

Entsperren von Office 365-Datenverkehr von der Authentifizierung und Entschlüsselung auf der Cisco Web Security Appliance (WSA)

Inhalt

[Einführung](#)

[Konfigurationsschritte](#)

[1. Erstellen einer benutzerdefinierten URL-Kategorie mit dem externen Office365-Feed](#)

[2. Erstellen eines Identifizierungsprofils für den Office 365-Datenverkehr](#)

[3. Entziehen des Office 365-Datenverkehrs von der Entschlüsselungsrichtlinie](#)

[Referenz](#)

Einführung

Dieser Artikel beschreibt den Prozess, mit dem Office 365-Datenverkehr von der Authentifizierung und Entschlüsselung auf der Web Security Appliance (WSA) ausgenommen wird. Es gibt mehrere bekannte Kompatibilitätsprobleme mit Office 365 und Proxys, und die Ausnahme von Office 365-Datenverkehrsauthentifizierung und -entschlüsselung kann bei einigen dieser Probleme hilfreich sein.

Hinweis: Dabei handelt es sich nicht um eine vollständige Umgehung vom Webproxy, und das Entschlüsseln von Datenverkehr verhindert, dass die WSA den von Office 365-Clients generierten verschlüsselten HTTPS-Datenverkehr überprüft.

Konfigurationsschritte

Überblick:

1. Erstellen einer **benutzerdefinierten URL-Kategorie** mit dem externen Feed Office365
2. Erstellen eines **Identifikationsprofils** für den Office 365-Datenverkehr
3. Entziehen des Office 365-Datenverkehrs von der **Entschlüsselungsrichtlinie**

Hinweis: Dieser Prozess erfordert die dynamische Aktualisierung des externen Office 365-JSON-Feeds, der alle mit Office 365 verknüpften URLs/IP-Adressen enthält.

Hinweis: Unterstützung für diesen Feed ist ab AsyncOS Version 10.5.3 und ab Version 11.5 vorhanden.

1. Erstellen einer benutzerdefinierten URL-Kategorie mit dem externen Office365-Feed

- Navigieren Sie zu **Websicherheits-Manager > Benutzerdefinierte und externe URL-**

Kategorien.

- Klicken Sie auf "**Kategorie hinzufügen**".
- Weisen Sie der Kategorie einen Namen zu, wählen Sie den Kategorietyt als "**Externe Live-Feed-Kategorie**" aus, und wählen Sie "**Office 365-Webdienst**".
- Klicken Sie auf "**Start Test**", wenn Sie die Fähigkeit der WSA testen möchten, den Office 365 JavaScript Object Notation (JSON)-Feed herunterzuladen.
- Setzen Sie unten die Option "**Auto Update the Feed**" (**Automatische Aktualisierung des Feeds**) auf "**Stündlich**" mit einem Intervall von 00:05 (alle 5 Minuten).
- Klicken Sie auf die Schaltfläche "**Senden**".

Custom and External URL Categories: Add Category

Edit Custom and External URL Category

Category Name: Office365

List Order: 1

Category Type: External Live Feed Category

Routing Table: Management

Feed File Location: Cisco Feed Format Office 365 Feed Format Office 365 Web Service

Web Service URL: https://endpoints.office.com/enc

Start Test

Checking DNS resolution of feed server...
Success: Resolved 'endpoints.office.com' address: 138.91.80.132

Retrieving feed content from server...
Success: Downloaded and Parsed the feed file.

Test completed successfully.

Excluded Sites:

Sort URLs
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

Advanced Match specific URLs by regular expressions.

Auto Update the Feed: Do not auto update Hourly Every 00:05 (HH:MM)

Cancel Submit

2. Erstellen eines Identifizierungsprofils für den Office 365-Datenverkehr

- Navigieren Sie zu **Web Security Manager > Identifikationsprofile**.
- Klicken Sie auf "**Identifikationsprofil hinzufügen**".
- Weisen Sie einen Namen zu, legen Sie "**Identifikation und Authentifizierung**" auf "**Von Authentifizierung/Identifikation ausnehmen**" fest.
- Klicken Sie auf die Schaltfläche "**Erweitert**", und klicken Sie auf den Link neben "**URL-Kategorien**".
- Suchen Sie die Kategorie, die Sie im vorherigen Schritt erstellt haben, und wählen Sie diese Kategorie aus. Scrollen Sie dann zum Ende der Seite, und klicken Sie auf die Schaltfläche "**Fertig**".

Identity Profiles: Policy "Office365.ID": Membership by URL Categories

Advanced Membership Definition: URL Category

Select any row below to use that URL Category as membership criteria. Leave all rows unselected if membership by URL Category is not desired.

Custom and External URL Categories		
Category	Category Type	
Office365	External Feed	<input type="checkbox"/>

Add
Select all
✓

Das Identifikationsprofil sollte nun wie folgt aussehen:

Identification Profiles: Office365.ID

Client / User Identification Profile Settings

Enable Identification Profile

Name:
(e.g. my IT Profile)

Description:

Insert Above:

User Identification Method

Identification and Authentication:
This option may not be valid if any preceding Identification Profile requires authentication on all subnets.

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by Subnet:
(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

Define Members by Protocol:

- HTTP/HTTPS
- Native FTP

Advanced

Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

URL Categories: Office365

User Agents: None Selected

The Advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories are not applicable for SOCKS transactions or transparent HTTPS (unless decrypted). When Advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.

- Klicken Sie unten auf dem Bildschirm auf die Schaltfläche "Submit" (Senden).

3. Entziehen des Office 365-Datenverkehrs von der Entschlüsselungsrichtlinie

- Navigieren Sie zu **Websicherheits-Manager > Entschlüsselungsrichtlinien**.

- Klicken Sie auf "Policy hinzufügen".
- Weisen Sie einen Namen zu, und wählen Sie dann im Feld "Identifikationsprofile und Benutzer" die Option **Ein oder mehrere Identifikationsprofile** auswählen aus dem vorherigen Schritt Ihre Office 365-Identität aus.

Decryption Policy: Add Group

Policy Settings

Enable Policy

Policy Name: (e.g. my 11 policy)

Description:

Insert Above Policy: 1 (Global Policy) ▾

Policy Expires: Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: :

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: Select One or Merc Identification Profiles ▾

Identification Profile	Authorized Users and Groups	Add Identification Profile
<input type="text" value="Office365.ID"/> ▾	No authentication required	

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

[Advanced](#) Define additional group membership criteria.

Cancel
Submit

- Klicken Sie auf die Schaltfläche "Senden".
- Klicken Sie auf den Link unter "URL-Filterung", der "Monitor: 1 Zoll
- Legen Sie die Kategorie Office 365 auf "Passthrough" fest, und klicken Sie auf die Schaltfläche "Submit" (Senden).

Decryption Policies: URL Filtering: Office365.DP

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
<input checked="" type="checkbox"/> Office365	External Feed	-	<input checked="" type="checkbox"/> Select all	<input type="checkbox"/> Select all	<input type="checkbox"/> Select all	<input type="checkbox"/> Select all	<input type="checkbox"/> (Unavailable)	<input type="checkbox"/> (Unavailable)

Cancel
Submit

- Bestätigen Sie schließlich Ihre Änderungen, indem Sie auf die gelbe Schaltfläche "Änderungen bestätigen" oben rechts in der GUI klicken.

Referenz

Offiziellere Dokumentation von Cisco zum **Aktivieren externer Office 365-Feeds** und **Wie wird Office 365 von der Entschlüsselungsrichtlinie in der WSA ausgenommen**:

[Aktivieren von externen Office 365-Feeds in AsyncOS für Cisco Web Security](#)