

مدخلات سواب Dynamic Multipoint VPN نيوكت GRE و NAT و EIGRP عم IPsec ربع GRE

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [التكوينات](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [أوامر استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يقدم هذا المستند نموذجاً لتكوين شبكة VPN الديناميكية متعددة النقاط المتصلة بالشبكة (DMVPN) باستخدام تضمين التوجيه العام (GRE) عبر IPsec مع بروتوكول توجيه العبارة الداخلي المحسن (EIGRP) وترجمة عنوان الشبكة (NAT) والتحكم في الوصول المستند إلى السياق (CBAC).

المتطلبات الأساسية

المتطلبات

قبل إنشاء نفق GRE متعدد النقاط (mGRE) و IPsec، يجب تحديد سياسة تبادل مفتاح الإنترنت (IKE) باستخدام أمر سياسة التشفير isakmp.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، استخدم [أداة بحث الأوامر \(للعلماء المسجلين فقط\)](#).

المكونات المستخدمة

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

- برنامج Cisco IOS © الإصدار 12.2(15)T1 على الموجه الموجه الموجه و 12.3(1.6) على الموجهات عبر الإنترنت
- الموجه Cisco 3620 كموجه محوري، موجهات Cisco 1720 وموجه Cisco 3620 واحد كموجهات يتم التحدث بها

تم إنشاء المعلومات المقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى [اصطلاحات تلميحات Cisco التقنية](#).

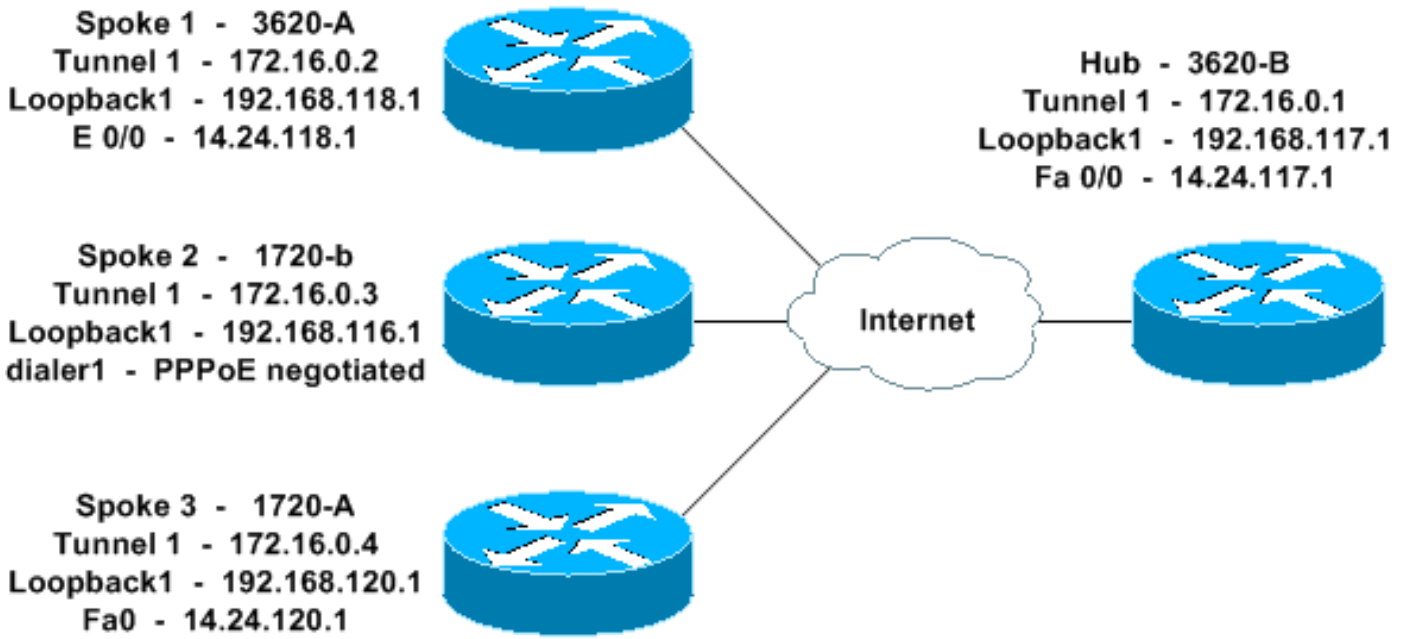
التكوين

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

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، استخدم [أداة بحث الأوامر \(للعلماء المسجلين فقط\)](#).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.



