ASA 8.x: وصول VPN لعميل AnyConnect VPN عم عمي ذاتي ةعقوم ةداهش نيوكت لاثم مادختساب

المحتويات

المقدمة

يوضح هذا المستند كيفية إستخدام الشهادات الموقعة ذاتيا للسماح بالوصول عن بعد إلى إتصالات SSL VPN إلى ASA من عميل Cisco AnyConnect 2.0.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- أساسي ASA تشكيل أن يركض برمجية صيغة 8.0
- (ASDM 6.0(2

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ASA 8.0(2) و 2) ASDM 6.0) من Cisco
- Cisco AnyConnect 2.0

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

عميل Cisco AnyConnect 2.0 هو عميل VPN مستند إلى SSL. يمكن إستخدام عميل AnyConnect وتثبيته على مجموعة متنوعة من أنظمة التشغيل، مثل Windows 2000 و XP و Vista و Linux (Multi Distros) و Mac OS X. يمكن تثبيت عميل AnyConnect يدويا على الكمبيوتر البعيد بواسطة مسؤول النظام. كما يمكن تحميلها على جهاز الأمان وجعلها جاهزة للتنزيل إلى المستخدمين البعيدين. بعد تنزيل التطبيق، يمكنه تلقائيا إزالة تثبيت نفسه بعد إنهاء الاتصال، أو يمكن أن يبقى على الكمبيوتر البعيد لاتصالات SSL VPN المستقبلية. يجعل هذا المثال عميل AnyConnect جاهزا للتنزيل عند مصادقة SSL الناجحة المستندة إلى المستعرض.

لمزيد من المعلومات حول عميل AnyConnect 2.0، ارجع إلى ملاحظات إصدار AnyConnect 2.0.

ملاحظة: خدمات MS الطرفية غير مدعومة بالاقتران مع عميل AnyConnect. لا يمكنك تنفيذ RDP على جهاز كمبيوتر ثم بدء جلسة عمل AnyConnect. لا يمكنك الحصول على بروتوكول RDP إلى عميل متصل عبر AnyConnect.

ملاحظة: يتطلب التثبيت الأول من AnyConnect أن يتمتع المستخدم بحقوق المسؤول (سواء كنت تستخدم حزمة AnyConnect MSI المستقلة أو تضغط على ملف PKG من ASA). إذا لم يكن لدى المستخدم حقوق المسؤول، يظهر مربع حوار يوضح هذا المتطلب. لن تتطلب عمليات الترقية التالية أن يتمتع المستخدم الذي قام بتثبيت AnyConnect سابقا بحقوق المسؤول.

التكوين

أكمل الخطوات التالية لتكوين ASA للوصول إلى VPN باستخدام عميل AnyConnect:

1. تكوين شهادة صادرة ذاتيا.
2. تحميل صورة عميل SSL VPN والتعرف عليها.
3. تمكين الوصول إلى AnyConnect.
4. إنشاء نهج مجموعة جديد.
5. تكوين تجاوز قائمة الوصول لاتصالات VPN.
6. إنشاء ملف تعريف اتصال ومجموعة أنفاق لاتصالات عميل AnyConnect.
7. تكوين إستثناء NAT لعملاء AnyConnect.
8. إضافة مستخدمين إلى قاعدة البيانات المحلية.

الخطوة 1. تكوين شهادة صادرة ذاتيا

بشكل افتراضي، يحتوي جهاز الأمان على شهادة موقعة ذاتيا يتم إعادة إنشائها في كل مرة يتم فيها إعادة تشغيل الجهاز. يمكنك شراء شهادتك الخاصة من الموردين، مثل Verisign أو EnTrust، أو يمكنك تكوين ASA لإصدار شهادة هوية لنفسه. تظل هذه الشهادة كما هي حتى عند إعادة تشغيل الجهاز. أكمل هذه الخطوة لإنشاء شهادة ذاتية الإصدار تستمر عند إعادة تشغيل الجهاز.

