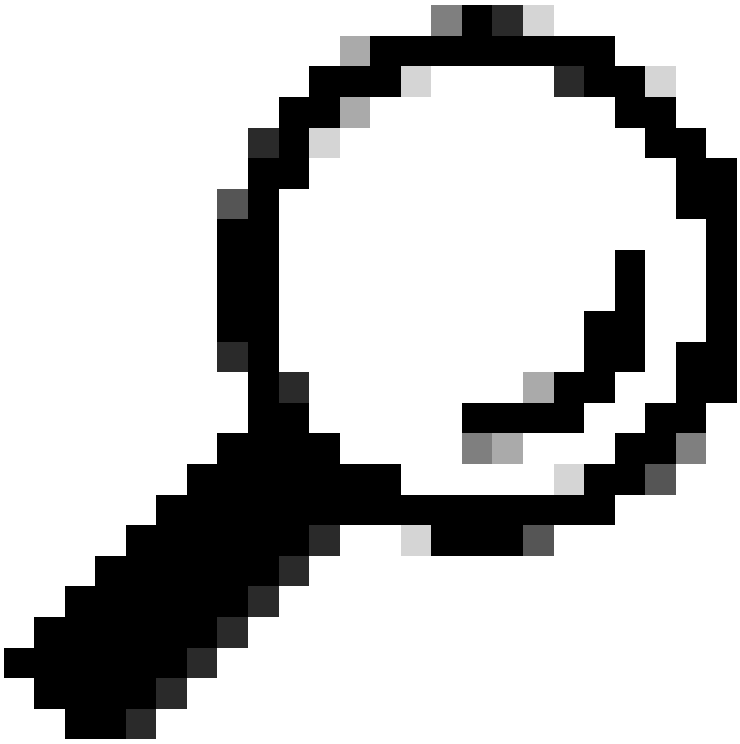
Transparente Bereitstellung	Sie können den Datenverkehr von Microsoft Updates über den Router oder die Layer-4-Switches umleiten, die für die Weiterleitung des Datenverkehrs an den Proxyserver zuständig sind.
	Sie können die Umgehungseinstellungen direkt in der grafischen Benutzeroberfläche (GUI) von SWA konfigurieren.
Explizite Bereitstellung	Um zu verhindern, dass der Datenverkehr von Microsoft Updates die SWA erreicht, müssen Sie die Umgehungsleitung an der Quelle konfigurieren. Dies bedeutet, dass die relevanten URLs auf den Client-Computern von der Pflicht zur Freistellung ausgenommen werden, um sicherzustellen, dass der Datenverkehr nicht an die SWA umgeleitet wird.

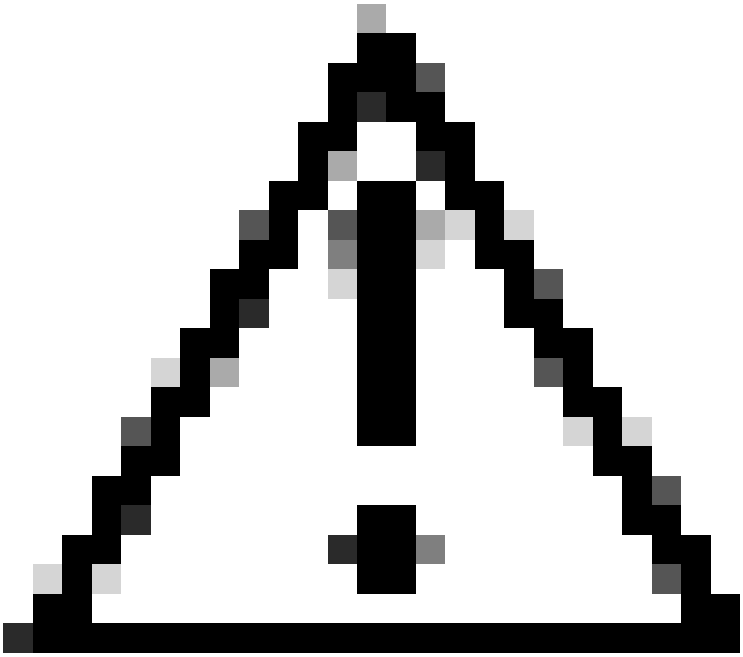
Wenn die Umgehung eines bestimmten Datenverkehrs eine umfassende Netzwerkneugestaltung erfordert und nicht durchführbar ist, besteht ein alternativer Ansatz darin, die SWA so zu konfigurieren, dass sie bestimmte Datenverkehrstypen durchläuft. Dies kann erreicht werden, indem der SWA so eingestellt wird, dass der designierte Datenverkehr weder entschlüsselt noch gescannt wird, sodass er ohne Überprüfung durch den Proxy geleitet werden kann. Mit dieser Methode wird sichergestellt, dass wichtiger Datenverkehr effizient bereitgestellt wird und die Auswirkungen auf die Netzwerkleistung und die Proxy-Ressourcen minimiert werden.