التكوينات

يستخدم هذا المستند التكوينات الموضحة أدناه.

- [الموزع - B-3620](#)
- [تحديث 1 - 3620 - ألف](#)
- [تكمم 2 - 1720-ب](#)
- [تكمم 3 - 1720 - ألف](#)

الموزع - B-3620

```
3620-B#write terminal
...Building configuration
```

```

Current configuration : 2607 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 3620-B
!
logging queue-limit 100
!
memory-size iomem 10
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
This is the CBAC configuration and what to inspect. ---!
!--- This will be applied outbound on the external
interface. ip inspect name in2out rcmd ip inspect name
in2out ftp ip inspect name in2out tftp ip inspect name
in2out tcp timeout 43200 ip inspect name in2out http ip
inspect name in2out udp ip audit po max-events 100 ! ! !
!--- Create an Internet Security Association and Key
Management !--- Protocol (ISAKMP) policy for Phase 1
negotiations. ! crypto isakmp policy 5 authentication
pre-share group 2 !--- Add dynamic pre-shared key. !---
Here "dmvpn" is the word that is used as the key. crypto
isakmp key dmvpnkey address 0.0.0.0 0.0.0.0 crypto
isakmp nat keepalive 20 ! ! !--- Create the Phase 2
policy for actual data encryption. crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
Create an IPSec profile to be applied dynamically !---
to the GRE over IPSec tunnels. crypto ipsec profile
dmvpnprof set transform-set dmvpnset ! ! no voice hpi
capture buffer no voice hpi capture destination ! ! mta
receive maximum-recipients 0 ! ! !--- This is the inside
interface. interface Loopback1 ip address 192.168.117.1
255.255.255.0 ip nat inside ! !--- This is the mGRE
interface for dynamic GRE tunnels. interface Tunnell
description MULTI-POINT GRE TUNNEL for BRANCHES
bandwidth 1000 ip address 172.16.0.1 255.255.255.0 no ip
redirects ip mtu 1400 ip nhrp authentication dmvpn ip
nhrp map multicast dynamic ip nhrp network-id 99 ip nhrp
holdtime 300 no ip split-horizon eigrp 1 no ip mroute-
cache delay 1000 tunnel source FastEthernet0/0 tunnel
mode gre multipoint tunnel key 100000 tunnel protection
ipsec profile dmvpnprof ! !--- This is the outside
interface. interface FastEthernet0/0 ip address
14.24.117.1 255.255.0.0 ip nat outside ip access-group
100 in ip inspect in2out out no ip mroute-cache duplex
auto speed auto ! interface Serial0/0 no ip address
shutdown clockrate 2000000 no fair-queue ! interface
FastEthernet0/1 no ip address no ip mroute-cache duplex
auto speed auto ! !--- Enable a routing protocol to
send/receive dynamic !--- updates about the private
networks over the tunnels. router eigrp 1 network
172.16.0.0 0.0.0.255 network 192.168.117.0 no auto-
summary ! !--- Perform NAT on local traffic !--- going
directly out FastEthernet0/0. ip nat inside source list
110 interface FastEthernet0/0 overload ip http server no
ip http secure-server ip classless ip route 0.0.0.0

```

```

0.0.0.0 14.24.1.1 ip route 2.0.0.0 255.0.0.0 14.24.121.1
!!! !--- Allow ISAKMP, ESP, and GRE traffic inbound.
!--- CBAC will open other inbound access as needed.
access-list 100 permit udp any host 14.24.117.1 eq 500
access-list 100 permit esp any host 14.24.117.1 access-
list 100 permit gre any host 14.24.117.1 access-list 100
deny ip any any access-list 110 permit ip 192.168.117.0
0.0.0.255 any !! call rsvp-sync !! mgcp profile
default ! dial-peer cor custom !! line con 0 exec-
timeout 0 0 line aux 0 line vty 0 4 login !! end 3620-
#B

