IP ف‌تاوه نيوكت لاثم ع‌م SSLVPN

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين هواتف IP عبر طبقة مآخذ التوصيل الآمنة VPN (SSL VPN)، المعروفة أيضا باسم WebVPN. يتم إستخدام إثنين من مديري الاتصالات الموحدة من Cisco (CallManager) وثلاثة أنواع من الشهادات مع هذا الحل. CallManager هي:

- برنامج CUCM (Cisco Unified Communications Manager)
- مدير الاتصالات الموحدة الفائق من Cisco (Cisco Unified CME)

أنواع الشهادات هي:

- شهادات موقعة ذاتيا
- شهادات الطرف الثالث، مثل Thawte، Entrust، و GoDaddy
- جهاز الأمان القابل للتكيف (ASA) شهادة المرجع المصدق (CA)/cisco IOS®

والمفتاح الذي يجب فهمه هو أنه بمجرد اكتمال التكوين على بوابة SSL VPN و CallManager، يجب عليك الانضمام إلى هواتف IP محليا. وهذا يمكن الهواتف من الانضمام إلى CUCM واستخدام معلومات VPN والشهادات الصحيحة. إذا لم يتم الانضمام إلى الهواتف محليا، فلن تتمكن من العثور على عبارة SSL VPN وليس لديها الشهادات الصحيحة لإكمال مصافحة SSL VPN.

أكثر التكوينات شيوعا هي CUCM/Unified CME مع شهادات ASA الموقعة ذاتيا وشهادات Cisco IOS الموقعة ذاتيا. وبالتالي، فهي الاسهل في التكوين.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco Unified Communications Manager (CUCM) أو Cisco Unified Communications Manager Express (Cisco Unified CME)
- SSL VPN (WebVPN)
- أجهزة الأمان المعدلة (ASA) Cisco Adaptive Security Appliances
- أنواع الشهادات، مثل التوقيع الذاتي، والطرف الثالث، وسلطات الشهادات

المكونات المستخدمة

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

- ترخيص ASA Premium.
- ترخيص هاتف AnyConnect VPN.
  - بالنسبة لإصدار ASA 8.0.x، يكون الترخيص هو AnyConnect for Linksys Phone.
  - بالنسبة لإصدار ASA 8.2.x أو إصدار أحدث، يكون الترخيص AnyConnect لهاتف Cisco VPN.
- عبارة SSL VPN: ASA 8.0 أو إصدار أحدث (مع AnyConnect لترخيص هاتف Cisco VPN)، أو برنامج Cisco IOS الإصدار 12.4T أو إصدار أحدث.
  - لا يتم دعم الإصدار 12.4T من برنامج Cisco IOS Software أو إصدار أحدث بشكل رسمي كما هو موثق في دليل تكوين SSL VPN.
  - في الإصدار M(1)15.0 من برنامج Cisco IOS Software، تعد بوابة SSL VPN ميزة ترخيص محسوبة بعدد المقاعد على الأنظمة الأساسية Cisco 880 و Cisco 890 و Cisco 1900 و Cisco 2900 و Cisco 3900. مطلوب ترخيص صالح لجلسة عمل SSL VPN ناجحة.
- CallManager: CUCM 8.0.1 أو إصدار أحدث أو Unified CME 8.5 أو إصدار أحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

ملاحظات:

استخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المُستخدمة في هذا القسم.

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

تكوين ASA SSL VPN الأساسي

يتم وصف تكوين ASA SSL VPN الأساسي في هذه المستندات:

- ASA 8.x: وصول VPN مع عميل AnyConnect VPN باستخدام مثال تكوين شهادة موقعة ذاتيا
- تكوين إتصالات عميل AnyConnect VPN

وبمجرد اكتمال هذا التكوين، يجب أن يكون كمبيوتر الاختبار عن بعد قادرا على الاتصال ببوابة VPN الخاصة ب SSL، والاتصال عبر AnyConnect، واختبار اتصال CUCM. تأكد من أن ASA لديه ترخيص هاتف AnyConnect لهاتف Cisco IP. (أستخدم الأمر **show ver**.) يجب أن يكون كلا من منفذ TCP و 443 UDP مفتوحا بين البوابة والعميل.

ملاحظة: لا يتم دعم SSL VPN المتوازن للحمولة لهواتف VPN.

CUCM: ASA SSL VPN مع تكوين الشهادات الموقعة ذاتيا

ارجع إلى IP Phone SSL VPN إلى ASA باستخدام AnyConnect للحصول على معلومات أكثر تفصيلا.

يجب أن يكون لدى ASA ترخيص ل AnyConnect لهاتف Cisco VPN. عقب يشكل أنت ال SSL VPN، أنت بعد ذلك شكلت ك CUCM ل ال VPN.

