# توصيات ضد هجمات رش كلمة المرور التي تؤثر على خدمات VPN للوصول عن بعد

## المحتويات



## المقدمة

يصف هذا المستند التوصيات التي يجب مراعاتها قبل حالات فشل تخصيص رمز المضيف المميز في جدار الحماية الآمن، المشتقة من هجمات رش كلمة المرور.

## معلومات أساسية

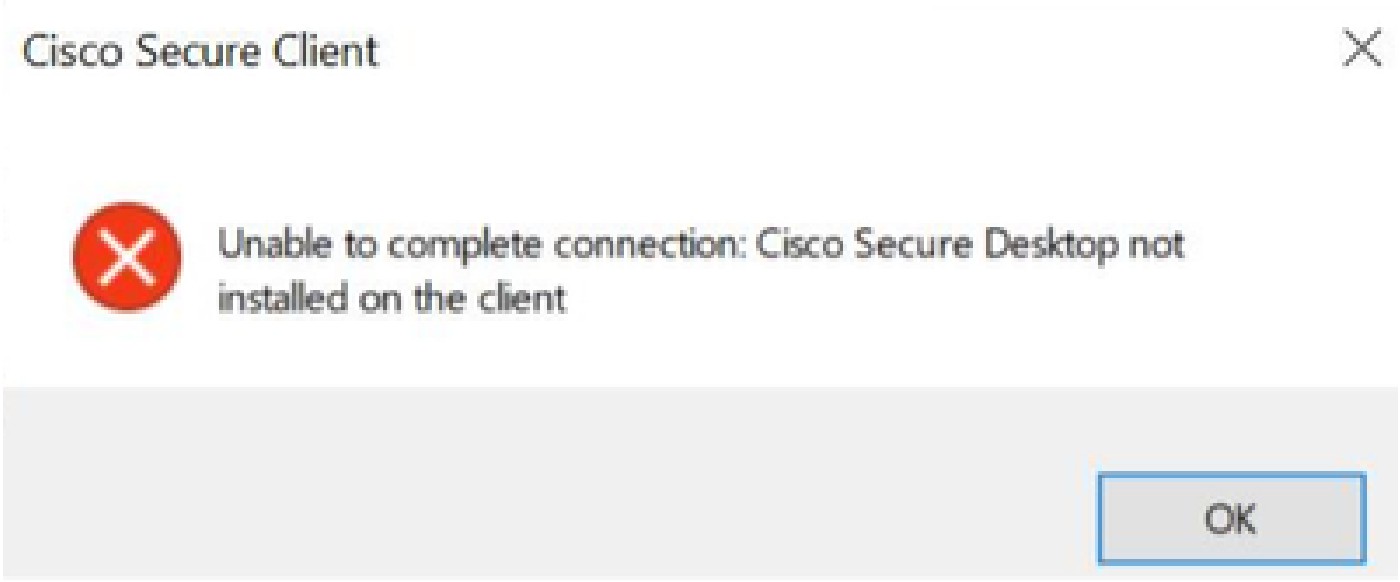
عند محاولة إنشاء اتصال RAPN باستخدام عميل Cisco الآمن (AnyConnect)، يمكن للمستخدمين مواجهة رسالة خطأ بشكل متقطع تذكر، "غير قادر على إكمال الاتصال. لم يتم تثبيت "سطح المكتب الآمن من Cisco" على العميل.". ينشأ هذا السلوك عادة عندما يكون هناك فشل في تخصيص رمز مميز للمسح الضوئي بواسطة وحدة الاستقبال والبث الخاصة بالشبكة الخاصة الظاهرية (VPN)، إما جهاز الأمان القابل للتكيف (ASA) أو الدفاع عن التهديد (FTD) لجدار الحماية الآمن من Cisco. وبشكل ملحوظ، يرتبط فشل التخصيص هذا بحالات هجمات عنيفة للقوة تستهدف البنية التحتية لجدار الحماية الآمن ويتم التعامل معه حاليا بأقصى درجة من الاستعجال بموجب معرف تصحيح الأخطاء من Cisco CSCwj45822.

## السلوكيات التي تمت ملاحظتها

تعذر إنشاء إتصالات VPN مع عميل Cisco الآمن (AnyConnect) عند تمكين

## وضع جدار الحماية (HostScan)

عند محاولة إنشاء اتصال VPN باستخدام عميل Cisco الآمن (AnyConnect)، يمكن للمستخدمين مواجهة رسالة خطأ بشكل متقطع تذكر، تعذر إكمال الاتصال. لم يتم تثبيت "سطح المكتب الآمن من Cisco" على العميل." يمنع هذا الإصدار الإكمال الناجح من اتصال VPN عميل.




ملاحظة: اذا يحدث السلوك المحدد إلا عند تمكين وضع جدار الحماية (HostScan) عند إصدار AnyConnect أو Secure Client استخدام النظر عن بغض ،والبث الاستقبال وحدة.