```

تحدث 1 - 3620 - ألف

```

3620-A#write terminal
...Building configuration

Current configuration : 2559 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3620-A
!
boot system flash slot0:c3620-ik9o3s7-mz.122-15.T1.bin
logging queue-limit 100
!
memory-size iomem 15
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
This is the CBAC configuration and what to inspect. ---!
!--- This will be applied outbound on the external
interface. ip inspect name in2out rcmd ip inspect name
in2out tftp ip inspect name in2out udp ip inspect name
in2out tcp timeout 43200 ip inspect name in2out
realaudio ip inspect name in2out vdolive ip inspect name
in2out netshow ip audit po max-events 100 !!! !---
Create an ISAKMP policy for !--- Phase 1 negotiations.
crypto isakmp policy 5 authentication pre-share group 2
!--- Add dynamic pre-shared key. crypto isakmp key
dmvpnkey address 0.0.0.0 0.0.0.0 !! !--- Create the
Phase 2 policy for actual data encryption. crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
Create an IPSec profile to be applied dynamically !---
to the GRE over IPSec tunnels. crypto ipsec profile
dmvpnprof set transform-set dmvpnset !! no voice hpi
capture buffer no voice hpi capture destination !! mta
receive maximum-recipients 0 !! !--- This is the inside
interface. interface Loopback1 ip address 192.168.118.1
255.255.255.0 ip nat inside ! !--- This is the mGRE
interface for dynamic GRE tunnels. interface Tunnell
description HOST DYNAMIC TUNNEL bandwidth 1000 ip
address 172.16.0.2 255.255.255.0 no ip redirects ip mtu
1400 ip nhrp authentication dmvpn ip nhrp map 172.16.0.1
14.24.117.1 ip nhrp map multicast 14.24.117.1 ip nhrp
network-id 99 ip nhrp holdtime 300 ip nhrp nhs
172.16.0.1 no ip mroute-cache delay 1000 tunnel source

```

```

Ethernet0/0 tunnel mode gre multipoint tunnel key 100000
tunnel protection ipsec profile dmvpnprof ! !--- This is
the outside interface. interface Ethernet0/0 ip address
14.24.118.1 255.255.0.0 ip nat outside ip inspect in2out
out ip access-group 100 in no ip mroute-cache half-
duplex ! interface Ethernet0/1 no ip address half-duplex
! interface Ethernet0/2 no ip address shutdown half-
duplex ! interface Ethernet0/3 no ip address shutdown
half-duplex ! !--- Enable a routing protocol to
send/receive dynamic !--- updates about the private
networks over the tunnel. router eigrp 1 network
172.16.0.0 0.0.0.255 network 192.168.118.0 no auto-
summary ! !--- Perform NAT on local traffic !--- going
directly out Ethernet0/0. ip nat inside source list 110
interface Ethernet0/0 overload ip http server no ip http
secure-server ip classless ip route 0.0.0.0 0.0.0.0
14.24.1.1 ! ! !--- Allow ISAKMP, ESP, and GRE traffic
inbound. !--- CBAC will open inbound access as needed.
access-list 100 permit udp any host 14.24.118.1 eq 500
access-list 100 permit esp any host 14.24.118.1 access-
list 100 permit gre any host 14.24.118.1 access-list 100
deny ip any any access-list 110 permit ip 192.168.118.0
0.0.0.255 any ! ! call rsvp-sync ! ! mgcp profile
default ! dial-peer cor custom ! ! line con 0 exec-
timeout 0 0 line aux 0 line vty 0 4 login ! ! end 3620-
#A