1. أستخدم هذا الأمر لتصدير الشهادة الموقعة ذاتيا من ASA:

```
ciscoasa(config)# crypto ca export trustpoint name identity-certificate
```

يعرض هذا الأمر شهادة هوية مرمزة بترميز PEM إلى الوحدة الطرفية.

2. انسخ الشهادة ولصقها في محرر نصوص، واحفظها كملف .pem. تأكد من تضمين "شهادة البدء" و"بنود شهادة النهاية"، وإلا فلن يتم إستيراد الشهادة بشكل صحيح. لا تقم بتعديل تنسيق الشهادة لأن ذلك سيؤدي إلى حدوث مشاكل عندما يحاول الهاتف المصادقة على ASA.
3. انتقل إلى **Cisco Unified Operating System Administration (إدارة نظام التشغيل الموحد من Cisco) > Security (الأمان) > Certificate Management (إدارة الشهادات) > Upload Certificate (تحميل الشهادة/سلسلة الشهادات)** لتحميل ملف الشهادة إلى قسم إدارة الشهادات في CUCM.
4. قم بتنزيل شهادات CallManager.pem و CAPF.pem و Cisco_Manufacturing_CA.pem من نفس المنطقة المستخدمة لتحميل الشهادات الموقعة ذاتيا من ASA (راجع الخطوة 1)، واحفظها على سطح المكتب الخاص بك.
1. على سبيل المثال، إستيراد CallManager.pem إلى ASA، أستخدم الأوامر التالية:

```
ciscoasa(config)# crypto ca trustpoint certificate-name
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate certificate-name
```

2. عندما يطلب منك نسخ ولصق الشهادة المقابلة ل the trustPoint، افتح الملف الذي قمت بحفظه من CUCM، ثم انسخ والصق الشهادة التي ترمز Base64. تأكد من تضمين علامات البداية وأسطر شهادة النهاية (مع الواصلات).
3. اكتب **end**، ثم اضغط على **Return**.
4. عندما يطلب منك قبول الشهادة، اكتب **نعم**، ثم اضغط على مفتاح **Enter**.
5. كرر الخطوات من 1 إلى 4 للشهادتين الأخريين (CAPF.pem، Cisco_MANUFACTURING_CA.pem) من CUCM.
5. قم بتكوين CUCM لتكوينات VPN الصحيحة، كما هو موضح في CUCM IPphone VPN config.pdf.

ملاحظة: يجب أن تطابق بوابة شبكة VPN التي تم تكوينها على CUCM عنوان URL الذي تم تكوينه على بوابة VPN. إذا لم تتطابق البوابة مع URL، فلن يتمكن الهاتف من حل العنوان ولن ترى أي تصحيح أخطاء

على بوابة VPN.

- على CUCM: عنوان URL لبوابة VPN هو https://192.168.1.1/VPNPhone
- على ال ASA، استعملت هذا أمر:

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group VPNPhones webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://192.168.1.1/VPNPhone
enable
ciscoasa(config-tunnel-webvpn)# exit
```

- يمكنك إستخدام هذه الأوامر على إدارة أجهزة الأمان المعدلة (ASDM) أو تحت ملف تعريف الاتصال.

CUCM: ASA SSL VPN مع تكوين شهادات الطرف الثالث

هذا تشكيل جدا مماثل إلى التشكيل يصف في CUCM: ASA SSLVPN مع قسم تكوين الشهادات الموقعة ذاتيا، ماعدا أن أنت تستخدم شهادات من طرف ثالث. قم بتكوين SSL VPN على ASA باستخدام شهادات الطرف الثالث كما هو موضح في ASA 8.x، قم بتثبيت شهادات مورد الطرف الثالث يدويا لاستخدامها مع مثال تكوين WebVPN.

ملاحظة: يجب عليك نسخ سلسلة الشهادات الكاملة من ASA إلى CUCM وتضمين جميع الشهادات المتوسطة والجذرية. إذا لم يتضمن CUCM السلسلة الكاملة، فإن الهواتف لا تحتوي على الشهادات اللازمة للمصادقة وستفشل في مصافحة SSL VPN.

تكوين IOS SSL VPN الأساسي

ملاحظة: يتم تخصيص هواتف بروتوكول الإنترنت (IP) على أنها غير مدعومة في الشبكة الخاصة الظاهرية (VPN) الخاصة بنظام التشغيل IOS SSL؛ ويتم إجراء التكوينات في أفضل الجهود فقط.

يتم وصف تكوين Cisco IOS SSL VPN الأساسي في هذه المستندات:

- SSL VPN Client (SVC) على IOS مع مثال تكوين SDM
- مثال تكوين جدار حماية السياسة المستند إلى منطقة IOS لعميل AnyConnect VPN على موجه IOS

وبمجرد اكتمال هذا التكوين، يجب أن يكون كمبيوتر الاختبار عن بعد قادرا على الاتصال ببوابة VPN الخاصة ب SSL، والاتصال عبر AnyConnect، واختبار اتصال CUCM. في Cisco IOS 15.0 والإصدارات الأحدث، يجب أن يكون لديك ترخيص SSL VPN صالح لإكمال هذه المهمة. يجب أن يكون كلا من منفذ TCP و 443 UDP مفتوحا بين البوابة والعميل.

CUCM: IOS SSL VPN مع تكوين الشهادات الموقعة ذاتيا

هذا التكوين مماثل للتكوين الموضح في CUCM: ASA SSLVPN مع تكوين شهادات الطرف الثالث وCUCM: ASA SSLVPN مع أقسام تكوين الشهادات الموقعة ذاتيا. والاختلافات هي:

1. أستخدم هذا الأمر لتصدير الشهادة الموقعة ذاتيا من الموجه:

