تكوين VPDN للطلب الهاتفي باستخدام TACACS+ ومجموعات VPDN

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
التكوين
الرسم التخطيطي للشبكة
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
أوامر استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يقدم هذا المستند نموذجا لتكوين شبكات الاتصال الخاصة الظاهرية (VPDN) للطلب الهاتفي، باستخدام مجموعات VPDN ونظام التحكم في الوصول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+) الإضافي.

المتطلبات الأساسية

المتطلبات

قبل محاولة هذا التكوين، تأكد من استيفاء المتطلبات التالية:

تحتاج إلى:

- موجه من Cisco للوصول إلى العميل (NAS/LAC)، وموجه Cisco للوصول إلى الشبكة (HGW/LNS) مع اتصال IP بينهما.
- أسماء الأجهزة المضيفة للموجهات، أو الأسماء المحلية التي سيتم إستخدامها على مجموعات VPDN.
- بروتوكول الاتصال النفقي المطلوب إستخدامه. هذا يستطيع كنت إما طبقة 2 L2T) tunneling) بروتوكول، أو طبقة 2 L2F) forwarding) بروتوكول.
- كلمة مرور للموجهات لمصادقة النفق.
- معيار الاتصال النفقي. قد يكون هذا اسم المجال أو خدمة التعرف على الرقم المطلوب (DNIS).
- أسماء المستخدمين وكلمات المرور الخاصة بالمستخدم (طلب العميل للدخول).
- عناوين ومفاتيح IP لخوادم TACACS+ لديك.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

معلومات أساسية

للحصول على مقدمة مفصلة لشبكات الاتصال الخاصة الظاهرية (VPDN) ومجموعات VPDN، راجع فهم VPDN. يتوسع هذا المستند في تكوين VDPN، ويضيف نظام التحكم في الوصول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+) الإضافي.

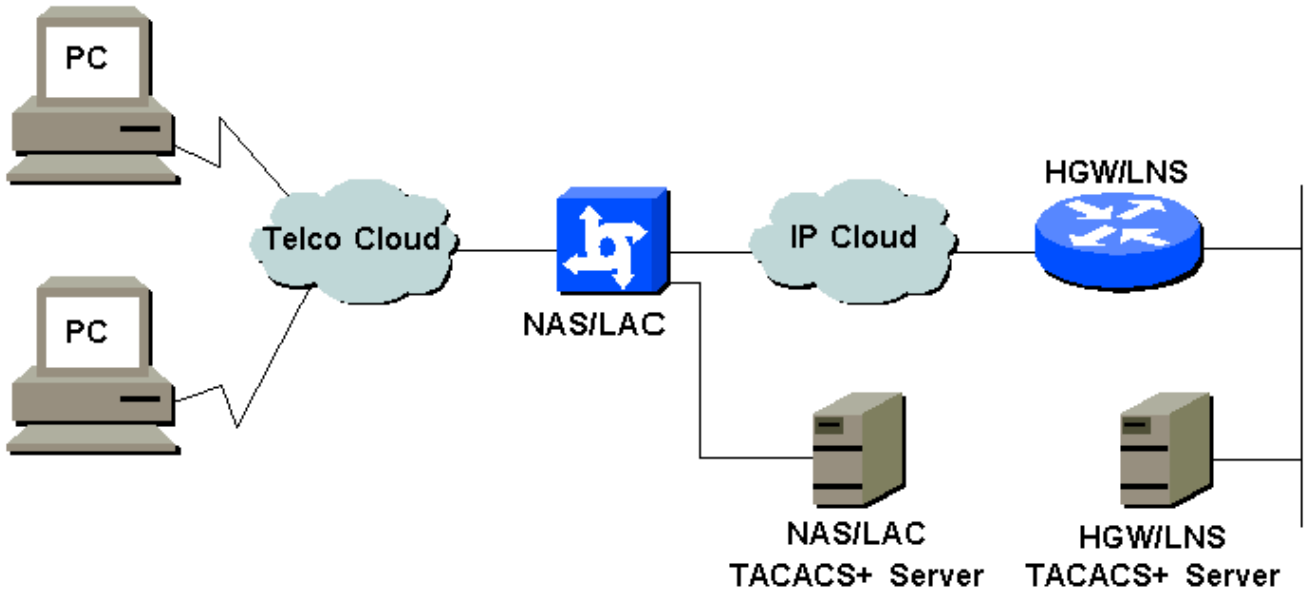
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- وحدة التخزين المتصلة بالشبكة/منطقة أمريكا اللاتينية والكاريبي HGW/LNS
- ملف تكوين NAS/LAC TACACS+
- ملف تكوين TACACS+ ل HGW/LNS

وحدة التخزين المتصلة بالشبكة/منطقة أمريكا اللاتينية والكاريبي

```
!
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname as5300
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
+aaa authentication ppp default if-needed group tacacs
+aaa authorization network default group tacacs
enable password somethingSecret
!
username john password 0 secret4me
!
ip subnet-zero
!
vpdn enable
!
isdn switch-type primary-5ess
!
controller T1 0
framing esf
clock source line primary
linecode b8zs
pri-group timeslots 1-24
!
controller T1 1
framing esf
clock source line secondary 1
linecode b8zs
pri-group timeslots 1-24
!
controller T1 2
framing esf
linecode b8zs
pri-group timeslots 1-24
!
controller T1 3
framing esf
linecode b8zs
pri-group timeslots 1-24
!
interface Ethernet0
ip address 172.16.186.52 255.255.255.240
no ip directed-broadcast
!
interface Serial023
no ip address
no ip directed-broadcast
encapsulation ppp
ip tcp header-compression passive
```

```
                                dialer rotary-group 1
                            isdn switch-type primary-5ess
                                isdn incoming-voice modem
                                        no cdp enable
                                                      !
                                     interface Serial123
                                          no ip address
                                 no ip directed-broadcast
                                       encapsulation ppp
                            ip tcp header-compression passive
                                        dialer rotary-group 1
                                isdn switch-type primary-5ess
                                    isdn incoming-voice modem
                                        no cdp enable
                                                      !
                                     interface Serial223
                                          no ip address
                                 no ip directed-broadcast
                                       encapsulation ppp
                            ip tcp header-compression passive
                                        dialer rotary-group 1
                                isdn switch-type primary-5ess
                                    isdn incoming-voice modem
                                        no cdp enable
                                                      !
                                     interface Serial323
                                          no ip address
                                 no ip directed-broadcast
                                       encapsulation ppp
                            ip tcp header-compression passive
                                        dialer rotary-group 1
                                isdn switch-type primary-5ess
                                    isdn incoming-voice modem
                                        no cdp enable
                                                      !
                                   interface FastEthernet0
                                          no ip address
                                 no ip directed-broadcast
                                               shutdown
                                                      !
                                   interface Group-Async1
                                  ip unnumbered Ethernet0
                                 no ip directed-broadcast
                                       encapsulation ppp
                            ip tcp header-compression passive
                                     async mode interactive
                    peer default ip address pool IPaddressPool
                                        no cdp enable
                                  ppp authentication chap
                                         group-range 1 96
                                                      !
                                     interface Dialer1
                                  ip unnumbered Ethernet0
                                 no ip directed-broadcast
                                       encapsulation ppp
                            ip tcp header-compression passive
                                           dialer-group 1
                    peer default ip address pool IPaddressPool
                                        no cdp enable
                                  ppp authentication chap
                                                      !
ip local pool IPaddressPool 10.10.10.1 10.10.10.254
                                       no ip http server
                                          ip classless
```

```
ip route 0.0.0.0 0.0.0.0 172.16.186.49
!
tacacs-server host 172.16.171.9
tacacs-server key 2easy
!
line con 0
login authentication CONSOLE
transport input none
line 1 96
autoselect during-login
autoselect ppp
modem Dialin
line aux 0
line vty 0 4
!
end
```

HGW/LNS

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
!
hostname access-9
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
+aaa authentication ppp default if-needed group tacacs
+aaa authorization network default group tacacs
enable password somethingSecret
!
ip subnet-zero
!
vpdn enable
!
vpdn-group DEFAULT
Default L2TP VPDN group !
accept-dialin
protocol any
virtual-template 1
local name LNS
lcp renegotiation always
l2tp tunnel password 0 not2tell
!
vpdn-group POP1
accept-dialin
protocol l2tp
virtual-template 2
terminate-from hostname LAC
local name LNS
l2tp tunnel password 0 2secret
!
vpdn-group POP2
accept-dialin
protocol l2f
virtual-template 3
terminate-from hostname NAS
local name HGW
lcp renegotiation always
!
```

```
                                interface FastEthernet0/0
                 ip address 172.16.186.1 255.255.255.240
                                no ip directed-broadcast
                                                      !
                                interface Virtual-Template1
                          ip unnumbered FastEthernet0/0
                                no ip directed-broadcast
                      ip tcp header-compression passive
            peer default ip address pool IPaddressPool
                                 ppp authentication chap
                                                      !
                                interface Virtual-Template2
                                 ip unnumbered Ethernet0/0
                                no ip directed-broadcast
                      ip tcp header-compression passive
          peer default ip address pool IPaddressPoolPOP1
                                              compress stac
                                 ppp authentication chap
                                                      !
                                interface Virtual-Template3
                                 ip unnumbered Ethernet0/0
                                no ip directed-broadcast
                      ip tcp header-compression passive
          peer default ip address pool IPaddressPoolPOP2
                                 ppp authentication pap
                                          ppp multilink
                                                      !
     ip local pool IPaddressPool 10.10.10.1 10.10.10.254
     ip local pool IPaddressPoolPOP1 10.1.1.1 10.1.1.254
     ip local pool IPaddressPoolPOP2 10.1.2.1 10.1.2.254
                                             ip classless
                                       no ip http server
                                                      !
                           tacacs-server host 172.16.186.9
                           tacacs-server key not2difficult
                                                      !
                                         line con 0

                              login authentication CONSOLE
                                      transport input none
                                               line 97 120
                                                line aux 0
                                              line vty 0 4
                                                      !
                                                      !
                                                    end
```

ملف تكوين NAS/LAC TACACS+

```
                                             key = 2easy

    Use L2TP tunnel to 172.16.186.1 when 4085555100 is #
                                                  dialed
                                 } user = dnis:4085555100
                 } service = ppp protocol = vpdn
                                tunnel-id = anonymous
                   ip-addresses = 172.16.186.1
                                    tunnel-type = l2tp
                                                 {
                                                   {

                      Password for tunnel authentication #
```

```
                                        } user = anonymous
                      chap = cleartext not2tell
                                              {

                                                  ###

    Use L2TP tunnel to 172.16.186.1 when 4085555200 is #
                                                    dialed
                                  } user = dnis:4085555200
                } service = ppp protocol = vpdn
                              tunnel-id = LAC
                  ip-addresses = 172.16.186.1
                           tunnel-type = l2tp
                                           {
                                             {

                    Password for tunnel authentication #
                                           } user = LAC
                       chap = cleartext 2secret
                                              {

                                                  ###

Use L2F tunnel to 172.16.186.1 when user authenticates #
                                     with cisco.com domain
                                        } user = cisco.com
                } service = ppp protocol = vpdn
                              tunnel-id = NAS
                  ip-addresses = 172.16.186.1
                           tunnel-type = l2f
                                           {
                                             {

                    Password for tunnel authentication #
                                           } user = NAS
                         chap = cleartext cisco
                                              {

                    Password for tunnel authentication #
                                           } user = HGW
                         chap = cleartext cisco
                                              {
```

ملف تكوين TACACS+ ل HGW/LNS

```
                                     key = not2difficult

                    Password for tunnel authentication #
                                           } user = NAS
                         chap = cleartext cisco
                                              {

                    Password for tunnel authentication #
                                           } user = HGW
                         chap = cleartext cisco
                                              {

                                    } user = santiago
                       chap = cleartext letmein

                { } service = ppp protocol = lcp
                 { } service = ppp protocol = ip
```

```
                                                {

                                    } user = santiago@cisco.com
                                global = cleartext letmein

                                { } service = ppp protocol = lcp
                            { } service = ppp protocol = multilink
                                   { } service = ppp protocol = ip
                                                {
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- **show vpdn tunnel all**—يعرض تفاصيل جميع الأنفاق النشطة.
- **show user**—يعرض اسم المستخدم المتصل.
- **show interface virtual-access #**— يمكنك من التحقق من حالة واجهة ظاهرية معينة على HGW/LNS.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، راجع المعلومات المهمة في أوامر تصحيح الأخطاء.

- **debug vpdn l2x-events**—يعرض الحوار بين NAS/LAC و HGW/LNS لإنشاء نفق أو جلسة.
- **debug ppp authentication**—يتيح لك التحقق مما إذا كان العميل يمر بالمصادقة.
- **debug ppp negotiation**—يتيح لك التحقق مما إذا كان العميل يمر عبر تفاوض PPP. ويمكنك أن ترى أي خيارات (مثل الاستدعاء، والشبكة متعددة المستويات (MLP)، وما إلى ذلك)، وأي بروتوكولات (مثل IP و IPX، وما إلى ذلك) يتم التفاوض عليها.
- **تصحيح أخطاء PPP**—يعرض أخطاء البروتوكول وإحصائيات الخطأ، المرتبطة بالتفاوض حول اتصال PPP وتشغيله.
- **debug vtemplate**— يعرض إستنساخ واجهات الوصول الظاهرية على HGW/LNS. يمكنك الاطلاع على وقت إنشاء الواجهة (المنسوخة من القالب الظاهري) في بداية اتصال الاتصال، وعندما يتم تدمير الواجهة عند قطع الاتصال.
- **debug aaa authentication**—يمكنك من التحقق من مصادقة المستخدم أو النفق بواسطة خادم المصادقة والتفويض والمحاسبة (AAA).
- **تخويل تصحيح الأخطاء AAA**—يمكنك من التحقق من تخويل المستخدم بواسطة خادم AAA.
- **debug aaa لكل مستخدم** — يمكنك من التحقق من ما يتم تطبيقه على كل مستخدم تمت مصادقته. يختلف هذا عن تصحيح الأخطاء العامة المذكورة أعلاه.

معلومات ذات صلة

- صفحات دعم التقنية - الطلب

- الدعم الفني - 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).