```

تکلم 2 - 1720-ب

```

1720-b#write terminal
...Building configuration

Current configuration : 2543 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1720-b
!
boot system flash flash:c1700-ny-mz.122-8.YJ
logging queue-limit 100
enable password cisco
!
username 7206-B password 0 cisco
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
This is the CBAC configuration and what to inspect. ---!
!--- This will be applied outbound on the external
interface. ip inspect name in2out rcmd ip inspect name
in2out tftp ip inspect name in2out udp ip inspect name
in2out tcp timeout 43200 ip inspect name in2out
realaudio ip inspect name in2out vdolive ip inspect name
in2out netshow ip audit po max-events 100 ! ! vpdn-group
1 request-dialin protocol pppoe ! ! !--- Create an
ISAKMP policy for !--- Phase 1 negotiations. crypto
isakmp policy 5 authentication pre-share group 2 !---
Add dynamic pre-shared key. crypto isakmp key dmvpnkey

```

```

address 0.0.0.0 0.0.0.0 ! ! !--- Create the Phase 2
policy for actual data encryption. crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
Create an IPSec profile to be applied dynamically !---
to the GRE over IPSec tunnels. crypto ipsec profile
dmvpnprof set transform-set dmvpnset ! ! !--- This is
the inside interface. interface Loopback1 ip address
192.168.116.1 255.255.255.0 ip nat inside ! !--- This is
the mGRE interface for dynamic GRE tunnels. interface
Tunnel1 description HOST DYNAMIC TUNNEL bandwidth 1000
ip address 172.16.0.3 255.255.255.0 no ip redirects ip
mtu 1400 ip nhrp authentication dmvpn ip nhrp map
172.16.0.1 14.24.117.1 ip nhrp map multicast 14.24.117.1
ip nhrp network-id 99 ip nhrp holdtime 300 ip nhrp nhs
172.16.0.1 no ip mroute-cache delay 1000 tunnel source
Dialer1 tunnel mode gre multipoint tunnel key 100000
tunnel protection ipsec profile dmvpnprof ! interface
Ethernet0 no ip address half-duplex ! interface
FastEthernet0 no ip address no ip mroute-cache speed
auto pppoe enable pppoe-client dial-pool-number 1 ! !---
This is the outside interface. interface Dialer1 ip
address 2.2.2.10 255.255.255.0 ip inspect in2out out ip
access-group 100 in encapsulation ppp dialer pool 1
dialer-group 1 ppp authentication pap chap callin ! !---
Enable a routing protocol to send/receive dynamic !---
updates about the private networks. router eigrp 1
network 172.16.0.0 0.0.0.255 network 192.168.116.0 no
auto-summary ! !--- Perform NAT on local traffic !---
going directly out Dialer1. ip nat inside source list
110 interface Dialer1 overload ip classless ip route
0.0.0.0 0.0.0.0 Dialer1 no ip http server no ip http
secure-server ! ! ! !--- Allow ISAKMP, ESP, and GRE
traffic inbound. !--- CBAC will open inbound access as
needed. access-list 100 permit udp any host 14.24.116.1
eq 500 access-list 100 permit esp any host 14.24.116.1
access-list 100 permit gre any host 14.24.116.1 access-
list 100 deny ip any any access-list 110 permit ip
192.168.116.0 0.0.0.255 any dialer-list 1 protocol ip
permit ! ! ! line con 0 exec-timeout 0 0 line aux 0 line
#vty 0 4 login ! no scheduler allocate end 1720-b

```

تکلم 3 - 1720 - ألف

```

1720-A#write terminal
...Building configuration

Current configuration : 1770 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 1720-A
!
logging queue-limit 100
!
memory-size iomem 25
ip subnet-zero
!
!
!
ip cef