Schritte zum Durchlaufen von Microsoft Updates

Es gibt vier Hauptphasen zum Durchlaufen von Microsoft Updates-Datenverkehr:

Phase	Schritte
1. Erstellen einer benutzerdefinierten URL-Kategorie für Microsoft Updates-URLs	Schritt 1.Wählen Sie aus der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Benutzerdefinierte und externe URL-Kategorien. Schritt 2: Klicken Sie aufKategorie hinzufügen,um eine benutzerdefinierte URL-Kategorie hinzuzufügen. Schritt 4: Zuweisen eines eindeutigen Kategorienamens. Schritt 5: (optional) Beschreibung hinzufügen. Schritt 6: Wählen Sie aus der Listenreihenfolge die erste Kategorie aus, die oben positioniert werden soll.

	Schritt 7. Wählen Sie aus der Dropdown-Liste Kategorie Typ die Option Lokale benutzerdefinierte Kategorie aus. Schritt 8: 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 - Informationen

	 Vorsicht: Kopieren/Einfügen der URLs nicht wie in den Microsoft-Dokumenten; Formatieren Sie sie ordnungsgemäß als SWA-Format. Weitere Informationen finden Sie unter: Benutzerdefinierte URL-Kategorien in Secure Web Appliance konfigurieren - Cisco Schritt 9. Senden.
2. Erstellen eines Identifizierungsprofils, um den Datenverkehr von Microsoft Updates von der Authentifizierung auszunehmen	Schritt 10.Wählen Sie in der GUI Web Security Manager aus, und klicken Sie dann auf Identification Profiles. Schritt 11.Klicken Sie auf Profil hinzufügen, um ein Profil hinzuzufügen. Schritt 12: Aktivieren Sie das Kontrollkästchen Identifikationsprofil aktivieren, um dieses Profil zu aktivieren, oder deaktivieren Sie es schnell, ohne es zu löschen. Schritt 13: Weisen Sie einen eindeutigen profileName zu. Schritt 14: (Optional) Beschreibung hinzufügen. Schritt 15.Wählen Sie aus der Dropdown-Liste Einfügen aus, wo dieses Profil in der Tabelle angezeigt werden soll. Schritt 16: Wählen Sie im Abschnitt User Identification Method die OptionExempt from authentication/identification aus. Schritt 17.Geben Sie im Feld Member nach Subnetz definieren, wenn Sie den Microsoft-Datenverkehr für

	bestimmte Benutzer weiterleiten möchten, die entsprechenden IP-Adressen oder Subnetze ein, oder lassen Sie dieses Feld leer, um alle IP-Adressen einzuschließen. Schritt 18: Wählen Sie im Abschnitt Erweitert die Option Benutzerdefinierte URL-Kategorien aus. Schritt 19: Fügen Sie die benutzerdefinierte URL-Kategorie hinzu, die für Microsoft-Updates erstellt wurde. Schritt 20: Klicken Sie auf Done (Fertig). Schritt 21: Senden.
3. Entschlüsselungsrichtlinie erstellen, um Datenverkehr von Microsoft Updates weiterzuleiten	Schritt 22.Wählen Sie aus der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Entschlüsselungsrichtlinie. Schritt 23: Klicken Sie auf Add-Richtlinie, um eine Entschlüsselungsrichtlinie hinzuzufügen. Schritt 24: Aktivieren Sie die Richtlinie über das Kontrollkästchen Enable Policy (Richtlinie aktivieren). Schritt 25: Zuweisen eines eindeutigen PolicyName. Schritt 26. (Optional) Beschreibung hinzufügen. Schritt 27.Wählen Sie aus der Dropdown-Liste "Insert Above Policy" (Über Richtlinie einfügen) die erste Richtlinie aus. Schritt 28.Wählen Sie aus den Identifikationsprofilen und Benutzern das Identifikationsprofil aus, das Sie in den vorherigen Schritten erstellt haben. Schritt 29: Senden. Schritt 30.Klicken Sie auf der Seite Entschlüsselungsrichtlinien unter URL-Filterung auf den Link, der dieser neuen Entschlüsselungsrichtlinie zugeordnet ist. Schritt 32.Wählen Sie Passthrough als Aktion für die URL-Kategorie von Microsoft Updates aus. Schritt 32: Senden.
4. Erstellen einer Zugriffsrichtlinie, um Microsoft Updates-Datenverkehr	Schritt 33.Wählen Sie aus der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Zugriffsrichtlinie.

zuzulassen	Schritt 34: Klicken Sie auf Add Policy, um eine Zugriffsrichtlinie hinzuzufügen. Schritt 35: Aktivieren Sie die Richtlinie über das Kontrollkästchen Enable Policy (Richtlinie aktivieren). Schritt 36: Zuweisen eines eindeutigen PolicyName. Schritt 37. (Optional) Beschreibung hinzufügen. Schritt 38: Wählen Sie aus der Dropdown-Liste "Insert Above Policy" (Über Richtlinie einfügen) die erste Richtlinie aus. Schritt 39: Wählen Sie aus den Identifikationsprofilen und Benutzern das Identifikationsprofil aus, das Sie in den vorherigen Schritten erstellt haben. Schritt 40: Senden. Schritt 9. Klicken Sie auf der Seite Access Policies (Zugriffsrichtlinien) unter URL Filtering (URL-Filterung) auf den Link, der dieser neuen Zugriffsrichtlinie zugeordnet ist. Schritt 10.Wählen Sie die Aktion für die benutzerdefinierte URL-Kategorie aus, die für Microsoft Updates erstellt wurde. Schritt 11. Senden. Schritt 12: Änderungen bestätigen.

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
- 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.