إجراء ASDM

1. انقر فوق **تكوين**، ثم انقر فوق **شبكة VPN للوصول عن بعد**.
2. قم بتوسيع **إدارة الترخيص**، ثم أختر **شهادات الهوية**.
3. انقر على **إضافة**، ثم انقر على زر **إضافة شهادة هوية جديدة**.
4. طقطقت **جديد**.
5. في شاشة إضافة زوج مفاتيح، انقر زر **إدخال اسم زوج مفاتيح جديد**.
6. أدخل اسما لتعريف زوج المفاتيح.يستخدم هذا المثال *sslvpnKeypair*.
7. انقر فوق **إنشاء الآن**.
8. في شاشة إضافة شهادة هوية، تأكد من تحديد زوج المفاتيح الذي تم إنشاؤه حديثا.
9. بالنسبة ل "عنوان الشهادة" DN، أدخل اسم المجال المؤهل بالكامل (FQDN) الذي سيتم إستخدامه للاتصال بواجهة إنهاء شبكة VPN.**CN=sslvpn.cisco.com**
10. انقر فوق **خيارات متقدمة**، وأدخل FQDN المستخدم لحقل DN لموضوع الشهادة.على سبيل المثال، :**FQDN** sslvpn.cisco.com
11. وانقر فوق **OK**.
12. حدد خانة الاختيار **إنشاء شهادة موقعة ذاتيا**، وانقر **إضافة شهادة**.
13. وانقر فوق **OK**.
14. انقر فوق **تكوين**، ثم انقر فوق **شبكة VPN للوصول عن بعد**.
15. قم بتوسيع **المتقدم**، واختر **إعدادات SSL**.
16. أخترت في الشهادات منطقة، القارن أن يكون استعملت أن ينهي ال SSL VPN (خارج)، وطقطقة **يحرر**.
17. في القائمة المنسدلة ترخيص، أختر الشهادة الموقعة ذاتيا التي قمت بتوليدها سابقا.
18. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.

مثال على سطر الأوامر

سيسكوسا

```
ciscoasa(config)#crypto key generate rsa label sslvpnkeypair
INFO: The name for the keys will be: sslvpnkeypair
...Keypair generation process begin. Please wait
Generate an RSA key for the certificate. (The name ---!
    should be unique. !--- For example, sslvpnkeypair.)
ciscoasa(config)#crypto ca trustpoint localtrust
    Create a trustpoint for the self-issued ---!
certificate. ciscoasa(config-ca-trustpoint)#enrollment self
ciscoasa(config-ca-trustpoint)#fqdn sslvpn.cisco.com
ciscoasa(config-ca-trustpoint)#subject-name CN=sslvpn.cisco.com
  The fully qualified domain name is used for both ---!
   fqdn and CN. !--- The name should resolve to the ASA
    outside interface IP address. ciscoasa(config-ca-
trustpoint)#keypair sslvpnkeypair
    The RSA key is assigned to the trustpoint for ---!
        certificate creation. ciscoasa(config-ca-
trustpoint)#crypto ca enroll localtrust noconfirm
The fully-qualified domain name in the certificate %
will be: sslvpn.cisco.com
ciscoasa(config)# ssl trust-point localtrust outside
    Assign the trustpoint to be used for SSL ---!
.connections on the outside interface
```

الخطوة 2. تحميل صورة عميل SSL VPN والتعرف عليها

يستخدم هذا المستند عميل AnyConnect SSL 2.0. يمكنك الحصول على هذا العميل على موقع تنزيل برامج Cisco على الويب. يلزم توفر صورة منفصلة في AnyConnect لكل نظام تشغيل يخطط المستخدمون البعيدين

لاستخدامها. لمزيد من المعلومات، ارجع إلى ملاحظات الإصدار Cisco AnyConnect 2.0.

بمجرد حصولك على عميل AnyConnect، أكمل الخطوات التالية:

إجراء ASDM

1. انقر فوق **تكوين**، ثم انقر فوق **شبكة VPN للوصول عن بعد**.
2. قم بتوسيع **الوصول إلى الشبكة (العميل)**، ثم قم بتوسيع **المتقدم**.
3. قم بتوسيع **SSL VPN**، واختر **إعدادات العميل**.
4. في منطقة صور عميل SSL VPN، انقر فوق **إضافة**، ثم انقر فوق **تحميل**.
5. استعرض الموقع الذي قمت فيه بتنزيل عميل AnyConnect.
6. حدد الملف، وانقر **تحميل الملف**.بمجرد تحميل العميل، تتلقى رسالة تفيد بأن الملف تم تحميله إلى flash بنجاح.
7. وانقر فوق **OK**.يظهر مربع حوار لتأكيد أنك تريد إستخدام الصورة التي تم تحميلها حديثا كصورة عميل SSL VPN الحالية.
8. وانقر فوق **OK**.
9. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.
10. كرر الخطوات الواردة في هذا القسم لكل حزمة AnyConnect خاصة بنظام التشغيل تريد إستخدامها.

مثال على سطر الأوامر

سيسكوسا

```
ciscoasa(config)#copy tftp://192.168.50.5/anyconnect-
                                win-2.0.0343-k9.pkg flash

        ?[Address or name of remote host [192.168.50.5

     ?[Source filename [anyconnect-win-2.0.0343-k9.pkg

  ?[Destination filename [anyconnect-win-2.0.0343-k9.pkg

  Accessing tftp://192.168.50.5/anyconnect-win-2.0.0343-
                                !!!!!!!!!!!!!...k9.pkg
   ...Writing file disk0:/anyconnect-win-2.0.0343-k9.pkg
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
                                !!!!!!!!!!!!!!!!!!!!
   (bytes copied in 4.480 secs (658933 bytes/sec 2635734
    AnyConnect image is downloaded to ASA via TFTP. ---!
                                ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#svc image disk0:/anyconnect-win-
                                2.0.0343-k9.pkg 1
   Specify the AnyConnect image to be downloaded by ---!
users. The image that is !--- downloaded the most should
  have the lowest number. This image uses 1 for the !---
                                .AnyConnect Windows image
```

الخطوة 3. تمكين الوصول إلى AnyConnect

للسماح لعميل AnyConnect بالاتصال ب ASA، يجب عليك تمكين الوصول على الواجهة التي تنهي إتصالات SSL VPN. يستخدم هذا المثال الواجهة الخارجية لإنهاء إتصالات AnyConnect.

إجراء ASDM

1. انقر فوق **تكوين**، ثم انقر فوق **شبكة VPN للوصول عن بعد**.
2. قم بتوسيع **الوصول إلى الشبكة (العميل)**، ثم أختر **توصيفات توصيل SSL VPN**.

3. حدد خانة الاختيار **enable Cisco AnyConnect VPN Client**.
4. حدد خانة الاختيار **السماح بالوصول** للواجهة الخارجية، وانقر **تطبيق**.

مثال على سطر الأوامر

سيسكوسا
ciscoasa(config)#**webvpn** ciscoasa(config-webvpn)#**enable outside** ciscoasa(config-webvpn)#**svc enable** *Enable AnyConnect to be downloaded to remote ---!* *.computers*

الخطوة 4. إنشاء نهج مجموعة جديد

يحدد نهج المجموعة معلمات التكوين التي يجب تطبيقها على العملاء عند إتصالهم. يقوم هذا المثال بإنشاء نهج مجموعة باسم *SSLClientPolicy*.

إجراء ASDM

1. انقر فوق **تكوين**، ثم انقر فوق **شبكة VPN للوصول عن بعد**.
2. قم بتوسيع **الوصول إلى الشبكة (العميل)**، واختر **نهج المجموعة**.
3. انقر فوق **إضافة (Add)**.
4. أخترت **عام**، ودخلت **SSLClientPolicy** في الإسم مجال.
5. قم بإلغاء تحديد خانة الاختيار **Inherit** لتجمعات العناوين.
6. انقر فوق **تحديد**، ثم انقر فوق **إضافة**.يظهر مربع الحوار إضافة تجمع IP.
7. قم بتكوين تجمع العناوين من نطاق IP غير المستخدم حاليا على شبكتك.يستخدم هذا المثال القيم التالية:**الاسم**: SSLClientPool**عنوان IP الأولي**: 192.168.25.1**نهاية عنوان IP**: 192.168.25.50**قناع الشبكة الفرعية**: 255.255.255.0
8. وانقر فوق **OK**.
9. أخترت ال newly created بركة، وطقطقة **يعين**.
10. انقر فوق **موافق**، ثم انقر فوق **المزيد من الخيارات**.
11. قم بإلغاء تحديد خانة الاختيار **Inherit** لبروتوكولات **الاتصال النفقي**.
12. تحقق من **عميل SSL VPN**.
13. في الجزء الأيسر، أختر **الخوادم**.
14. قم بإلغاء تحديد خانة الاختيار **توريث** خوادم DNS، وأدخل عنوان IP الخاص بخادم DNS الداخلي الذي سيستخدمه عملاء AnyConnect.يستخدم هذا المثال *192.168.50.5*.
15. انقر فوق **المزيد من الخيارات**.
16. قم بإلغاء تحديد خانة الاختيار **Inherit** للمجال الافتراضي.
17. أدخل المجال المستخدم من قبل الشبكة الداخلية. على سبيل المثال، *tsweb.local* .
18. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.

مثال على سطر الأوامر

سيسكوسا
ciscoasa(config)#**ip local pool SSLClientPool** **192.168.25.1-192.168.25.50 mask 255.255.255.0** *Define the IP pool. The IP pool should be a range ---!* *of IP addresses !--- not already in use on the internal* *network.* ciscoasa(config)#**group-policy SSLClientPolicy** **internal** ciscoasa(config)#**group-policy SSLClientPolicy attributes**

```
ciscoasa(config-group-policy)#dns-server value
192.168.50.5
Specify the internal DNS server to be used. ---!
ciscoasa(config-group-policy)#vpn-tunnel-protocol svc
Specify VPN tunnel protocol to be used by the Group ---!
Policy. ciscoasa(config-group-policy)#default-domain
value tsweb.local
Define the default domain assigned to VPN users. ---!
ciscoasa(config-group-policy)#address-pools value
SSLClientPool
Assign the IP pool created to the SSLClientPolicy ---!
.group policy
```

تكوين تجاوز قائمة الوصول لاتصالات VPN

عند تمكين هذا الخيار، يمكنك السماح لعملاء SSL/IPsec بتجاوز قائمة الوصول إلى الواجهة.

إجراء ASDM

1. انقر فوق **تكوين**، ثم انقر فوق **شبكة VPN للوصول عن بعد**.
2. قم بتوسيع **الوصول إلى الشبكة (العميل)**، ثم قم بتوسيع **المتقدم**.
3. قم بتوسيع **SSL VPN**، واختر **قائمة الوصول إلى واجهة التجاوز**.
4. تأكد من تحديد خانة الاختيار **تمكين جلسات عمل SSL VPN و IPSec لتجاوز قوائم الوصول إلى الواجهة**، ثم انقر فوق **تطبيق**.

مثال على سطر الأوامر

سيسكوسا
`` ciscoasa(config)#sysopt connection permit-vpn Enable interface access-list bypass for VPN ---! connections. !--- This example uses the vpn-filter .command for access control #(ciscoasa(config-group-policy ```

الخطوة 6. إنشاء ملف تعريف اتصال ومجموعة أنفاق لاتصالات عميل AnyConnect

عندما يتصل عملاء VPN ب ASA، فإنهم يربطون بملف تعريف توصيل أو مجموعة نفق. يتم إستخدام مجموعة الأنفاق لتحديد معلمات الاتصال لأنواع محددة من إتصالات VPN، مثل IPsec L2L، والوصول عن بعد ل IPsec، و SSL بدون عملاء، و SSL للعميل.

إجراء ASDM

1. انقر فوق **تكوين**، ثم انقر فوق **شبكة VPN للوصول عن بعد**.
2. قم بتوسيع **الوصول إلى الشبكة (العميل)**، ثم قم بتوسيع **SSL VPN**.
3. أختر **توصيفات توصيل**، ثم انقر على **إضافة**.
4. أختر **أساسي**، وأدخل القيم التالية:**الاسم**: SSLClientProfile**المصادقة**: محلي**نهج المجموعة الافتراضي**: SSLClientPolicy
5. تأكد من تحديد خانة الاختيار **SSL VPN Client Protocol**.
6. في الجزء الأيسر، قم بتوسيع **المتقدم**، واختر **SSL VPN**.
7. تحت أسماء الاتصال المستعارة، انقر فوق **إضافة**، وأدخل اسما يمكن للمستخدمين إرفاق إتصالات VPN به. على سبيل المثال، *SSLVPNClient*.
8. انقر فوق **موافق**، ثم انقر فوق **موافق** مرة أخرى.

9. في أسفل نافذة ASDM، حدد خانة الاختيار **السماح للمستخدم بتحديد الاتصال، المعرف باسم مستعار في الجدول أعلاه في صفحة تسجيل الدخول**، وانقر فوق **تطبيق**.

مثال على سطر الأوامر

سيسكوسا

```
ciscoasa(config)#tunnel-group SSLClientProfile type
remote-access
Define tunnel group to be used for VPN remote ---!
access connections. ciscoasa(config)#tunnel-group
SSLClientProfile general-attributes
ciscoasa(config-tunnel-general)#default-group-policy
SSLCLientPolicy
ciscoasa(config-tunnel-general)#tunnel-group
SSLClientProfile webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias SSLVPNClient
enable
Assign alias for tunnel group. ciscoasa(config- ---!
tunnel-webvpn)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
Enable alias/tunnel group selection for SSL VPN ---!
.connections
```

الخطوة 7. تكوين إستثناء NAT لعملاء AnyConnect

يجب تكوين إستثناء NAT لأي عناوين IP أو نطاقات تريد السماح لعملاء SSL VPN بالوصول إليها. في هذا المثال، يحتاج عملاء SSL VPN إلى الوصول إلى IP الداخلي 192.168.50.5 فقط.

ملاحظة: في حالة عدم تمكين التحكم في NAT، لا تكون هذه الخطوة مطلوبة. أستخدم الأمر **show run nat-control** للتحقق. طقطقت in order to دقق من خلال ASDM، **تشكيل**، **جدار حماية**، واخترت **nat قاعدة**. في حالة تحديد خانة الاختيار **تمكين حركة مرور البيانات من خلال جدار الحماية بدون ترجمة العنوان**، يمكنك تخطي هذه الخطوة.

إجراء ASDM

1. طقطقت **تشكيل**، وبعد ذلك طقطقت **جدار حماية**.
2. أخترت **nat قاعدة**، وطقطقة **يضيف**.
3. أختر **إضافة قاعدة إستثناء nat**، وأدخل القيم التالية:**الإجراء**: إستثناء**الواجهة**: الداخلا**لمصدر**: 192.168.50.5**الوجهة**: 24/192.168.25.0**إتجاه إستثناء NAT**: إستثناء حركة مرور البيانات الصادرة من الواجهة 'داخل' إلى واجهات أمان أقل (الافتراضي)
4. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.

مثال على سطر الأوامر

سيسكوسا

```
ciscoasa(config)#access-list no_nat extended permit
ip host 192.168.50.5 192.168.25.0
255.255.255.0
Define access list to be used for NAT exemption. ---!
ciscoasa(config)#nat (inside) 0 access-list no_nat
Allow external connections to untranslated internal ---!
!--- addresses defined by access lisy no_nat.
#(ciscoasa(config
```

الخطوة 8. إضافة مستخدمين إلى قاعدة البيانات المحلية

إذا كنت تستخدم المصادقة المحلية (الافتراضية)، يجب عليك تحديد أسماء المستخدمين وكلمات المرور في قاعدة البيانات المحلية لمصادقة المستخدم.

إجراء ASDM

1. انقر فوق **تكوين**، ثم انقر فوق **شبكة VPN للوصول عن بعد**.
2. قم بتوسيع **إعداد AAA**، واختر **المستخدمين المحليين**.
3. انقر **إضافة**، وأدخل القيم التالية:**username**: ماثيو**كلمة المرور**: p@ssw0rd**تأكيد كلمة المرور**: p@ssw0rd
4. حدد الزر **No ASDM أو SSH أو Telnet أو** Radio **Console Access**.
5. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.
6. كرر هذه الخطوة للمستخدمين الإضافيين، ثم انقر فوق **حفظ**.

مثال على سطر الأوامر

سيسكوسا

```
ciscoasa(config)#username matthewp password p@ssw0rd
ciscoasa(config)#username matthewp attributes
ciscoasa(config-username)#service-type remote-access
Assign user remote access only. No SSH, Telnet, ---!
ASDM access allowed. ciscoasa(config-username)#write
memory
.Save the configuration ---!
```

التحقق من الصحة

أستخدم هذا القسم للتحقق من نجاح تكوين SSL VPN

الاتصال ب ASA مع عميل AnyConnect

قم بتثبيت العميل مباشرة على جهاز كمبيوتر، وتوصيله بواجهة ASA الخارجية، أو أدخل https وعنوان FQDN/IP الخاص ب ASA في مستعرض ويب. إذا كنت تستخدم مستعرض ويب، يقوم العميل بتثبيت نفسه عند تسجيل الدخول الناجح.

التحقق من إتصالات عميل SSL VPN

أستخدم الأمر **show vpn-sessionDB svc** للتحقق من عملاء SSL VPN المتصلين.

```
ciscoasa(config-group-policy)#show vpn-sessiondb svc

Session Type: SVC

Username     : matthewp              Index        : 6
Assigned IP  : 192.168.25.1          Public IP    : 172.18.12.111
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128            Hashing      : SHA1
Bytes Tx     : 35466                 Bytes Rx     : 27543
Group Policy : SSLClientPolicy       Tunnel Group : SSLClientProfile
Login Time   : 20:06:59 UTC Tue Oct 16 2007
Duration     : 0h:00m:12s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none
```

```
#(ciscoasa(config-group-policy
```

يقوم الأمر **vpn-sessiondb logoff name** username بتسجيل خروج المستخدمين حسب اسم المستخدم. يتم إرسال رسالة *إعادة تعيين المسؤول* إلى المستخدم عند قطع الاتصال.

```
ciscoasa(config)#vpn-sessiondb logoff name matthewp
[Do you want to logoff the VPN session(s)? [confirm
INFO: Number of sessions with name "matthewp" logged off : 1

#(ciscoasa(config
```

لمزيد من المعلومات حول عميل AnyConnect 2.0، ارجع إلى دليل مسؤول Cisco AnyConnect VPN.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر أستكشاف الأخطاء وإصلاحها (إختيارية)

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **debug webVPN svc 255** — يعرض رسائل تصحيح الأخطاء حول الاتصالات بعملاء SSL VPN عبر WebVPN.**تسجيل دخول AnyConnect بنجاح**

```
ciscoasa(config)#debug webvpn svc 255
.INFO: debug webvpn svc enabled at level 255
:ciscoasa(config)#ATTR_FILTER_ID: Name
                                    SSLVPNClientAccess
                                     Id: 1, refcnt: 1 ,
                                webvpn_rx_data_tunnel_connect
                               CSTP state = HEADER_PROCESSING
                                     ()http_parse_cstp_method
                        'input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1...
                                        ()webvpn_cstp_parse_request_field
  input: 'Host: 10.10.1.5' - !--- Outside IP of ASA Processing CSTP header line: 'Host:...
                                                                    '10.10.1.5
                                        ()webvpn_cstp_parse_request_field
  input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' - !--- AnyConnect Version...
 Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' Setting
 user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343' webvpn_cstp_parse_request_field()
                         ...input: 'Cookie: webvpn=3338474156@28672@1192565782@EFB9042D72C
                    63CE02164F790435897AC72EE70AE' Processing CSTP header line: 'Cookie:
webvpn=3338474156@28672@119 2565782@EFB9042D72C63CE02164F790435897AC72EE70AE' Found WebVPN
    cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C 63CE02164F790435897AC72EE70AE'
                    WebVPN Cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C63CE02
        164F790435897AC72EE70AE' IPADDR: '3338474156', INDEX: '28672', LOGIN: '1192565782'
webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Version: 1' Processing CSTP header line:
 'X-CSTP-Version: 1' Setting version to '1' webvpn_cstp_parse_request_field() ...input: 'X-
 CSTP-Hostname: wkstation1' - !--- Client desktop hostname Processing CSTP header line: 'X-
                                                    'CSTP-Hostname: wkstation1
                                                'Setting hostname to: 'wkstation1
                                                ()webvpn_cstp_parse_request_field
                                    'input: 'X-CSTP-Accept-Encoding: deflate;q=1.0...
                            'Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0
                                                ()webvpn_cstp_parse_request_field
                                                     'input: 'X-CSTP-MTU: 1206...
```

```
'Processing CSTP header line: 'X-CSTP-MTU: 1206
                                                ()webvpn_cstp_parse_request_field
                                             'input: 'X-CSTP-Address-Type: IPv4...
                                  'Processing CSTP header line: 'X-CSTP-Address-Type: IPv4
                                                ()webvpn_cstp_parse_request_field
          input: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451CB0948AFBE98296FD849...
          '49EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51
          Processing CSTP header line: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451C
          'B0948AFBE98296FD84949EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51
                                                ()webvpn_cstp_parse_request_field
          'input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA...
                :Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA
                                  'DES-CBC3-SHA:DES-CBC-SHA
                                                    Validating address: 0.0.0.0
                                                  CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.25.1/255.255.255.0 - !--- IP assigned from IP Pool CSTP
         state = HAVE_ADDRESS SVC: NP setup np_svc_create_session(0x7000, 0xD41612C8, TRUE)
webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn_put_uauth success!
  SVC IPv6 ACL Name: NULL SVC IPv6 ACL ID: -1 SVC: adding to sessmgmt SVC: Sending response
  Unable to initiate NAC, NAC might not be enabled or invalid policy CSTP state = CONNECTED
  webvpn_rx_data_cstp webvpn_rx_data_cstp: got internal message Unable to initiate NAC, NAC
                                                    might not be enabled or invalid policy
```

تسجيل الدخول إلى AnyConnect غير ناجح (كلمة مرور غير صحيحة)

```
                                                [webvpn_portal.c:ewaFormSubmit_webvpn_login[1808
                                                        ewaFormSubmit_webvpn_login: tgCookie = 0
                                                ewaFormSubmit_webvpn_login: cookie = d53d2990
                                                  ewaFormSubmit_webvpn_login: tgCookieSet = 0
                                                    ewaFormSubmit_webvpn_login: tgroup = NULL
                                                 [webvpn_portal.c:http_webvpn_kill_cookie[627
                                             [webvpn_auth.c:http_webvpn_pre_authentication[1905
                                  !(WebVPN: calling AAA with ewsContext (-717386088) and nh (-717388536
                                                    ...WebVPN: started user authentication
                                                  [webvpn_auth.c:webvpn_aaa_callback[4380
                                                            (WebVPN: AAA status = (REJECT
                                                [webvpn_portal.c:ewaFormSubmit_webvpn_login[1808
                                                        ewaFormSubmit_webvpn_login: tgCookie = 0
                                                ewaFormSubmit_webvpn_login: cookie = d53d2990
                                                  ewaFormSubmit_webvpn_login: tgCookieSet = 0
                                                    ewaFormSubmit_webvpn_login: tgroup = NULL
                                             [webvpn_auth.c:http_webvpn_post_authentication[1180
                                                        .WebVPN: user: (matthewp) rejected
                                              !http_remove_auth_handle(): handle 9 not found
                                            [webvpn_portal.c:ewaFormServe_webvpn_login[1749
                                                 [webvpn_portal.c:http_webvpn_kill_cookie[627
```

معلومات ذات صلة

- دليل مسؤول عميل AnyConnect VPN من Cisco، الإصدار 2.0
- ملاحظات الإصدار الخاصة بعميل AnyConnect VPN، الإصدار 2.0
- الدعم التقني والمستندات - Cisco Systems

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).