Blockieren von Datenverkehr in einer sicheren Web-Appliance

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Blockieren von Datenverkehr in einer sicheren Web-Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

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

- SWA-Verwaltung.

Cisco empfiehlt Folgendes:

- Installierte physische oder virtuelle SWA.
- 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.

Blockieren des Datenverkehrs

Die Blockierung des Datenverkehrs in den SWAs ist ein wichtiger Schritt, um die Netzwerksicherheit zu gewährleisten, die Einhaltung interner Richtlinien zu gewährleisten und sich vor böswilligen Aktivitäten zu schützen. Hier einige häufige Gründe für die Blockierung von Datenverkehr:

Gründe für die Sperrung nach Quelle

- Flooding durch einzelne oder mehrere Benutzer: Wenn ein oder mehrere Benutzer übermäßigen Datenverkehr generieren, kann dies zu einer Überlastung des Netzwerks und damit zu Leistungseinbußen und potenziellen Serviceausfällen führen.
- Nicht vertrauenswürdiger Ressourcenzugriff durch Anwendungen (Benutzer-Agents): Bestimmte Anwendungen können versuchen, auf nicht vertrauenswürdige oder potenziell schädliche Ressourcen zuzugreifen. Die Blockierung dieser Benutzer-Agenten trägt dazu bei, Sicherheitslücken und Datenlecks zu verhindern.
- Einschränkung des Internetzugriffs für bestimmte IP-Bereiche: Möglicherweise muss der Zugriff auf das Internet für einige IP-Adressen oder Bereiche aufgrund von Sicherheitsrichtlinien oder zur Verhinderung einer nicht autorisierten Nutzung eingeschränkt werden.
- Verdächtiges Datenverkehrsverhalten: Datenverkehr mit ungewöhnlichen Mustern oder Verhaltensweisen, die auf schädliche Aktivitäten oder Sicherheitsbedrohungen hinweisen können, muss blockiert werden, um das Netzwerk zu schützen.

Gründe für die Sperrung nach Ziel

- Einhaltung interner Unternehmensrichtlinien: Unternehmen verfügen häufig über Richtlinien, die den Zugriff auf bestimmte Websites oder Online-Ressourcen beschränken, um die Produktivität und die Einhaltung gesetzlicher oder behördlicher Auflagen sicherzustellen.
- Nicht vertrauenswürdige Websites: Das Blockieren des Zugriffs auf Websites, die als nicht vertrauenswürdig oder potenziell schädlich eingestuft werden, schützt Benutzer vor Phishing, Malware und anderen Online-Bedrohungen.
- Bösartiges Verhalten: Websites, die für das Hosting bösartiger Inhalte oder für schädliche Aktivitäten bekannt sind, müssen blockiert werden, um Sicherheitsvorfälle und Datensicherheitsverletzungen zu verhindern.

.

Schritte zur Blockierung von Datenverkehr

In der Regel gibt es drei Hauptstufen zum Blockieren des Datenverkehrs in SWA:

- Erstellen Sie ein Identifikationsprofil für die Benutzer.
- Blockieren Sie den HTTPS-Datenverkehr in der Entschlüsselungsrichtlinie.

- Blockieren Sie den HTTP-Verkehr in der Zugriffsrichtlinie.