## إستهلاك رمز Hostscan Token

يعرض جهاز الاستقبال والبث الخاص بشبكة VPN Cisco Secure Firewall Adaptive Security Appliance (ASA) أو Threat Defense (FTD) أعراض حالات فشل تخصيص الرمز المميز للتحميل. للتحقق من ذلك، قم بتشغيل الأمر debug list webVPN 187 0.

<#root>

```
ASA# debug menu webvpn 187 0
Allocated Hostscan token = 1000
```

**Hostscan token allocate failure = xxx - - - - > Increments**

ملاحظة: أيتي حدوث هذه المسألة نتيجة للهجمات. يتم حاليا معالجة المسألة بأقصى سرعة بموجب معرف تصحيح الأخطاء من Cisco CSCwj45822.

## مبلغ غير عادي لطلبات المصادقة

تظهر وحدة الاستقبال والبث الخاصة بشبكة VPN Cisco Secure Firewall ASA أو FTD أعراض هجمات رش كلمة المرور باستخدام 100-آلاف أو الملايين من محاولات المصادقة المرفوضة.

ملاحظة: يمكن توجيه هذه المحاولات غير العادية للمصادقة إما إلى قاعدة البيانات المحلية أو إلى خوادم المصادقة الخارجية.

أفضل طريقة لاكتشاف هذا من خلال النظر إلى syslog. ابحث عن رقم غير عادي من أي من معرفات ASA syslog التالية:

- ٪ASA-6-113015

<#root>

**%ASA-6-113015**

: AAA user authentication Rejected : reason = User was not found : local database :

**user**

= *admin* : user

**IP**

= *x.x.x.x*

- ٪ASA-6-113005

<#root>

**%ASA-6-113005**

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =

- ٪ASA-6-716039

<#root>

**%ASA-6-716039**

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN.

اسم المستخدم مخفي دائما حتى يتم تكوين الأمر no logging hide username على ASA.

---

ملاحظة: هذا يعطي فكرة عن التحقق من إنشاء المستخدمين الصحيحين أو معرفتهم عن طريق الإساءة إلى عناوين IP، الرجاء توخي الحذر حيث أن أسماء المستخدمين ستكون مرئية في السجلات.

---

للتحقق، قم بتسجيل الدخول إلى واجهة سطر الأوامر (CLI) ASA أو FTD، ثم قم بتشغيل الأمر show aaa-server ، وتحقق من وجود عدد غير عادي من طلبات المصادقة التي تم المحاولة عليها أو رفضها إلى أي من خوادم AAA التي تم تكوينها:

<#root>

```
ciscoasa# show aaa-server

Server Group: LDAP-SERVER - - - - - >>>> Sprays against external server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms

Number of authentication requests 2228536 - - - - - >>>> Unusual increments


Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312

Number of rejects 2225363 - - - - - >>>> Unusual increments / Unusual rejection rate


Number of challenges 0
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
```

# توصيات

في حين أنه لا يوجد حاليا حل واحد للقضاء بشكل كامل على الخطر، إلا أنه يمكنك مراجعة وتطبيق الممارسات التالية الموصى بها، والتي تم تصميمها للمساعدة في تقليل أحتمالية حدوث ذلك والحد من تأثير هذه الهجمات العنيفة على إتصالات RAVPN الخاصة بك.

## 1. تمكين التسجيل

التسجيل هو جزء مهم من أمن الإنترنت الذي يتضمن تسجيل الأحداث التي تحدث داخل النظام. ويترك عدم وجود سجلات مفصلة ثغرات في الفهم، مما يعوق إجراء تحليل واضح لطريقة الهجوم. يوصى بتمكين التسجيل إلى خادم syslog عن بعد لتحسين إرتباط ومراجعة حوادث الشبكة والأمان عبر أجهزة الشبكة المختلفة.

للحصول على معلومات حول كيفية تكوين التسجيل، راجع الأدلة التالية الخاصة بالنظام الأساسي:

برامج Cisco ASA:

- إستخدام دليل جدار حماية ASA الآمن
- فصل التسجيل من دليل تكوين واجهة سطر الأوامر الخاصة بالعمليات العامة Cisco Secure Firewall ASA Series General Operations CLI

برنامج FTD من Cisco:

- تكوين تسجيل الدخول إلى FTD من خلال مركز إدارة جدار الحماية (FMC)
- تكوين قسم syslog في فصل إعدادات النظام الأساسي من دليل تكوين جهاز مركز إدارة جدار الحماية الآمن من Cisco
- تكوين syslog والتحقق من صحته في FirePOWER Device Manager
- تكوين قسم إعدادات تسجيل النظام في فصل إعدادات النظام من دليل تكوين الدفاع عن تهديد FirePOWER ل FirePOWER

---

ملاحظة: يجب تمكين معرفات رسائل syslog اللازمة للتحقق من السلوكيات الموضحة في هذا المستند (716039 و 113005 و 113015) على مستوى المعلومات (6). وتندرج هذه المعرفات ضمن فئات التسجيل "المصادقة" و"webVPN".