```
R1(config)# crypto pki export trustpoint-name pem terminal
```

2. أستخدم هذه الأوامر لاستيراد شهادات CUCM:

```
R1(config)# crypto pki trustpoint certificate-name
R1(config-ca-trustpoint)# enrollment terminal
R1(config)# crypto ca authenticate certificate-name
```

يجب أن يعرض تكوين سياق WebVPN هذا النص:

```
gateway webvpn_gateway domain VPNPhone
```

قم بتكوين CUCM كما هو موضح في CUCM: ASA SSLVPN مع قسم تكوين الشهادات الموقعة ذاتيا.

CUCM: IOS SSL VPN مع تكوين شهادات الطرف الثالث

هذا تشكيل مماثل إلى التشكيل يصف في CUCM: ASA SSLVPN مع قسم تكوين الشهادات الموقعة ذاتيا. قم بتكوين WebVPN باستخدام شهادة جهة خارجية.

ملاحظة: يجب نسخ سلسلة شهادات WebVPN الكاملة إلى CUCM وتضمين جميع الشهادات المتوسطة والجذرية. إذا لم يتضمن CUCM السلسلة الكاملة، فإن الهواتف لا تحتوي على الشهادات اللازمة للمصادقة وستفشل في مصافحة SSL VPN.

Unified CME: ASA/Router SSL VPN مع شهادات موقعة ذاتيا/تكوين شهادات من أطراف ثالثة

تكوين CME الموحد مماثل لتكوينات CUCM، على سبيل المثال، تكوينات نقطة نهاية WebVPN هي نفسها. يكمن الاختلاف الوحيد المهم في تكوينات وكيل الاتصال الموحد لإدارة البنية الأساسية (CME). قم بتكوين مجموعة VPN ونهج VPN ل CME الموحد كما هو موضح في تكوين عميل SSL VPN لهواتف IP SCCP.

ملاحظة: يدعم CME الموحد بروتوكول التحكم في المكالمات (SCCP) Skinny فقط ولا يدعم بروتوكول بدء جلسة عمل (SIP) لهواتف VPN.

ملاحظة: لا حاجة لتصدير الشهادات من نظام CME الموحد إلى ASA أو الموجه. تحتاج فقط إلى تصدير الشهادات من بوابة ASA أو WebVPN للموجه إلى CME الموحد.

لتصدير الشهادات من بوابة WebVPN، ارجع إلى قسم ASA/الموجه. إذا كنت تستخدم شهادة من طرف خارجي، يجب أن تقوم بتضمين سلسلة الشهادات الكاملة. لاستيراد الشهادات إلى CME الموحد، أستخدم الطريقة نفسها المستخدمة لاستيراد الشهادات إلى موجه:

```
CME(config)# crypto pki trustpoint certificate-name
CME(config-ca-trustpoint)# enrollment terminal
CME(config)# crypto ca authenticate certificate-name
```

هواتف IP UC 520 مع تكوين SSL VPN

يختلف هاتف بروتوكول الإنترنت Cisco Unified Communications 500 Series UC 520 IP Phone تماما عن تكوينات CUCM و CME.

- بما أن هاتف IP UC 520 هو كل من CallManager وبوابة WebVPN، فلا حاجة لتكوين الشهادات بين الاثنين.

- قم بتكوين WebVPN على موجه كما تفعل عادة باستخدام شهادات موقعة ذاتيا أو شهادات من جهات خارجية.
- يحتوي هاتف بروتوكول الإنترنت UC 520 IP على عميل WebVPN مدمج، ويمكنك تكوينه بنفس الطريقة التي تقوم بها بتكوين جهاز كمبيوتر عادي للاتصال بشبكة WebVPN. أدخل البوابة، ثم مجموعة اسم المستخدم/كلمة المرور.
- هاتف بروتوكول الإنترنت UC 520 IP متوافق مع هواتف SPA 525G لهاتف Cisco Small Business IP.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

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).