Wie werden Funktionen von Facebook-Chat und E-Mail auf der Cisco Web Security Appliance blockiert?

Frage:

Wie werden Chat- und E-Mail-Funktionen auf Facebook.com blockiert?

Umgebung: Cisco Web Security Appliance (WSA) für alle AsyncOS-Versionen

Auf AsyncOS Version 7.1 und höher mit aktivierter AVC

In Version 7.1 hat die WSA eine neue Funktion namens "Application Visibility Controls" (AVC) eingeführt, die es ermöglicht, Anwendungen wie Facebook automatisch zu erkennen. Für die AVC-Funktion ist ein Lizenzschlüssel für "Cisco Web Usage Controls" erforderlich, der unter *GUI > Security Services > Acceptable Use Controls* aktiviert werden kann.

Wenn AVC aktiviert ist, können wir AVC verwenden, um bestimmte Funktionen auf "Facebook" wie Facebook-Nachrichten und Chat, Facebook-Spiele usw. zu blockieren. AVC bietet außerdem die Möglichkeit, viele andere Anwendungen wie ITunes, Google+ usw. zu erkennen und zu steuern.

Facebook-"Chat"-Funktion mit AVC blockieren
1. Navigieren Sie zu *GUI > Web Security Manager > Access Policies (Zugriffsrichtlinien).* 2. Klicken Sie für eine bestimmte Zugriffsrichtlinie oder "*Globale Richtlinie"* auf den Link in der Spalte "***Anwendungen***". 3. Klicken Sie unter "*Anwendungseinstellungen bearbeiten"* auf das Pluszeichen (+) neben "Facebook", um alle verfügbaren Optionen anzuzeigen. 4. Konfigurieren Sie "***Facebook-Nachrichten und -Chat***" auf "**Blockieren".** 5. Wenn Sie den Video-Chat nur blockieren möchten, wählen Sie "**Monitor**" und aktivieren Sie dann die Option **"Video Chat**".

Auf allen AsyncOS-Versionen oder mit Version 7.1 und höher, wenn AVC deaktiviert ist

Wenn die AVC-Funktion nicht verfügbar ist, können wir auch die Chat- und E-Mail-Funktionen in Facebook blockieren, indem wir bestimmte URLs zuordnen.

Facebook.com-Chat-Funktion blockieren
1. Navigieren Sie zu *Sicherheitsmanager -> Benutzerdefinierte URL-Kategorien ->*

Benutzerdefinierte Kategorie hinzufügen

2. Füllen Sie "Kategoriename" aus und klicken Sie auf "Erweitert".
3. Geben Sie "**facebook.*chat**" im Fenster "***Regulärer Ausdruck***" ein.
4. Navigieren Sie zur Seite *Security Manager -> Access* Policies (Sicherheitsmanager -> Zugriffsrichtlinien).
5. Klicken Sie in der Richtlinientabelle unter der Spalte "*URL-Kategorien*" auf den Link für die betreffende Zugriffsrichtlinie, die Sie bearbeiten möchten.
6. Wählen Sie im Bereich "Benutzerdefinierte URL-Kategoriefilterung" die Aktion "**Blockieren**" aus.
7. Senden und bestätigen Sie Ihre Änderungen.

Facebook.com-Funktion "Nachrichten" blockieren

1. Navigieren Sie zu *Sicherheitsmanager > Benutzerdefinierte URL-Kategorien > Benutzerdefinierte Kategorie hinzufügen.*
2. Füllen Sie "Kategoriename" aus und klicken Sie auf "Erweitert".
3. Geben Sie "**facebook.*gigaboxx**" im Fenster Regulärer Ausdruck ein.
4. Navigieren Sie zur Seite *"Security Manager -> Access Policies" (Sicherheitsmanager -> Zugriffsrichtlinien*).
5. Klicken Sie in der Richtlinientabelle unter der Spalte "*URL-Kategorien*" auf den Link für die betreffende Zugriffsrichtlinie, die Sie bearbeiten möchten.
6. Wählen Sie im Bereich Benutzerdefinierte URL-Kategoriefilterung die Aktion "**Blockieren**" aus.
7. Senden und bestätigen Sie Ihre Änderungen.

Hinweis:

Die Konfigurationsschritte in der zweiten Methode sind nicht dynamisch. Wenn sich die von Facebook verwendeten Websites/URLs ändern, müssen wir die Konfiguration ändern, um die Funktionen für Chat und Nachrichten zu blockieren.

Andererseits aktualisiert die AVC-Funktion ihre Signaturen regelmäßig, um sicherzustellen, dass die Anwendungen ordnungsgemäß erkannt werden. Daher **empfehlen** wir, statt der zweiten Methode den Facebook-Chat und -Nachrichten mit AVC zu blockieren.