Phasen	Sperren des Zugriffs auf Websites durch bestimmte Benutzer	Sperren des Zugriffs bestimmter Benutzer auf bestimmte Websites
Benutzerdefinierte URL-Kategorie	Nicht zutreffend.	Erstellen Sie eine benutzerdefinierte URL-Kategorie für die Websites, deren Zugriff Sie blockieren möchten. Weitere Informationen finden Sie unter: [Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco]
Identifizierungsprofil	Schritt 1: Wählen Sie in der GUI Web Security Manager aus, und klicken Sie dann auf Identification Profiles. Schritt 2: Klicken Sie auf Profil hinzufügen, um ein Profil hinzuzufügen. Schritt 3: Verwenden Sie das Kontrollkästchen Identifikationsprofil aktivieren, um dieses Profil zu aktivieren oder es schnell zu deaktivieren, ohne es zu löschen. Schritt 4: Weisen Sie einen eindeutigen Profilnamen zu. Schritt 5: (optional) Beschreibung hinzufügen. Schritt 6: Wählen Sie aus der Dropdown-Liste Insert Above (Oben einfügen) aus, wo dieses Profil in der Tabelle angezeigt werden soll. Schritt 7. Wählen Sie im	Hinweis: Um den Zugriff auf bestimmte Websites für alle Benutzer zu blockieren, ist es nicht erforderlich, ein separates ID-Profil zu erstellen. Dies kann über die globale Entschlüsselungs-/Zugriffsrichtlinie effizient verwaltet werden. Schritt 1: Wählen Sie in der

	Abschnitt User Identification Method die Option Exempt from authentication/identification (Von Authentifizierung/Identifizierung ausnehmen) aus. Schritt 8: Geben Sie unter Mitglieder nach Subnetz definieren die IP-Adressen oder Subnetze ein, die dieses Identifikationsprofil anwenden muss. Sie können IP-Adressen, CIDR-Blöcke (Classless Inter-Domain Routing) und Subnetze verwenden.	GUI Web Security Manager aus, und klicken Sie dann auf Identification Profiles. Schritt 2: Klicken Sie auf Profil hinzufügen, um ein Profil hinzuzufügen. Schritt 3: Verwenden Sie das Kontrollkästchen Identifikationsprofil aktivieren, um dieses Profil zu aktivieren oder es schnell zu deaktivieren, ohne es zu löschen. Schritt 4: Weisen Sie einen eindeutigen Profilnamen zu. Schritt 5: (optional) Beschreibung hinzufügen. Schritt 6: Wählen Sie aus der Dropdown-Liste Insert Above (Oben einfügen) aus, wo dieses Profil in der Tabelle angezeigt werden soll. Schritt 7. Wählen Sie im Abschnitt User Identification Method die Option Exempt from authentication/identification (Von Authentifizierung/Identifizierung ausnehmen) aus. Schritt 8: Geben Sie unter Mitglieder nach Subnetz definieren die IP-Adressen oder Subnetze ein, die dieses Identifikationsprofil anwenden muss. Sie können IP-Adressen, CIDR-Blöcke (Classless Inter-Domain Routing) und Subnetze verwenden. Schritt 9. Klicken Sie auf Erweitert, und fügen Sie die URL-Kategorie hinzu, die den Zugriff blockieren soll.

Entschlüsselungsrichtlinie	Schritt 1: Wählen Sie in der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Entschlüsselungsrichtlinie. Schritt 2: Klicken Sie auf Richtlinie hinzufügen, um eine Entschlüsselungsrichtlinie hinzuzufügen. Schritt 3: Verwenden Sie das Kontrollkästchen Enable Policy (Richtlinie aktivieren), um diese Richtlinie zu aktivieren. Schritt 4: Weisen Sie einen eindeutigen Richtliniennamen zu. Schritt 5: (optional) Beschreibung hinzufügen. Schritt 6: Wählen Sie aus der Dropdown-Liste Insert Above Policy (Über Richtlinie einfügen) die erste Richtlinie aus. Schritt 7. Wählen Sie unter Identifikationsprofile und Benutzer das Identifikationsprofil aus, das Sie mit den vorherigen Schritten erstellt haben. Schritt 8: Senden. Schritt 9. Klicken Sie auf der Seite Entschlüsselungsrichtlinien unter URL-Filterung auf den Link, der dieser neuen Entschlüsselungsrichtlinie zugeordnet ist.	Schritt 1: Wählen Sie in der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Entschlüsselungsrichtlinie. Schritt 2: Klicken Sie auf Richtlinie hinzufügen, um eine Entschlüsselungsrichtlinie hinzuzufügen. Schritt 3: Verwenden Sie das Kontrollkästchen Enable Policy (Richtlinie aktivieren), um diese Richtlinie zu aktivieren. Schritt 4: Weisen Sie einen eindeutigen Richtliniennamen zu. Schritt 5: (optional) Beschreibung hinzufügen. Schritt 6: Wählen Sie aus der Dropdown-Liste Insert Above Policy (Über Richtlinie einfügen) die erste Richtlinie aus. Schritt 7. Wählen Sie unter Identifikationsprofile und Benutzer das Identifikationsprofil aus, das Sie mit den vorherigen Schritten erstellt haben. Schritt 8: Senden. Schritt 9. Klicken Sie auf der Seite Entschlüsselungsrichtlinien unter URL-Filterung auf den Link, der dieser neuen Entschlüsselungsrichtlinie zugeordnet ist. Schritt 10. Wählen Sie Drop als Aktion für die benutzerdefinierte URL-Kategorie aus, die für die