---

## 2. تطبيق تدابير التعزيز للوصول عن بعد إلى VPN

للتخفيف من أثر هذه الهجمات، قم بتنفيذ تدابير التعزيز التالية:

1. تعطيل مصادقة AAA في DefaultWebVPN وتوصيفات توصيل DefaultRagGroup (خطوة بخطوة: ASA | تتم إدارة برنامج الإرسال فائق السرعة (FTD) بواسطة FMC).
2. تعطيل وضع جدار الحماية الآمن (Hostscan) من DefaultWEBvpngGroup و DefaultRAGgroup (خطوة بخطوة: ASA | تتم إدارة برنامج الإرسال فائق السرعة (FTD) بواسطة FMC).
3. تعطيل أسماء المجموعات المستعارة وتمكين عناوين URL الخاصة بالمجموعات في بقية ملفات تعريف الاتصال (خطوة بخطوة: ASA | تتم إدارة برنامج الإرسال فائق السرعة (FTD) بواسطة FMC).

---

ملاحظة: إذا كنت بحاجة إلى دعم من خلال برنامج الإرسال فائق السرعة (FTD) الذي تتم إدارته من خلال إدارة أجهزة جدار الحماية المحلية (FDM)، فيرجى الاتصال بمركز المساعدة التقنية (TAC) للحصول على إرشادات الخبراء.

---

للحصول على مزيد من التفاصيل، يرجى الرجوع إلى دليل تنفيذ تدابير التعزيز لبروتوكول AnyConnect VPN الآمن الخاص بالعميل.

## 3. حظر محاولات الاتصال من المصادر الضارة

من أجل منع محاولات الاتصال من مصادر غير مصرح لها، يمكنك تنفيذ أي من الخيارات المدرجة أدناه:

تنفيذ قوائم التحكم في الوصول (ACL) على مستوى الواجهة

قم بتنفيذ قائمة التحكم في الوصول (ACL) على مستوى الواجهة على ASA/FTD لتصفية عناوين IP العامة غير المصرح بها ومنعها من بدء جلسات عمل VPN البعيدة.

أستخدم الأمر "تغاضي"

هذا أسلوب واضح لحظر بروتوكول الإنترنت خبيث، ولكن، يجب أن يتم يدويا. الرجاء قراءة المقطع التكوين البديل لحظر الهجمات على جدار الحماية الآمن باستخدام الأمر 'shun' للحصول على مزيد من التفاصيل.

تكوين قائمة التحكم في الوصول إلى مستوى التحكم

تطبيق قائمة التحكم في الوصول (ACL) على ASA/FTD لتصفية عناوين IP العامة غير المصرح بها ومنعها من بدء جلسات عمل VPN البعيدة. تكوين سياسات التحكم في الوصول إلى مستوى التحكم للدفاع الآمن عن تهديد جدار الحماية و ASA.

---

ملاحظة: قام Cisco Talos بنشر قائمة بعناوين IP وبيانات الاعتماد المرتبطة بهذه الهجمات. يمكن العثور على رابط لمستودع GitHub الخاص بهم في قسم "IOCs" من الاستشارات الخاصة بهم. من المهم ملاحظة أن عناوين IP للمصدر لحركة المرور هذه من

---

المرجح أن تتغير، لذلك، يجب عليك مراجعة سجلات الأمان (syslog) لتحديد عناوين IP التي تحتوي على مشاكل. عند تحديد الهوية، يمكن إستخدام أي من الخيارات الثلاثة لحظرها.

## تطبيقات التعزيز الإضافية ل RAVPN

وتهدف التوصيات المقدمة حتى الآن إلى تقليل مخاطر وأثر الهجمات على خدمات الشبكة. ومع ذلك، يمكنك التفكير في إتخاذ تدابير مضادة إضافية تتطلب تغييرات إضافية على عمليات النشر الخاصة بك لتعزيز أمان نشر الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد، مثل اعتماد مصادقة قائمة على الشهادة ل RAPN. يرجى الرجوع إلى مستند تنفيذ تدابير التعزيز لعميل AnyConnect VPN الآمن للحصول على إرشادات التكوين التفصيلية.

## معلومات إضافية

- إجراءات التحقيق الجنائي ل Cisco ASA للمستجيبين الأوائل
- إجراءات التحقيق الجنائي للدفاع عن التهديد الذي تشكله Cisco للمستجيبين الأوائل
- إخطارات تهديد Telos من Cisco
- للحصول على مساعدة إضافية، يرجى الاتصال بمركز المساعدة التقنية (TAC). يلزم عقد دعم صالح: جهات إتصال الدعم العالمية من Cisco.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).