

نم نيقفن نيب رورمل ا ةكرح ريقشت نيوكت عقوم ىلا عقوم

تایوتیم

مدخل

وهي ملائكة ملائكة

تاتل طت ملا

ةمدختس ملابسان وكملا

قطط خال

مراجع و آثار

نیوکرک

لایک شت (ب عوام) ASA

ریفشه تلابنیوکت (ASA C عوامل)

دیفشن تلارنیوکت (A عوچ، ملار)

(ج) عوقب ملائیلا (ب) عوقب ملائیلا

ةمدقملا

دیجوراپ نانثا نیب رورم ڈکھ VPN لسري ناؤ فیک ڈکھو اذه فصی

ةيسيس ألا تابلطت ملأ

تابلطتما

CISCO مەمۇت ئەفرۇع مەلۇمۇت ئەپلىكاشن

عقولل VPN ۋە كېپشىلىق دىن تىسىملىقى عقولل يساساً مەھ.

ASA رماؤ رطس عم ةبرجت

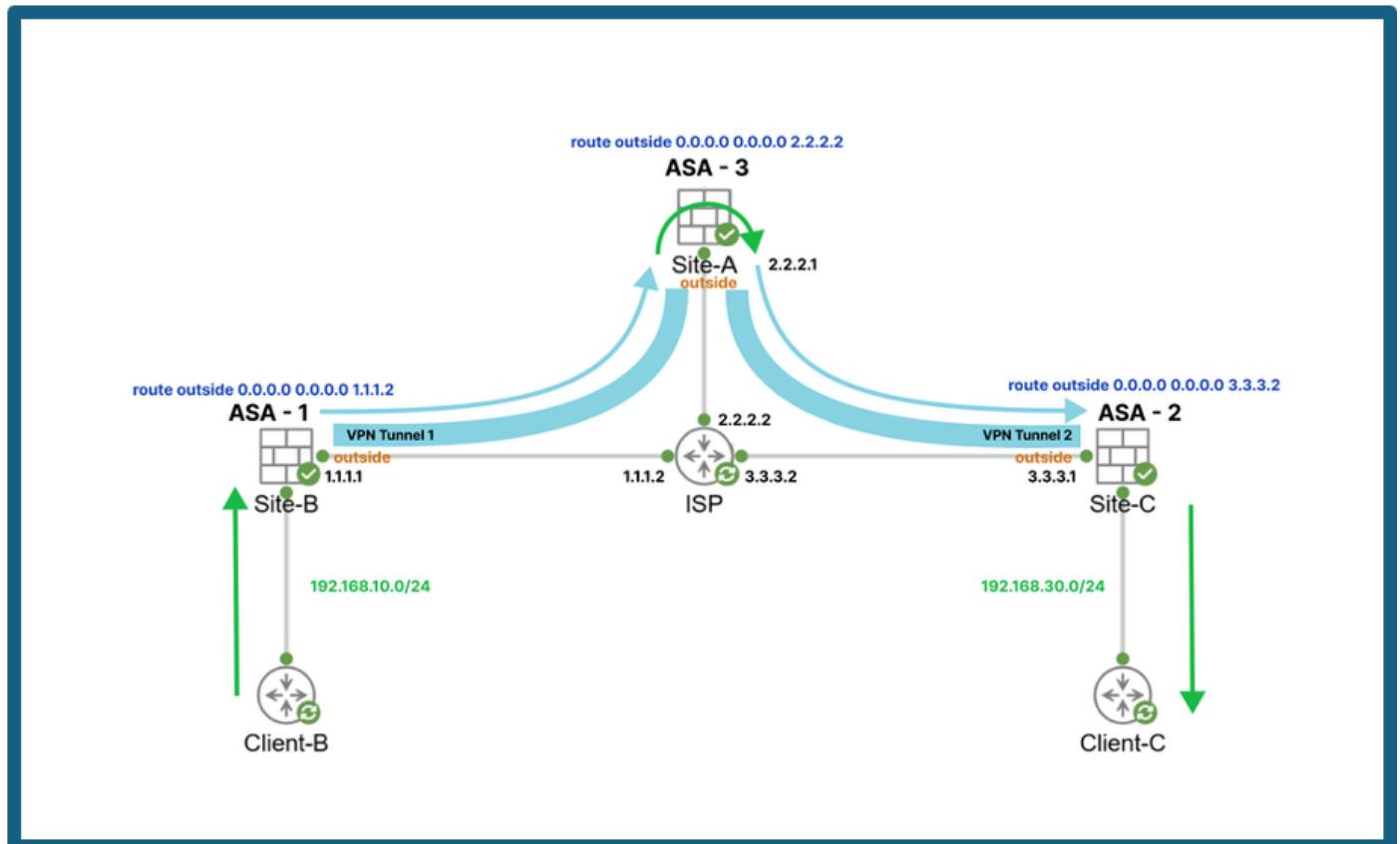
ةم دختس ملا تان وكملا

• ئىلاتلا ئىداملا تانوكمل او جماربلا تارادصا ىلإ دنتسملا اذه يف ئىدراولما تامولعملما دنتسست 9.20 رادصا لىا، (ASA) فىكتلل لباقلما ناما لىا زاوج · IIEV1

ڇاڻا خ ڦيلم ڻا ڦي ڦوچ ڦيلملا ڦيزه ج ڦيلا نم دن ڦتس ڦيلملا اذه ڦيف ڦيزه ج ڦيلملا تام ڦولع ڦيلملا ڦاڻن ڦا م ڦت ڦن ڦاك اذا (ڦي ڦض ارت ڦفا) حوس ڦيلم ن ڦي و ڦوك ڦتب دن ڦتس ڦيلملا اذه ڦيف ڦيزه ج ڦيلملا ڦيزه ج ڦيلا ع ڦيم ڦج ڦت ڦأدب

رما يأ لمحمل ريا ثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ططخمل



ططخمل

ةيساسأ تامولعم

ىلע רחא ילא עقوم נמ קפנ נמ רורמל אckerה הייגות אداعא כיוקטלא אזהחצוי עقومלאו A עقومלא L思ת ASA Tadhoh Thalath Anmdختס ,دادעה לא אזהחצוטל .סفن זאהגלא עقومלאו C.

نيوكتل

ىلإ (ب عقوملا) ASA-1 نم رورمل اckerה حامسلل بولطملا نيوكتل مسقلاء اذه حصوى عقوملاو C عقوملا (ASA-3).

امهنيوكت مت VPN ةكبشل نيقفن انيدل:

- عقوملاو B VPN قفن 1 : قفن A
- عقوملاو C VPN قفن 2 : مقر A

ةسايسلا يلإ دنتسم VPN قفن عاشن ةيفيك لوح ةيليقفت تاداشرا يلע لوصحلل

ع ASA ىل اع جرا، Cisco: [Cisco IPsec IKEv1 ASA قفـن نـيـوكـت](#) نـيـوكـت مـسـقـىـاـثـوـيـفـ

لـيـكـشـتـ (ـبـ عـقـوـمـلـاـ)

ةـمـئـاـقـ يـفـ Cـعـقـوـمـلـاـ ةـكـبـشـ ىـلـاـ Bـعـقـوـمـلـاـ ةـكـبـشـ نـمـ روـرـمـلـاـ ةـكـرـحـبـ حـامـسـلـاـ ىـلـاـ جـاتـجـنـ لـةـيـجـرـاخـلـاـ ةـهـجـاـولـاـ ىـلـعـ 1ـ VPNـ قـفـنـلـ ۆـرـفـشـلـاـبـ ةـصـاخـلـاـ لـوـصـوـلـاـ 1ـ ASAـ 1ـ.

فـوـجـوـمـ وـ Ciscoـ XEـ Ciscoـ IOSـ نـمـ

ريـفـشـتـلـاـ ىـلـاـ لـوـصـوـلـاـ ةـمـئـاـقـ:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

عـانـثـتـسـاـ nat:

```
nat (inside,outside) source static192.168.10.0_24192.168.10.0_24 destination static192.168.30.0_24192.168.30.0_24
```

لـرـيـفـشـتـلـاـ ةـطـيـرـخـ VPN~ Tunnel~ 1~:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 2.2.2.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map interface outside
```

رـيـفـشـتـلـاـ نـيـوكـتـ (ـعـقـوـمـلـاـ)ـ Cـ

ةـصـاخـلـاـ لـوـصـوـلـاـ ةـمـئـاـقـ يـفـ SITE-Bـ ةـكـبـشـ ىـلـاـ SITE-Cـ ةـكـبـشـ نـمـ روـرـمـلـاـ ةـكـرـحـبـ حـامـسـلـاـ ىـلـاـ رـيـفـشـتـلـاـ ىـلـعـ 2ـ VPN~ Tunnel~ 2~ لـةـيـجـرـاخـلـاـ ةـهـجـاـولـاـ 2ـ ASA~ 2~.

نام 192.168.30.0/24 ىلإ 192.168.10.0/24، ويرانيسلا اذه يف

ريشتلا ىلإ لوصولاً ٰمئاً:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
```

nat: ثنتسا عان:

```
nat (inside,outside) source static 192.168.30.0_24 192.168.30.0_24 destination static 192.168.10.0_24 192.168.10.0_24
```

طيرخ ٰمئاً لـ VPN Tunnel 2:

```
crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 2.2.2.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ريشتلا نيكوت (ASA A) عقولاً

ريشتلا لوصولاً ٰمئاً يف Site-B ٰكبش نام رورملأا ٰكرحب حامسلا لوصولاً ٰمئاً يف C ٰكبش ىلإ Site-B ٰكبش نام رورملأا ٰكرحو 1 VPN قفنب ٰصالخا يف نيكوت يتلـا Site-A يـف ASA لـ ٰيجراـخـلا ٰهـجـاـولـا ىـلـعـ 2 VPN قـفـنـبـ ٰصـالـخـاـ رـيـفـشـتـلـاـ ىـلـعـ هـنـيـوـكـتـبـ اـنـمـقـ اـمـلـ يـسـكـعـلـاـ ـاـجـتـاـلـاـ.

نام 192.168.30.0/24 ىلإ 192.168.10.0/24 لـ VPN Tunnel 1، ويرانيسلا اذه يف 192.168.10.0/24 ىلإ 192.168.30.0/24 لـ VPN Tunnel 2

ريشتلا ىلإ لوصولاً ٰمئاً:

```
object network 192.168.30.0_24
```

```

subnet 192.168.30.0 255.255.255.0
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0
access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
access-list 120 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24

```

و 1 و 2 ل VPN Tunnel ةطيـخ نـيـوكـت:

```

crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 1.1.1.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 3.3.3.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside

```

يـتلـاـوـجـرـاخـلـاـىـلـاـجـرـاخـلـاـنـمـتـانـاـيـبـلـاـرـورـمـةـكـرـحـهـيـجـوـتـىـلـاـجـاتـحـنـاـنـنـأـلـاـذـهـىـلـإـفـاضـإـلـاـبـ:ـرـمـأـلـاـنـيـوكـتـىـلـاـقـاحـبـاـنـنـإـفـ،ـهـسـفـنـنـاـمـأـلـاـىـوـتـسـمـعـمـةـهـجـاـوـلـاـسـفـنـيـهـنـوـكـتـ:

```
same-security-traffic permit intra-interface
```

(ج) عـقـوـمـلـاـىـلـاـ(ـبـ)ـعـقـوـمـلـاـنـمـرـورـمـلـاـةـكـرـحـقـفـدـتـ

نـم~C~عـقـوـمـلـاـىـلـا~B~عـقـوـمـلـا~نـم~اـهـلـيـغـشـت~عـدـب~مـت~يـتـلـا~رـورـمـلـا~ةـكـرـح~رـابـتـعـاـلـا~نـيـعـب~ذـخـأـنـلـ192.168.10.0/24~192.168.30.0/24.

(ردـصـمـلـاـ)ـعـقـوـمـلـاـ(ـعـقـوـمـلـاـ)

لـةـهـجـوـمـلـاـوـ(ـsite-bـ)ـرـادـصـإـلـاـنـمـتـأـدـبـيـتـلـاـرـورـمـلـاـةـكـرـحـهـيـجـوـتـمـتـيـ.ـيـذـلـاـهـيـجـوـتـلـاـلـوـدـجـىـلـاـاـدـاـنـتـسـاـ1ـلـةـيـجـرـاخـلـاـةـهـجـاـوـلـاـىـلـاـASA-1ـ)ـعـقـوـمـلـاـىـلـاـ(ـsite-Cـ)ـلـةـيـجـرـاخـلـاـةـهـجـاـوـلـاـىـلـاـ.ـنـيـوكـتـمـتـ.

يـتـلـا~110~رـيـفـشـتـلـل~لـوـصـوـلـا~ةـمـئـاـقـقـبـاـطـتـاـهـنـإـفـ،ـرـورـمـلـا~ةـكـرـح~لـوـصـوـدـرـجـمـبـ.ـعـقـوـمـلـا~وـحـنـنـمـآـلـكـشـبـتـانـاـيـبـلـا~لـسـرـيـيـذـلـا~VPN~1~قـفـنـمـاـدـخـتـسـاـبـرـورـمـلـا~ةـكـرـح~رـيـفـشـت~لـيـغـشـت~ىـلـا~اـذـه~يـدـؤـيـ.~اـلـع~اـهـن~نـيـوـكـت~مـت~A~.

طسوتム-A-عقول

ل ةيجرالا ةهجاولى لىع 192.168.10.0/24 to 192.168.30.0/24 arrives
ASA يف عقولما اركح.

2. ةداعتسال 1 VPN قفن ةطساوب تانايبلارورم ةكرح ريفشت كف متي، عقوملا يف ةيلصلأا ئلومحلا.

مادختساب اهريفشت كف مت يتلاتان ايبلارورم كرح ريفشت دادعامت، كلذ دعبو.
A. عقوملا يف ASA L ئيجراخلا ئوهجاولا يف 2 VPN قفن.

جول()-عقوم

ل ئىجراخلى ئەجأولى 192.168.10.0/24 to 192.168.30.0/24 reaches رورملا ئەكح ASA-2 يىف site-C.

ىلإ مزح لـا هي جوـت ةـداع اوـ 2 VPN قـفن مـادـخـتـسـاب رـورـمـلـا ةـكـرـحـ رـيـفـشـتـ كـفـبـ 2 ASA مـوقـيـ 2. 192.168.30.0/24 نـمـضـ ةـدـوـصـقـمـلـا ةـهـجـوـلـا ىـلـا اـهـمـيـلـسـتـوـ Site-C نـمـ LAN بـنـاجـ.

ب سکع قفدت ةكح رورملا نم عقوملا ىلإ C

C-عقوملـا نـم أـشـنـت يـتلـا ،ـيـسـكـعـلـا رـوـرـمـلـا ةـكـرـح قـفـدـت نـع جـتـنـي :ـيـسـكـعـلـا هـاجـتـإـلـا يـف نـكـلـو ةـيـلـمـعـلـا سـفـنـ،ـ بـعـقـوـمـلـاب صـاخـلـا

ىلى اهل اسرا لبىق 2 VPN قفن ئەتساوب تانايىپلا رورم ئەكىرەت مەتى، عقوملا يىف 1. ع القوملا A.

ةداعاً متى مث، 2، VPN قفن ظطساً واب تان ايبل رورم ةكرح ريفشت كف متى، A، عقوملا يف. عقوملا يل اهه جوت ةداعاً لباق 1 VPN قفن مادختس اب اهري فشت B.

3. اهمیلس، و 1 VPN قفن ۃطس، او بـ تـانـاـیـبـلـا رورم ۃکـرـحـ رـیـفـشـتـ کـفـ مـتـیـ، Bـ عـقـوـمـلـاـ یـفـ.

192.168.10.0/24 network.

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).