<table>
<tr>
<td></td>
<td>

Tipp: Da Sie alle URL-Kategorien blockieren, können Sie die Richtlinie optimieren, indem Sie benutzerdefinierte URL-Kategorien entfernen und nur die vordefinierten URL-Kategorien verwenden. Dadurch wird die Verarbeitungslast für die SWA verringert, da der zusätzliche Schritt des Abgleichs von URLs mit benutzerdefinierten URL-Kategorien vermieden wird.

Schritt 10. Wählen Sie Drop als Aktion für jede URL-Kategorie aus.

Schritt 11. Scrollen Sie auf derselben Seite nach unten zu Nicht kategorisierte URLs, und wählen Sie Drop from drop-down list aus.

Schritt 12: Senden.

Bild - Entschlüsselungsrichtlinie, um die gesamte Website für bestimmte Benutzer

</td>
<td>

gesperrten Websites erstellt wurde.

Schritt 11. Klicken Sie auf Senden.

Bild: Sperren bestimmter URLs in der Entschlüsselungsrichtlinie

</td>
</tr>
</table>

	zu sperren	
Zugriffsrichtlinie	Schritt 1: Wählen Sie in der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Zugriffsrichtlinie. Schritt 2: Klicken Sie auf Add Policy (Richtlinie hinzufügen), um eine Zugriffsrichtlinie hinzuzufügen. Schritt 3: Verwenden Sie das Kontrollkästchen Enable Policy (Richtlinie aktivieren), um diese Richtlinie zu aktivieren. Schritt 4: Weisen Sie einen eindeutigen Richtliniennamen zu. Schritt 5: (optional) Beschreibung hinzufügen. Schritt 6: Wählen Sie aus der Dropdown-Liste Insert Above Policy (Über Richtlinie einfügen) die erste Richtlinie aus. Schritt 7. Wählen Sie unter Identifikationsprofile und Benutzer das Identifikationsprofil aus, das Sie mit den vorherigen Schritten erstellt haben. Schritt 8: Senden. Schritt 9. Klicken Sie auf der Seite Zugriffsrichtlinien unter Protokolle und Benutzer-Agents auf den Link, der mit dieser neuen Zugriffsrichtlinie verknüpft ist. Schritt 10. Wählen Sie in der Dropdown-Liste Edit Protocols and User Agents Settings (Protokolle und Benutzer-	Schritt 1: Wählen Sie in der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Zugriffsrichtlinie. Schritt 2: Klicken Sie auf Add Policy (Richtlinie hinzufügen), um eine Zugriffsrichtlinie hinzuzufügen. Schritt 3: Verwenden Sie das Kontrollkästchen Enable Policy (Richtlinie aktivieren), um diese Richtlinie zu aktivieren. Schritt 4: Weisen Sie einen eindeutigen Richtliniennamen zu. Schritt 5: (optional) Beschreibung hinzufügen. Schritt 6: Wählen Sie aus der Dropdown-Liste Insert Above Policy (Über Richtlinie einfügen) die erste Richtlinie aus. Schritt 7. Wählen Sie unter Identifikationsprofile und Benutzer das Identifikationsprofil aus, das Sie mit den vorherigen Schritten erstellt haben. Schritt 8: 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 Blockieren als Aktion für die benutzerdefinierte URL-Kategorie aus, die für die

<table>
<tr>
<td></td>
<td>
Agents bearbeiten Einstellungen) die Option Define Custom Settings (Benutzerdefinierte Einstellungen definieren).

Schritt 11. In Protokolle sperren Wählen Sie die Kontrollkästchen für beide FTP über HTTP und HTTP.

Schritt 12: In HTTP CONNECT Ports: Entfernen Sie alle Port-Nummern, um alle Ports zu blockieren.

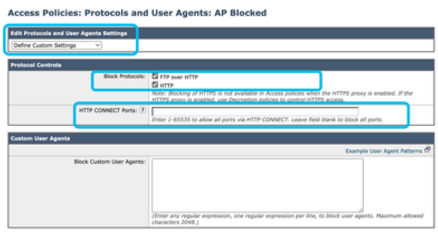


Image - Blockieren von Protokollen und Verbinden von Ports in Zugriffsrichtlinien

Schritt 13: Senden.

Schritt 14 (optional) Klicken Sie auf der Seite Access Policies (Zugriffsrichtlinien) unter URL Filtering (URL-Filterung) auf den Link, der dieser neuen Zugriffsrichtlinie zugeordnet ist, und Wählen Sie für jede URL-Kategorie Block als Aktion aus, und Nicht kategorisierte URLs dann senden.
</td>
<td>
blockierten Websites erstellt wurde.

Schritt 11. Senden.

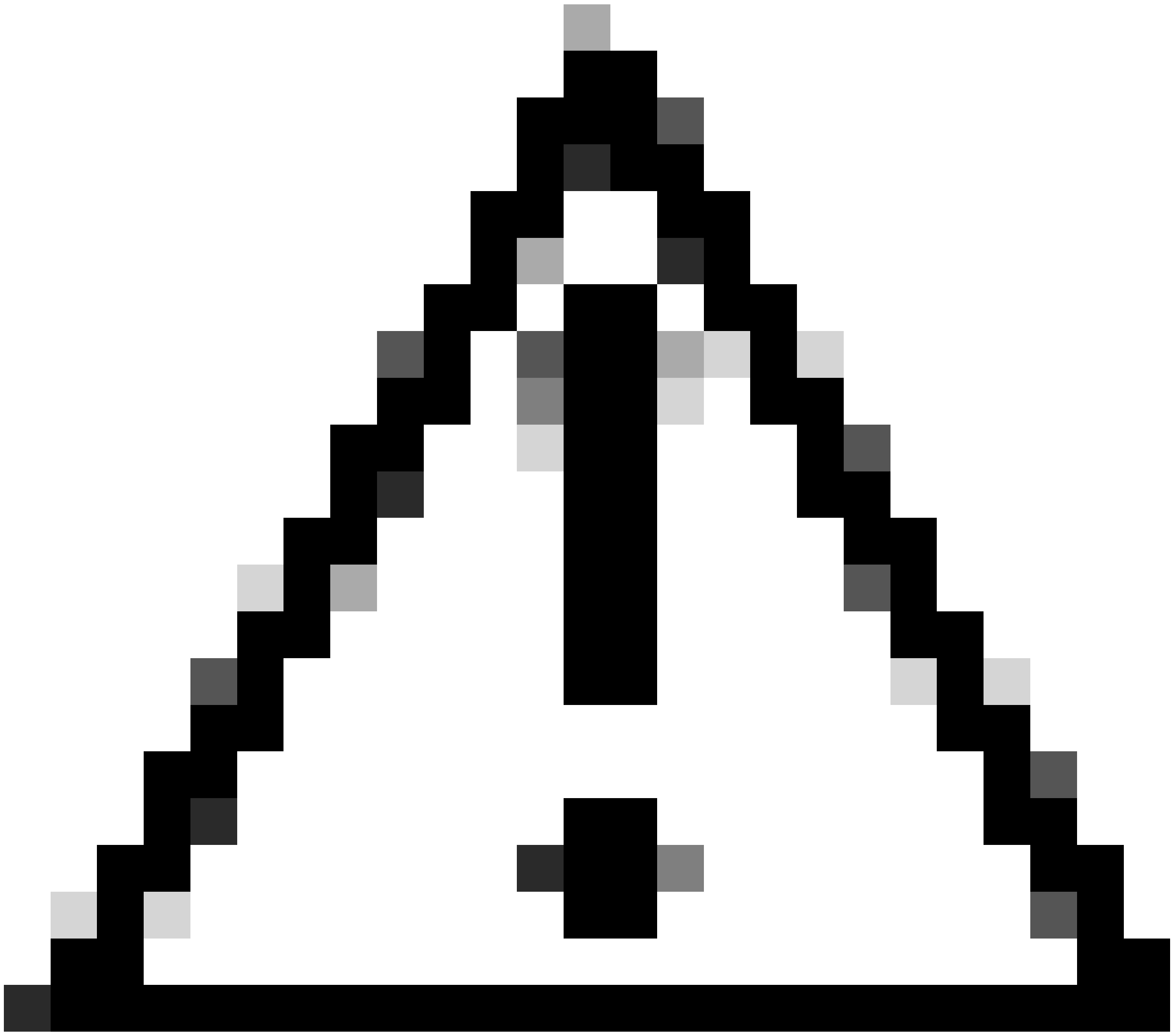
Schritt 12: Änderungen bestätigen.

Bild: Sperren bestimmter URLs in der Zugriffsrichtlinie
</td>
</tr>
</table>

Tipp: Da Sie alle URL-Kategorien blockieren, können Sie die Richtlinie optimieren, indem Sie benutzerdefinierte URL-Kategorien entfernen und nur die vordefinierten URL-Kategorien verwenden. Dadurch wird die Verarbeitungslast für die SWA verringert, da der zusätzliche Schritt des Abgleichs von URLs mit benutzerdefinierten URL-Kategorien vermieden wird.

Schritt 16: Änderungen bestätigen.

Bild: Zugangsrichtlinie zum Sperren aller Standorte



Achtung: Bei einer transparenten Proxy-Bereitstellung kann SWA keine Benutzer-Agenten oder die vollständige URL für HTTPS-Datenverkehr lesen, es sei denn, der Datenverkehr wird entschlüsselt. Wenn Sie das Identifizierungsprofil mithilfe von Benutzer-Agents oder einer benutzerdefinierten URL-Kategorie mit regulären Ausdrücken konfigurieren, stimmt dieser Datenverkehr nicht mit dem Identifizierungsprofil überein.

Sperren von Websites mit regulären Ausdrücken in einer transparenten Proxybereitstellung

Wenn Sie bei der Bereitstellung eines transparenten Proxys eine benutzerdefinierte URL-Kategorie blockieren möchten, die die Bedingung Reguläre Ausdrücke aufweist - beispielsweise wenn Sie den Zugriff auf einige YouTube-Kanäle blockieren -, können Sie die folgenden Schritte ausführen:

Schritt 1: Erstellen Sie eine benutzerdefinierte URL-Kategorie für die Hauptwebsite. (In diesem Beispiel: YouTube.com).

Schritt 2: Erstellen Sie eine Entschlüsselungsrichtlinie, weisen Sie diese benutzerdefinierte URL-Kategorie zu, und legen Sie als Aktion "Entschlüsseln" fest.

Schritt 3: Erstellen Sie eine Zugriffsrichtlinie, weisen Sie die benutzerdefinierte URL-Kategorie den regulären Ausdrücken zu (in diesem Beispiel die benutzerdefinierte URL-Kategorie für die YouTube-Kanäle), und legen Sie die Aktion auf Blockieren fest.

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

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.