```

```

This is the CBAC configuration and what to inspect. ---!
!--- This will be applied outbound on the external
interface. ip inspect name in2out rcmd ip inspect name
in2out tftp ip inspect name in2out udp ip inspect name
in2out tcp timeout 43200 ip inspect name in2out
realaudio ip inspect name in2out vdolive ip inspect name
in2out netshow ip audit po max-events 100 ! ! !---
Create an ISAKMP policy for !--- Phase 1 negotiations.
crypto isakmp policy 5 authentication pre-share group 2
!--- Add dynamic pre-shared key. crypto isakmp key
dmvpnkey address 0.0.0.0 0.0.0.0 ! ! !--- Create the
Phase 2 policy for actual data encryption. crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
Create an IPSec profile to be applied dynamically !---
to the GRE over IPSec tunnels. crypto ipsec profile
dmvpnprof set transform-set dmvpnset ! ! !--- This is
the inside interface. interface Loopback1 ip address
192.168.120.1 255.255.255.0 ip nat inside ! !--- This is
the mGRE interface for dynamic GRE tunnels. interface
Tunnel1 description HOST DYNAMIC TUNNEL bandwidth 1000
ip address 172.16.0.4 255.255.255.0 no ip redirects ip
mtu 1400 ip nhrp authentication dmvpn ip nhrp map
172.16.0.1 14.24.117.1 ip nhrp map multicast 14.24.117.1
ip nhrp network-id 99 ip nhrp holdtime 300 ip nhrp nhs
172.16.0.1 no ip mroute-cache delay 1000 tunnel source
FastEthernet0 tunnel mode gre multipoint tunnel key
100000 tunnel protection ipsec profile dmvpnprof !
interface Ethernet0 no ip address no ip mroute-cache
half-duplex ! !--- This is the outside interface.
interface FastEthernet0 ip address 14.24.120.1
255.255.0.0 ip nat outside ip inspect in2out out ip
access-group 100 in no ip mroute-cache speed auto ! !---
Enable a routing protocol to send/receive dynamic !---
updates about the private networks. router eigrp 1
network 172.16.0.0 0.0.0.255 network 192.168.120.0 no
auto-summary ! !--- Perform NAT on local traffic !---
going directly out FastEthernet0. ip nat inside source
list 110 interface FastEthernet0 overload ip classless
ip route 0.0.0.0 0.0.0.0 14.24.1.1 no ip http server no
ip http secure-server ! ! ! !--- Allow ISAKMP, ESP, and
GRE traffic inbound. !--- CBAC will open inbound access
as needed. access-list 100 permit udp any host
14.24.116.1 eq 500 access-list 100 permit esp any host
14.24.116.1 access-list 100 permit gre any host
14.24.116.1 access-list 100 deny ip any any access-list
110 permit ip 192.168.120.0 0.0.0.255 any ! ! ! line con
0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! no
#scheduler allocate end 1720-A

```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك استخدامها 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 crypto isakmp sa** — يعرض حالة اقتران أمان (SA) (ISAKMP).
- **show crypto engine connections active** — يعرض إجمالي التشفير/فك التشفير لكل SA.
- **show crypto ipsa** — يعرض الإحصائيات على الأنفاق النشطة.

- `show ip route`—يعرض جدول التوجيه.
- `show ip eigrp neighbor`—يعرض جيران EIGRP.
- `show ip nhrp`—يعرض ذاكرة التخزين المؤقت لبروتوكول تحليل الخطوة التالية (NHRP) ل IP، والتي تقتصر اختياريًا على إدخالات ذاكرة التخزين المؤقت الديناميكية أو الثابتة لواجهة معينة.
- `show crypto socket`— يعرض جدول مأخذ التشفير بين NHRP و IPsec.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: قبل إصدار أوامر تصحيح الأخطاء، يرجى الاطلاع على [المعلومات المهمة في أوامر تصحيح الأخطاء](#).

- `debug crypto ipsec`—يعرض أحداث IPsec.
 - `debug crypto isakmp`—يعرض الرسائل المتعلقة بأحداث IKE.
 - `debug crypto engine`—يعرض معلومات من محرك التشفير.
 - `debug crypto socket`—يعرض معلومات حول جدول مأخذ التوصيل بين NHRP و IPsec.
 - `debug nhrp`—يعرض معلومات حول أحداث NHRP.
 - `debug nhrp` ربط—يعرض معلومات حول حزم NHRP.
 - `debug tunnel protection`—يعرض معلومات حول أنفاق GRE الديناميكية.
- يمكن العثور على معلومات إضافية حول استكشاف أخطاء IPsec وإصلاحها في [استكشاف أخطاء أمان IP وإصلاحها](#) - فهم أوامر تصحيح الأخطاء واستخدامها.

معلومات ذات صلة

- [نظرة عامة على DMVPN و Cisco IOS](#)
- [صفحة دعم IPsec](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا