

نەم ققحتل او FlexVPN لە نیوکت

تاي وتحمل

[قىدقملا](#)

[قىس اس الاتابل طتملا](#)

[تابل طتملا](#)

[قىدخت سملاتان وكملا](#)

[قىس اس ا تامولع](#)

[IKEv2 لباقم IKEv1](#)

[رىوطتلار قىلباق](#)

[قىسىئىرلار تازىملا](#)

[ھىجوت](#)

[لىيوختلار قىس اس](#)

[ىرخأ تاي نقطت لباقم FlexVPN](#)

[قىكبشلىلى طىطختلار مس رىلار](#)

[نيوكتلار](#)

[عقۇم دىلار عقۇم نەم نیوكت FlexVPN](#)

[عۇزوملار نیوكت 1: ۋوطخلار A](#)

[عۇزوملار نیوكت 2: ۋوطخلار B](#)

[قىصلانم ققحتلار](#)

[FlexVPN قىنونقىت Hub-and-Talk](#)

[عۇزوملار نیوكت 1: ۋوطخلار](#)

[مىڭىدىچىلار مىڭىدىچىلار نیوكتلار 2: ۋوطخلار](#)

[قىصلانم ققحتلار](#)

[مىڭىدىچىلار FlexVPN دىلار نىچەت](#)

[عۇزوملار نیوكت 1: ۋوطخلار](#)

[نىوكت نىچەت 2: ۋوطخلار](#)

[نىوكتلار ئىف ئىچىت 3: ۋوطخلار B](#)

[قىصلانم ققحتلار](#)

[اھالىسى او ئاطخالا فاش كىتسى](#)

ةمدقملا

حىرىشىو، اهتازىمم مدقىي، (Flex) ئىرها ئۆللا ئەصاخلا ئەكپشلار ئەئىپ دەنت سملار اذە فصىي ئەنۋەتلىك FlexVPN.

ةيىس اس الاتابل طتملا

تابل طتملا

ئەيلاتلار عيضاً مولاب ئەفرعيم كىيدل نوكت نأب Cisco يىصوت:

- IOS و Cisco IOS XE
- 2 رادص إلـا (IKE) تـنرـتـنـإـلـا حـاتـفـمـلـدـابـتـ
- تـنرـتـنـإـلـا لـوـكـوـتـورـبـنـأـمـاـ
- FlexVPN

ةمدختسملا تانوكمل

: ئيلاتلا ئيداملا تانوكمل اوجماربلـا تـارـادـصـاـىـلـا دـنـتـسـمـلـا دـنـتـسـتـ

- Cisco IOS XE Amsterdam-17.3.6

ةـصـاخـ ئـيـلـمـعـمـ ئـيـبـ يـفـ ئـدـوـجـوـمـلـاـ ئـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ئـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ عـاشـنـاـ مـتـ
تنـاـكـ اـذـاـ (يـضـارـتـفـاـ)ـ حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ئـمـدـخـتـسـمـلـاـ ئـزـهـجـأـلـاـ عـيـمـجـ تـأـدـبـ
رـمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ،ـ لـيـغـشـتـلـاـ دـيـقـ كـتـكـبـشـ.

ةـيـسـاسـأـ تـامـوـلـعـمـ

مـمـصـمـ Ciscoـ،ـ هـمـدـقـتـ لـمـاـشـ وـتـامـاـدـخـتـسـالـاـ دـدـعـتـمـ (VPN)ـ ئـيـرـهـاـظـ ئـصـاخـ ئـكـبـشـ لـحـ وـهـ
ىـلـعـ ـهـدـامـتـعـاـلـ اـرـطـنـوـ.ـ تـاكـبـشـ تـالـاـصـتـاـ نـمـ ئـفـلـتـخـ عـاوـنـأـلـ دـحـومـ لـمـعـ رـاطـاـ مـيـدـقـتـلـ
طـيـسـبـتـلـ FlexVPNـ مـيـمـصـتـ مـتـ،ـ (2ـ رـادـصـ إـلـاـ تـنـرـتـنـإـلـاـ حـاتـفـمـلـدـابـتـ)ـ لـوـكـوـتـورـبـ
نـمـ ئـقـسـاـنـتـمـ ئـعـوـمـجـمـ ئـلـيـاعـفـ ئـدـايـزـ ئـلـعـ لـمـعـيـ اـمـمـ،ـ اـهـرـشـنـوـ اـهـتـرـادـاـوـ VPNـ ئـكـبـشـ نـيـوـكـتـ
تـاكـبـشـ نـمـ ئـفـلـتـخـ عـاوـنـأـلـ رـبـعـ اـهـقـيـبـطـتـ مـتـيـ يـتـلـاـ نـيـوـكـتـلـاـ تـاوـطـخـوـ رـمـاـوـأـلـاـ سـفـنـوـ تـاوـدـأـلـاـ
لـيـلـقـتـ ئـلـعـ قـسـاـنـتـلـاـ اـذـهـ دـعـاـسـيـوـ.ـ (كـلـذـ ئـلـاـ اـمـ دـعـبـ نـعـ لـوـصـوـلـاـوـ عـقـوـمـ ئـلـاـ عـقـوـمـ نـمـ)
لـقـلـوـهـسـ رـثـكـأـ رـشـنـلـاـ ئـلـمـعـ لـعـجـيـوـ عـاطـخـأـلـاـ.

IKEv2 لـبـاقـمـ IKEv1

رـاـيـعـمـ AESـ لـثـمـ ئـثـيـدـحـلـاـ ئـرـفـشـمـلـاـ تـايـمـزـراـوـخـلـاـ مـعـدـتـ يـتـلـاـ IKEv2ـ نـمـ دـيـفـتـسـتـ
ارـيـفـشـتـ تـايـمـزـراـوـخـلـاـ ـهـذـهـ رـفـوتـوـ.ـ (ةـنـمـآـلـاـ ئـزـجـتـلـاـ ئـيـمـزـراـوـخـ)ـ وـ (مـدـقـتـمـلـاـ رـيـفـشـتـلـاـ)
ةـيـرـهـاـظـلـاـ ئـصـاخـلـاـ ئـكـبـشـلـاـ رـبـعـ ئـلـسـرـمـلـاـ تـانـاـيـبـلـاـ يـمـحـيـ اـمـمـ،ـ تـانـاـيـبـلـاـ ئـمـالـسـوـ اـيـوـقـ
اـهـ بـعـاـلـتـلـاـ وـأـ اـهـضـارـتـعـاـ مـتـيـ نـأـ نـمـ.

اـقـبـسـمـ كـرـتـشـمـ حـاتـفـمـ بـنـاجـ ئـلـاـوـ IKEv1ـ بـ ئـنـرـاقـمـ ئـقـدـاـصـمـلـاـ قـرـطـ نـمـ دـيـزـمـلـاـ IKEv2ـ مـدـقـيـ
مـاـدـخـتـسـابـ بـيـجـمـلـلـ IKEv2ـ حـمـسـيـ،ـ ئـدـاهـشـلـاـ ئـلـعـ ئـمـئـاـقـوـ ئـطـلـتـخـمـ ئـقـدـاـصـمـ عـاوـنـأـوـ (PSK)
لـيـمـعـلـاـ ئـقـدـاـصـمـلـاـ عـسـوـتـمـلـاـ ئـقـدـاـصـمـلـاـ لـوـكـوـتـورـبـ.

لـئـاسـرـ رـرـمـيـوـ،ـ لـيـحـرـتـكـ هـجـوـمـلـاـ لـمـعـيـوـ،ـ لـيـمـعـلـاـ ئـقـدـاـصـمـلـاـ مـدـخـتـسـيـ،ـ يـفـ EAPـ
قـرـطـ نـمـ دـيـدـعـلـاـ FlexVPNـ ئـكـبـشـ مـعـدـتـ.ـ دـادـعـ RADIUSـ مـدـاـخـ وـهـوـ،ـ يـفـلـخـلـاـ EAPـ مـدـاـخـوـ لـيـمـعـلـاـ نـيـبـ
ةـقـدـاـصـمـلـاـ ئـلـيـلـمـعـ نـاـمـضـلـ،ـ اـهـرـيـغـوـ EAP-PEAPـ وـ EAP-PSKـ وـ EAP-TLSـ كـلـذـ يـفـ اـمـبـ،ـ EAPـ.

لـئـاسـرـ IKEv1ـ وـ IKEv2ـ فـيـاـطـوـنـيـبـ تـافـاـلـتـخـاـ لـوـدـجـلـاـ حـضـوـيـ:

	IKEv2	IKEv1
لـوـكـوـتـورـبـلـاـ عـاشـنـاـ لـئـاسـرـ	لـئـاسـرـ 4	لـئـاسـرـ 6
عـمـدـ EAPـ	(ةـيـفـاـضـ ئـلـاسـرـ)ـ مـعـنـ	اـلـ
هـيـنـمـاـلـاـ تـادـاحـتـاـلـلـ ضـوـافـتـلـاـ	نـاتـيـفـاـضـ ئـنـاتـلـاسـرـ	ةـيـفـاـضـ ئـلـاسـرـ 3

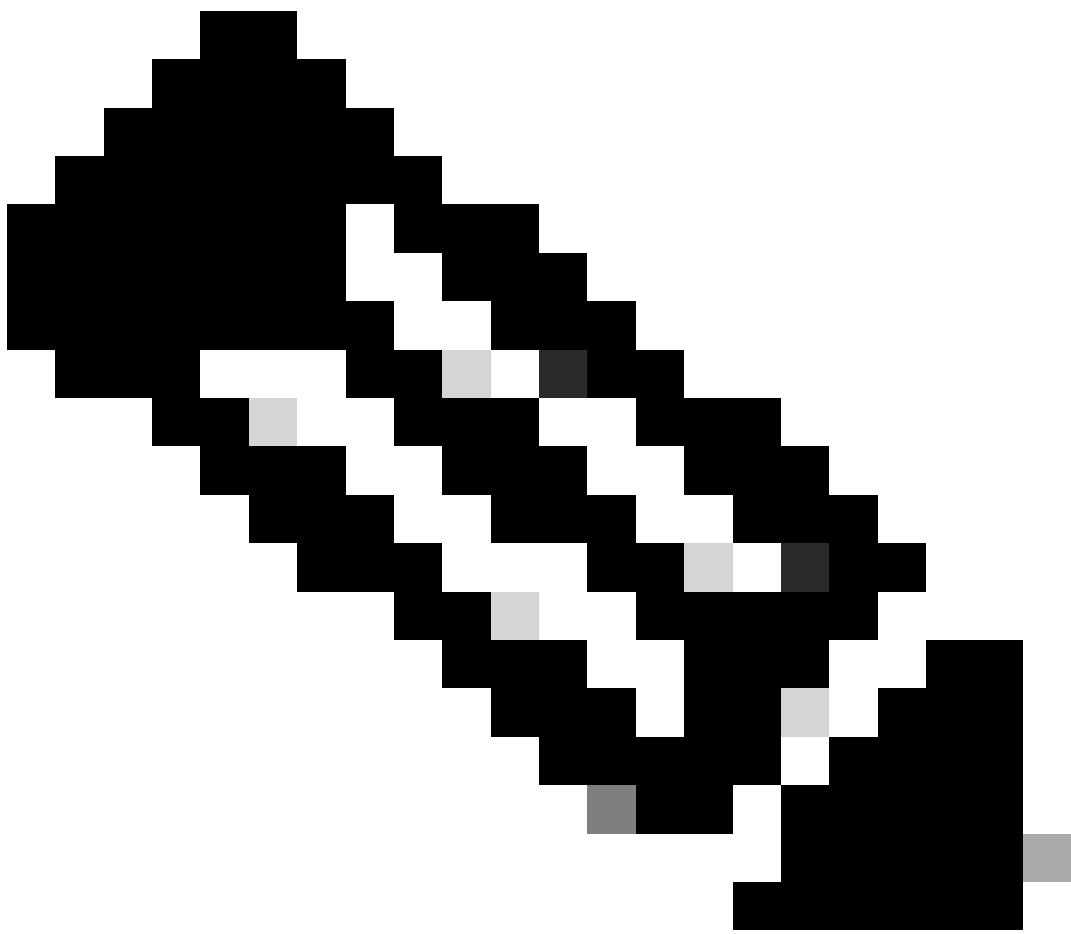
UDP 500/4500 رباعي لغش تلا	معن	معن
NAT (NAT-T) زاي تجا	معن	معن
رارق إالا أو لاس إالا ادعى ماهم	معن	معن
ةيلآو ةي وهل ل ةي امحلا ريفوت ةمدخلأا ضفر نم ةي امحلا ةداع إالا ةماتلا ةيرسلاؤ ^(DoS) هيجوت لا ^(PFS)	معن	معن
يلاتلا لي جلا تارفش معن د	معن	ال

ريوطتل ا ةيلباق

تاكرشلا تاكبش ىلا ةريغصلاب تاكملاب نم ةمات ٖل و هسب FlexVPN ةكبش ٖعسوت نكمي نم ريبك ددع اه برفوت ي يتلا تاسسؤم ل ايلاثم ارایخ نم لعجي اذهو. ةريبكلا ةكبشلا ىلا قوთوملاو نمآلاب لوصولا ىلا نوجاتحي نمم دعب نع نيمدختسملا.

ةيسئرلا تازيملا

- بطلاب سح قافنأ او يكي مانيدلا نيوكتلا
 - ادانتسا ةي ضارت فا لوصو ٖه جاو ٖاشنإب ماظنلا موقيو FlexVPN، لاصتا عدب مت ي ◦ ٖدم ل ٖفنلا ةي اهن ٖطقن ك ٖه جاولما هذه لمعت. اقبس م هنيوكت مت بلاق ىلا، ةيرهاظلا لوصولا ٖه جاو ريمدت مت ي، ٖفنلا ىلا ٖجاجلما ٖاهتناد درجمب و لاصتا الـ ماظنلا دراوم ريفوت ىلع لمعي امم
- رشنلا ٖانثأ ٖنورملما
 - ةيعرفلا بتاكملاب نم ديدعلاب يزكرملا روحملاب لصت ي: مالكلاب روحملاب جذونم ◦ لمع راطإ لالخ نم تالاصتا الـ دادعإ ةي لممع طي سبـت ىـلع ةكبـش لـمعـت ◦ ةـريـبـكـلـا تـاكـبـشـلـل ةـيلـاثـم اـهـلـعـجـي اـمـم ،ـدـحـاـوـ لـصـاـوـتـلـا عـقـاـوـمـلـا عـيـمـجـلـ نـكـمـي :ـةـيـئـزـجـلـا ةـكـبـشـلـاو ةـلـمـاـكـلـا ةـكـبـشـلـا اـيـجـوـلـوبـطـ ◦ عـادـأـلـا نـسـحـيـوـرـيـخـأـلـا نـم لـلـقـيـ اـمـم ،ـيـزـكـرمـ زـكـرمـ رـبـعـ رـورـمـلـا نـودـ رـشـابـمـ
- راركتو لاع رفوت
 - دحأ لشف ٖلاح يف. يـطاـيـتحـالـا خـسـنـلـل ٖددـعـتـم زـكـارـمـ معـدي :ـةـرـكـمـلـا عـيـزـوـتـلـا تـاحـوـلـ ◦ رـمـتـسـمـ لـاصـتا نـمـضـيـ اـمـم ،ـرـخـآـعـزـوـمـبـ عـورـفـلـا لـصـتـتـنـأـ نـكـمـيـ ،ـرـواـحـمـلـاـ (ـVPNـ) ةـيـرـهـاظـلـا ةـصـاخـلـا ةـكـبـشـلـا تـالـاصـتا عـيـزـوـتـ ىـلعـ لـمـعـيـ اـدـهـوـ لـيـمـحـتـلـا ةـنـزـاـوـمـ ◦ غـلـابـ اـرـمـأـ دـعـيـ اـمـ وـهـوـ ،ـدـئـازـلـكـشـبـ دـحـاـوـ زـاهـجـ يـأـ لـيـمـحـتـ بـنـجـتـلـ ٖددـعـتـم ٖزـهـجـأـ رـبـعـ ◦ ةـريـبـكـلـا رـشـنـلـا تـاـيـلـمـعـ يـفـ عـادـأـلـا ىـلعـ ظـافـحـلـلـ ةـيـمـهـأـلـاـ



لامحألا ةنزاوم نيوكت لوح تامولعملانم ديزملاليلاتلا ليلدلا رفوي: ةظحالمعيزوتلاتاحول لاصتال.

IKEv2 لمح نزاوم نيوكت

• ريوطتلل نالباق ضيوفتو ةقداصم:

- Cisco ISE لثم AAA مداوخ عم لمعي: (AAA) ةبساحمل او ضيوفتل او ةقداصمل اجمد
- مادختسالل ةيرورضلارمدختسملا تاسايسو تاغوسمل ةيزكرملا ةرادإلل عساو قاطن ىلع
- تاداهشل او (PKI) ماعلا حاتفم لل ةيساسألا ةينبلا معدي: تاداهشل او PKI تادحو
- مادختسالن رثكأ ريوطتلل ةلباق نوكت يتلأاو، ةنمآللا ةقداصملالجأ نم ةيمقرلاةريبكلا تائيبلاليف ةصاخ، اقبسم كرتشم حاتفم.

٥ي جوت

ةلاعفلارادالا ريوطتلل ةيلباق نيسحتل FlexVPN يف هي جوتللا ةفيظومي مصت مت لك ىلإ تانايبلارورم ةكرح هي جوتل ةيكيمانيد ةقيرطب حامسل او ةددعتملا VPN تالاصتال

الاعف FlexVPN هيجوت لعجت يتلا ئيلاتلا ئيساساً تاييلآل او تانوكملما. اهنم دح او

- لاصتاً ئازاللا تادادع إلأ عيمج نمضتي نيوكت بلاق اذه: يرهاظلا بلاقلا ههجاو، VPN، زرمألا نيوكت مت ههجاو اولما هذه يف IPsec. تادادع او قفنلار دضم و IP ناونع نييعت لثمم رضمك ددم IP ناونع نيوكت نم الدب عاجرسا نم هداع، IP ناونع ضارتقال unnumbered نأ ملكتي لك حمسى، ثدحتي لك ب لممعتسى نأ بلاق هسفن لاناكمي اذه. قفنلل ناونع هرضم لممعتسى.

- بلاقلا ههجاو نم اهتادادع اثرت و ايكماني داهؤاشن مت تاهج او هذهب: يرهاظلا لوصولا ههجاو لوصو ههجاو ئاشن ا متي، ديدج VPN لاصتا ئاشن ا هييف متى ئرم لك يف. يرهاظلا لمع تاسلچ نم هسلچ لك نأ ينعمي اذهو. يرهاظلا بلاقلا ئلا ادانتسا ةديدج ةيضرارت فا ىلع لممعي امم، اب ةصالخ ةديرف ههجاو ىلع يوتحت (VPN) ئيرهاظلا ةصالخلا ةكبشلا سايقل او ةرادإلا طيس بت.

- و OSPF لثمم هيجوتلا تالوكوتورب عم لممعي وهو: ئيكيماني دلما هيجوتلا تالوكوتورب هيجوتلا تامولعم ثي دحت رارماتسا ئلا كلذ يدوئي. VPN ةكبش قافنأ ربعم BGP و EIGRP. ئيكيماني دلما و ةريبكلا تاكبس لل مهتم رمأ وهو، ايئاقت.

- ةكبشلا تامس عفدب FlexVPN مداخل حامسلا لالخ نم تاهجوملا نع نالع إلاب IKEv2 موقعي اضيأ ليجعلها موقعي. قفنللا ههجاو ىلع تاهجوملا هذه تيبثتب موقعي يذل او، ليجعلها ئلا تاثي دحت حيتى امم، نيوكتلا عضول دابت ئانثأ مداخلاب ةصالخلا هتاكبس مالعاب نيتىاهنلا الـ ك ىلع راسملما.

- NHRP ناونعلا ليلحـت لوكوتورب وه (ئيلاتلا Hop) ةوطخلـا ليـلحـت لوكوتورب) ةـمامـعـلـا IP نـيـوانـعـ نـيـيـعـتـلـ ةـمـلـاـكـمـلـاـوـ ةـيـرـوحـمـلـاـ تـاطـطـخـمـلـاـ يـفـ مـدـخـتـسـمـلـاـ يـكـيـمـانـيـ دـلـاـ لـاصـتـالـلـ ئـرـخـأـ IP نـيـوانـعـ فـاشـتـكـاـ نـمـ دـافـصـأـلـاـ نـكـمـيـ وهـوـ ةـصـالـخـلـاـ ئـيـاهـنـ طـاقـنـ ئـلـاـ رـشـابـمـلـاـ.

ليوختلا ئس اي س

لاصتا نم ئفلتخـمـ بـناـوجـ يـفـ مـكـحـتـلـلـ FlexVPN IKEv2 ضـيـوفـتـ ئـسـ ايـسـ نـيـوـكـتـ نـكـمـيـ VPN: دـعـبـ نـعـ وـأـوـ ئـيـلـحـمـ تـامـسـ ىـلـعـ يـوـتـحـيـ وـيـلـحـمـلـاـ لـيـوـخـتـ جـهـنـ دـدـحـيـ

- ئيرهاظلا ةصالخلا ةكبشلا هيجوت ئداع او هيجوت لثمم، ئيلحملـا تامـسـلـاـ قـيـبـطـتـ مـتـيـ ايـلـحـمـ، ةـمـدـخـلـاـ ةـدـوـجـ جـهـنـ وـ (VRF).
- نـيـوـكـتـلـاـ عـضـوـ رـيـظـنـلـاـ ئـلـاـ، تـارـاسـمـلـاـ لـثـمـ، ةـدـيـعـبـلـاـ تـامـسـلـاـ عـفـدـ مـتـيـ.
- ئـيـلـحـمـلـاـ ئـسـ ايـسـلـاـ دـيـدـحـتـلـ crypto ikev2 authorization policy رـمـأـلـاـ مـدـخـتـسـأـ.
- ضـيـوفـتـ رـمـأـ لـالـخـ نـمـ IKEv2 فيـرـعـتـ فـلـمـ نـمـ IKEv2 ضـيـوفـتـ ئـسـ ايـسـ ئـلـاـ ئـرـاشـإـلـاـ مـتـ AAA.

ليوخت جـهـنـ بـجـوـمـبـ اـهـنـيـوـكـتـ نـكـمـيـ يـتـلاـ حـيـتـافـمـلـاـ تـامـلـعـ ىـلـعـ ئـمـاعـ ئـرـظنـ لـوـدـجـلـاـ اـهـ رـفـوـيـ IKEv2.

رفـمـارـابـ	فصـولـاـ
AAA	تـاغـوـسـمـ نـمـ قـقـحـتـلـلـ AAA مـدـاـخـ عـمـ لـمـاـكـتـلـاـ باـسـحـلـاـوـ لـوـصـولـاـ لـيـوـخـتـوـ مـدـخـتـسـمـلـاـ مـتـيـ نـاـكـ اذاـ اـمـ جـهـنـلـاـ دـدـحـيـ نـأـ نـكـمـيـ مـاـدـخـتـسـاـلـلـ نـعـ وـأـ هـجـوـمـلـاـ ئـلـعـ اـيـلـحـمـ قـحـصـلـاـ نـمـ قـقـحـتـلـاـ

	RADIUS م داخ لالخ نم لثم ، دع ب
لي مع لا ن يو كت	مي ق لثم ، لي مع لا ى لـ نـ يـ وـ كـ تـ لـ اـ تـ اـ دـ اـ دـ عـ اـ عـ فـ دـ يـ نـ يـ يـ عـ تـ وـ . keepalives وـ DNS ، زـ وـ رـ وـ ، لـ وـ مـ خـ لـ اـ ئـ لـ هـ مـ كـ لـ ذـ ىـ لـ اـ اـ مـ وـ WINS ،
لي مع لا بـ صـ اـ خـ لـ اـ نـ يـ وـ كـ تـ لـ اـ	فـ لـ تـ خـ مـ لـ اـ ئـ فـ لـ تـ خـ مـ لـ اـ تـ اـ نـ يـ وـ كـ تـ لـ اـ بـ حـ مـ سـ يـ يـ فـ مـ هـ تـ يـ وـ ضـ عـ وـ أـ مـ هـ تـ يـ وـ هـ ىـ لـ اـ اـ دـ اـ نـ تـ سـ اـ عـ الـ مـ عـ لـ اـ ئـ عـ وـ مـ جـ مـ لـ اـ
تـ اـ رـ اـ سـ مـ لـ اـ ئـ عـ وـ مـ جـ مـ	رـ مـ تـ نـ أـ ئـ نـ يـ عـ مـ رـ وـ رـ مـ ئـ كـ رـ حـ لـ نـ يـ وـ كـ تـ لـ اـ اـ ذـ حـ يـ تـ يـ نـ قـ حـ ذـ يـ فـ نـ تـ ىـ لـ اـ يـ دـ وـ يـ اـ مـ اـ ذـ هـ وـ . VPN قـ فـ نـ رـ بـ عـ ىـ لـ عـ VPN لـ يـ مـ عـ ىـ لـ اـ هـ عـ فـ دـ مـ تـ يـ يـ ذـ لـ اـ رـ اـ سـ مـ لـ اـ حـ جـ انـ لـ اـ صـ تـ اـ

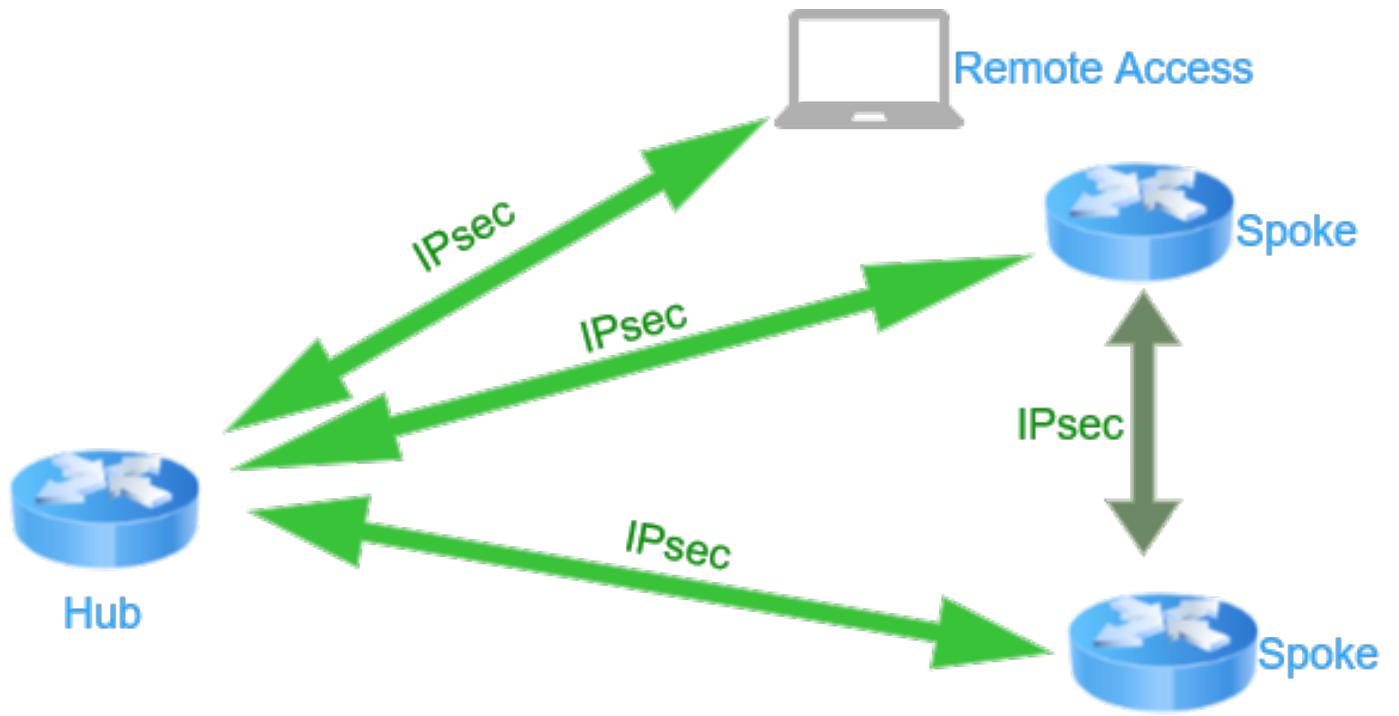
ىـ رـ خـ أـ تـ اـ يـ نـ قـ تـ لـ بـ اـ قـ مـ FlexVPN

تاـ كـ بـ شـ لـ اـ تـ اـ ئـ يـ بـ لـ اـ بـ اـ ذـ جـ اـ رـ اـ يـ خـ اـ هـ لـ عـ جـ تـ يـ تـ لـ اـ تـ اـ زـ يـ مـ لـ اـ نـ مـ ئـ عـ وـ مـ جـ مـ FlexVPN ئـ كـ بـ شـ رـ فـ وـ تـ يـ لـ مـ عـ طـ يـ سـ بـ تـ ىـ لـ عـ FlexVPN ئـ كـ بـ شـ لـ مـ عـ تـ ، دـ حـ وـ مـ لـ مـ عـ رـ اـ طـ اـ رـ يـ فـ وـ تـ لـ اـ لـ الـ خـ نـ مـ ئـ ثـ يـ دـ حـ لـ اـ يـ نـ يـ بـ لـ اـ لـ يـ غـ شـ تـ لـ اـ ئـ لـ بـ اـ قـ نـ اـ مـ ضـ وـ رـ يـ وـ طـ تـ لـ اـ ئـ لـ بـ اـ قـ مـ عـ دـ وـ نـ اـ مـ الـ اـ نـ يـ سـ حـ تـ وـ ئـ رـ اـ دـ الـ اـ اوـ ئـ يـ هـ تـ لـ اـ دـ يـ قـ عـ تـ لـ اـ لـ يـ لـ قـ تـ وـ

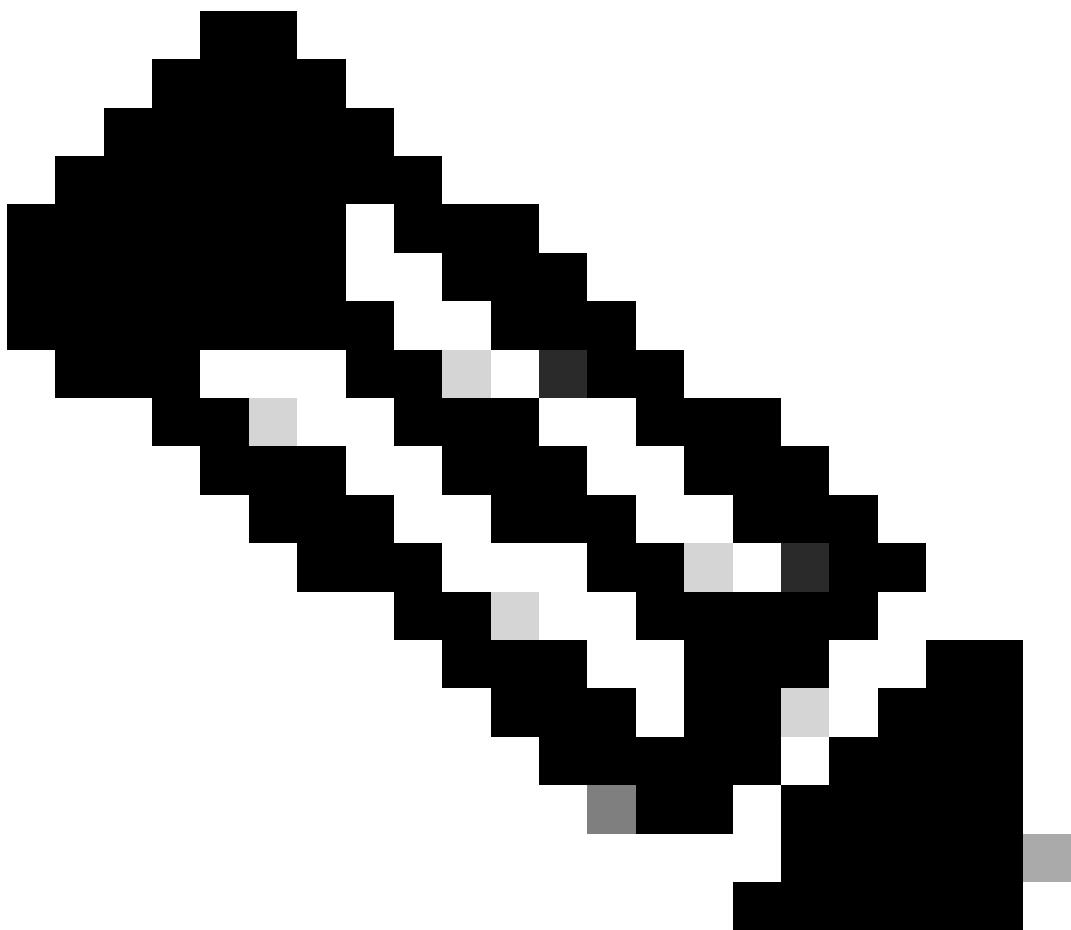
	ريـ فـ شـ تـ لـ اـ ئـ طـ يـ رـ خـ	DMVPN	FlexVPN
يـ كـ يـ مـ اـ نـ يـ دـ لـ اـ هـ يـ جـ وـ تـ لـ اـ	اـ لـ	مـ عـ نـ	مـ عـ نـ
رـ شـ اـ بـ مـ لـ اـ صـ تـ اـ يـ كـ يـ مـ اـ نـ يـ دـ	اـ لـ	مـ عـ نـ	مـ عـ نـ
لـ وـ صـ وـ لـ لـ VPN ئـ كـ بـ شـ دـ عـ بـ نـ عـ	مـ عـ نـ	اـ لـ	مـ عـ نـ
ةـ ئـ يـ هـ تـ لـ اـ طـ غـ ضـ	اـ لـ	اـ لـ	مـ عـ نـ
رـ يـ ظـ نـ لـ اـ نـ يـ و~ ك~ ت~	اـ لـ	اـ لـ	مـ عـ نـ
رـ يـ ظـ نـ لـ اـ ئـ مـ دـ خـ ئـ دـ و~ ج~	اـ لـ	مـ عـ نـ	مـ عـ نـ
اـ مـ دـ اـ خـ لـ مـ اـ كـ ت~ AAA	اـ لـ	اـ لـ	مـ عـ نـ

ةـ كـ بـ شـ لـ لـ يـ طـ يـ طـ خـ تـ لـ اـ مـ سـ رـ لـ اـ

عـ زـ و~ مـ لـ اـ ص~ ت~ اـ ع~ اـ ش~ ن~ اـ ى~ ل~ ع~ ل~ م~ ع~ ي~ ا~ م~ ، ئـ زـ هـ جـ ا~ ل~ ا~ ن~ ي~ ب~ ق~ ا~ ف~ ن~ ا~ ع~ ا~ ش~ ن~ ا~ ب~ ح~ م~ س~ ت~ ي~ م~ د~ خ~ ت~ س~ م~ ل~ ا~ ص~ ت~ ا~ ل~ او~ م~ د~ ا~ خ~ ل~ ا~ ن~ ي~ ب~ ر~ ش~ ا~ ب~ م~ ل~ ا~ ل~ ا~ ص~ ت~ ا~ ل~ ل~ ق~ ا~ ف~ ن~ ا~ ع~ ا~ ش~ ن~ ا~ ح~ ي~ ت~ ي~ ا~ م~ ك~ . د~ ي~ د~ ا~ خ~ ا~ ل~ او~ ي~ ط~ ي~ ط~ خ~ ت~ ل~ ا~ م~ س~ ر~ ل~ ا~ ي~ ف~ ح~ ض~ و~ م~ و~ ه~ ا~ م~ ك~ ، د~ ع~ ب~ ن~ ع~ ل~ و~ ص~ و~ ل~



FlexVPN طختل مس رلا يطي



لېلدل اذه يف دعب نع لوصلل VPN ةكبش نيوكت ئي طغت مدت ال : ئظحالم
لېلدل اىلا عجرا ، هننيوكت لوح ليصافت ئلعا لوصلل

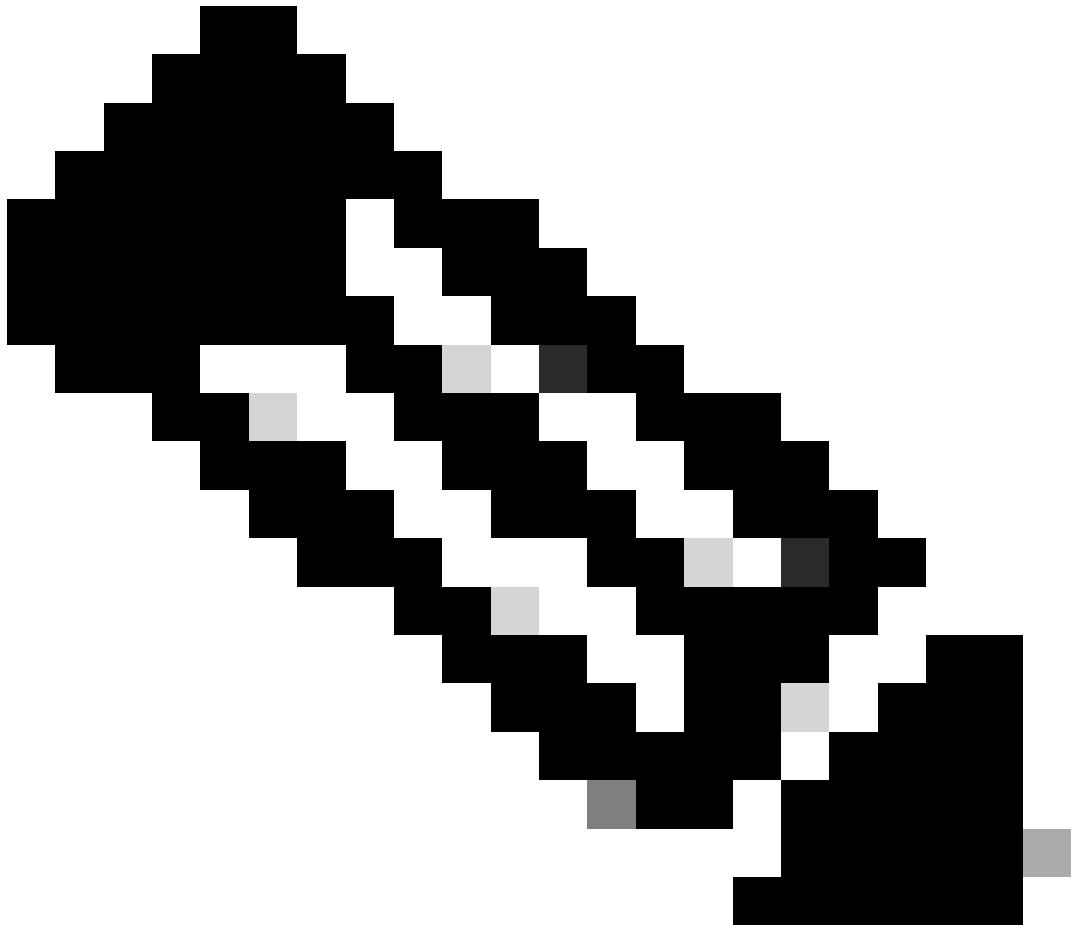
[نما ليمعل دعب نع لوصلل FlexVPN ثبلالا بقتسىلا ئدحو نيوكت](#)
[يلىخملام دختسىملاتانايىب دعاق مادختساب IKEv2](#)

نيوكتلار

نيوكتلار لتك يف ئطاسبلار هذه ئىلچىتت و اهتئيەت ئطاسسب FlexVPN ةكبش زىمتت لتك FlexVPN ةكبش رفوت. تاكبش نم ئفلىت خم عاوناڭل ئمدختسىملار ئقسانتمىلا ئيفاضا تاو طخ و أ ئيرايىت خا ئىيەت تايىلمۇع عم ، ماع لكىش ب اھقىب طت نكىمىي ئوشابم نيوكت ططاخملل ئددىحملار تابلطتمىلا و أ تازىمملل اقفو ئرفوتىم:

- IKEv2 نامأ نارتقا لوح ضوافتلا يف ئمدىتسىملاتايىم زراوخلا فيىرعت: IKEv2 حارتقا ئانثأ ھدى دىجىت مەتى ئىتەجىن ب حارتقا اذه قافرالا اذىق، ھىاشندا درجمب و ضوافتلا.

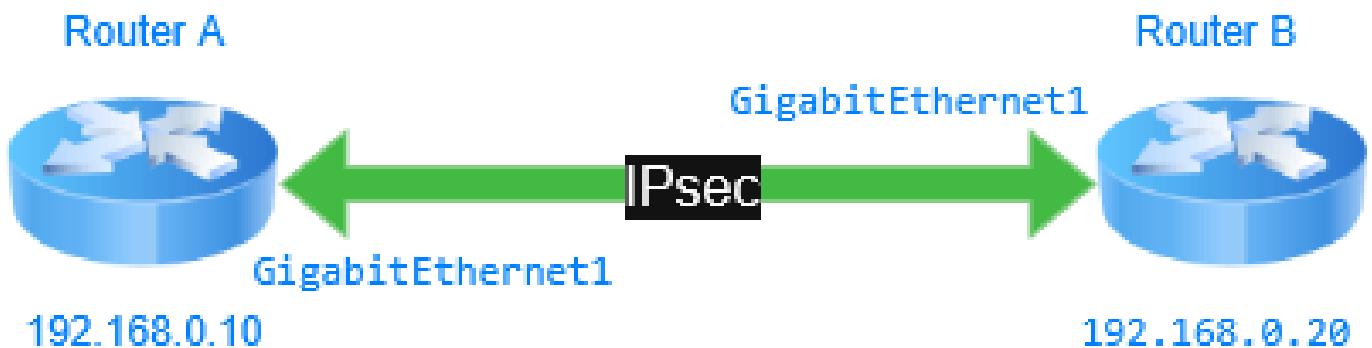
- IP ناونع وأ (VRF) يرهاظلا هيجوتلا ةداع او هيجوتلا ليثمب حرتفملأا طبري: IKEv2 جهـنـ حـارـتـ قـابـ جـهـنـلا طـابـتـراـ يـلـحـمـلـاـ IKEv2ـ.
- رـيـغـ نـوـكـتـ نـأـ نـكـمـيـ يـتـلـاوـ،ـ (PSKsـ)ـ اـقـبـسـمـ ةـكـرـتـشـمـ حـيـتـافـمـ دـدـحـيـ:ـ IKEv2ـ حـيـتـافـمـ ةـقـلـحـ رـيـظـنـلـاـ ةـقـدـاصـمـلـ اـهـمـادـخـتـسـاـ مـتـ اـذـاـ ةـلـثـامـتـمـ.
- دـنـعـ رـيـظـنـلـاـ ةـقـدـاصـمـلـ (CAـ)ـ ةـدـاهـشـلـاوـ ةـيـوـهـلـاـ عـجـرـمـ تـامـسـ نـيـوـكـتـ:ـ (يـرـايـتـخـ)ـ TrustPointـ دـاـوـخـ جـمـدـ FlexVPNـ مـوـقـتـ:ـ (يـرـايـتـخـ)ـ AAAـ ةـبـسـاحـمـلـاوـ ضـيـوـفـتـلـاوـ ةـقـدـاصـمـلـاـ جـمـدـ لـثـمـ Cisco ISEـ (Identity Services Engineـ)ـ مـاـعـلـاـ حـاـتـفـمـلـلـ ةـيـسـاسـأـلـاـ ةـيـنـبـلـاـ مـادـخـتـسـاـ.
- لـثـمـ IKE SAـ لـلـوـادـتـلـلـ ةـلـبـاـقـلـاـ رـيـغـ تـاـمـلـعـمـلـاـ نـيـزـخـتـبـ مـوـقـيـ:ـ IKEv2ـ فـيـرـعـتـ فـلـمـ بـجـيـ كـلـذـلـ،ـ يـضـارـتـفـاـ IKEv2ـ فـيـرـعـتـ فـلـمـ دـجـوـيـ الـ.ـ ةـقـدـاصـمـلـاـ قـرـطـوـ VPNـ رـيـظـنـ نـاـونـعـ مـادـخـتـسـاـ ةـلـاحـ يـفـ.ـ ئـدـابـلـاـ ئـلـعـ IPsecـ فـيـرـعـتـ فـلـمـبـ هـقـافـرـاـوـ فـيـرـعـتـ فـلـمـ نـيـوـكـتـ مـادـخـتـسـاـ مـتـ اـذـاـ IKEv2ـ حـيـتـافـمـلـاـ ةـقـلـحـ ئـلـاـ IKEv2ـ فـيـرـعـتـ فـلـمـ رـيـشـيـ،ـ ةـقـدـاصـمـ PSKـ،ـ آـنـهـ ئـلـاـ رـيـشـتـ اـهـنـافـ،ـ AAAـ ةـقـدـاصـمـ وـأـ PKIـ ةـقـدـاصـمـ وـأـ ةـقـيـرـطـ.
- لـلـوـبـقـمـلـاـ تـايـمـزـراـوـخـلـاـ نـمـ ةـعـوـمـجـمـ دـيـدـحـتـ لـلـيـوـحـتـ ةـعـوـمـجـمـ IPsecـ SAـ.
- هـقـيـبـطـتـ نـكـمـيـ دـحـاوـ فـيـرـعـتـ فـلـمـ يـفـ FlexVPNـ تـادـاعـاـ جـمـدـ مـوـقـيـ:ـ IPsecـ فـيـرـعـتـ فـلـمـ دـحـاوـ فـيـرـعـتـ فـلـمـ وـأـ IPsecـ لـلـيـوـحـتـ ةـعـوـمـجـمـ ئـلـاـ اـذـهـ فـيـرـعـتـلـاـ فـلـمـ رـيـشـيـ.ـ ةـهـجـاـوـ ئـلـعـ IKEv2ـ.



ضرع ريفوتل اقبسم ڈكرتشم هيتابم نيوكتلا ڈلثماً مدخلتسست: ظحالم
هيتابم مادختسنا نكمي امنيب .هـ طاسب و FlexVPN نيوكتل رشابم يحيضوت
ڈقادصل قرط نإف ،وريغصل اتاططخمل او لهـ سـ لـ اـ رـ شـ نـ لـ لـ اـ قـ بـ سـ مـ ڈـ كـ رـ تـ شـ مـ
ربـ كـ أـ لـ اـ زـ رـ طـ لـ لـ ةـ مـ عـ الـ مـ رـ ثـ كـ أـ نـ وـ كـ تـ PKI وـ (AAA) ةـ بـ سـ اـ حـ مـ لـ اوـ ضـ يـ وـ فـ تـ لـ اوـ.

عقوبـ مـ ئـ لـ اـ عـ قـ وـ مـ نـ مـ نـ يـ وـ كـ تـ

نـ يـ بـ ةـ رـ شـ اـ بـ مـ لـ اـ VPN تـ الـ اـ صـ تـ الـ اـ صـ يـ صـ خـ عـ قـ وـ مـ ئـ لـ اـ عـ قـ وـ مـ نـ مـ FlexVPN طـ طـ خـ مـ يـ مـ صـ تـ مـ تـ
رـ وـ رـ مـ لـ اـ رـ وـ رـ مـ لـ اـ ةـ كـ رـ حـ لـ نـ كـ مـ يـ ةـ نـ مـ آـ ةـ انـ قـ دـ دـ حـ تـ قـ فـ نـ ةـ هـ جـ اـ وـ بـ عـ قـ وـ مـ لـ كـ دـ يـ وـ زـ تـ مـ تـ يـ .نـ يـ عـ قـ وـ مـ
يـ فـ حـ ضـ وـ مـ وـ هـ اـ مـ كـ ،نـ يـ عـ قـ وـ مـ نـ يـ بـ رـ شـ اـ بـ مـ VPN لـ اـ صـ تـ اـ عـ اـ شـ نـ اـ ةـ يـ فـ يـ كـ نـ يـ وـ كـ تـ لـ اـ حـ رـ شـ يـ .اـ هـ ربـ عـ
طـ طـ خـ مـ لـ اـ.



site_to_site_diagram

هـجومـلـا نـيـوـكـتـ: 1ـ وـطـخـلـا

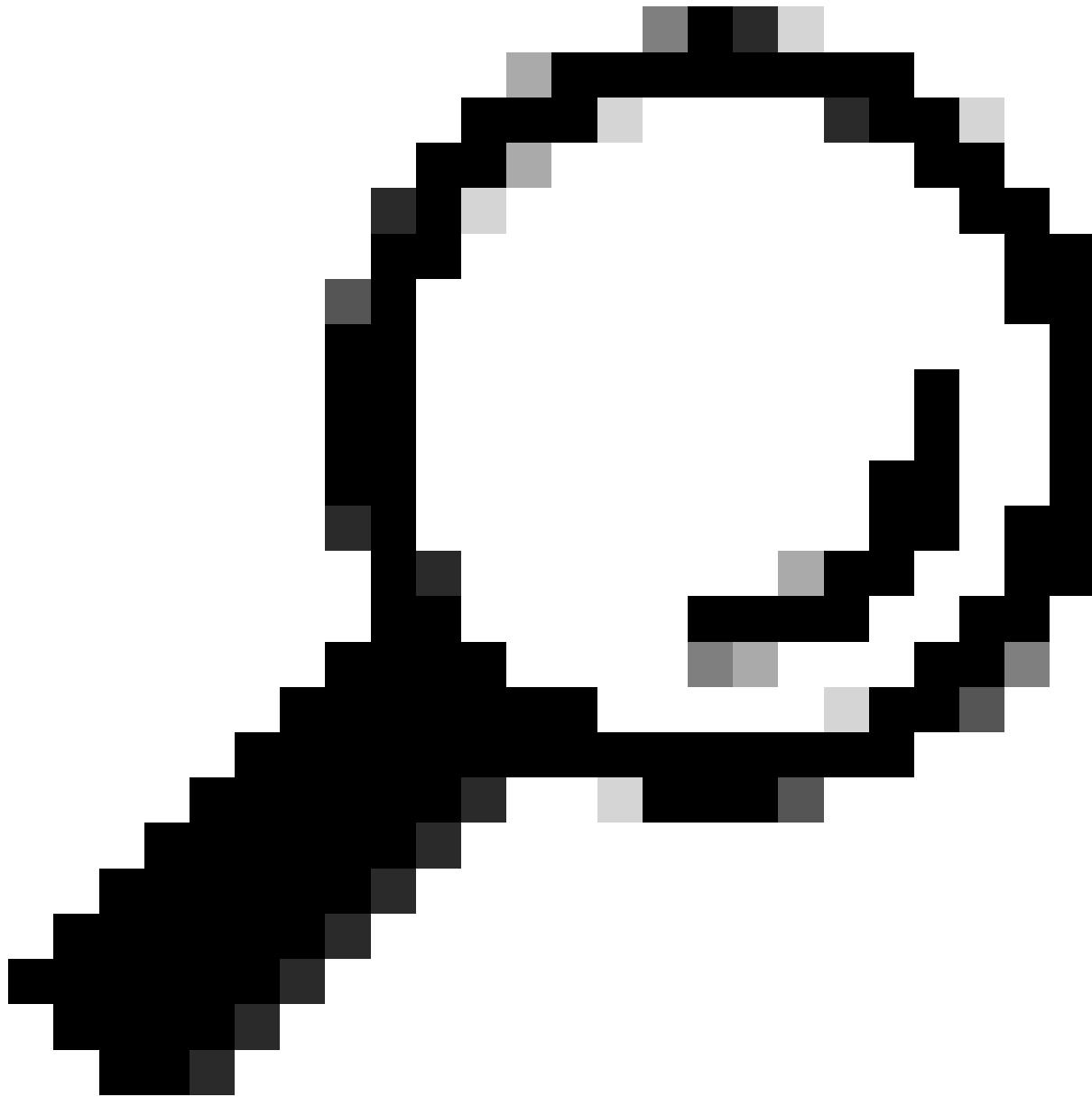
أـ. IKEv2ـ سـيـسـوـحـرـتـقـمـ دـيـدـحـتـ.

ـقـدـاصـمـلـ اـهـمـادـخـتـسـاـ مـتـيـ حـيـتـافـمـ ـقـلـحـ نـيـوـكـتـ بـ مـقـ .ـبـ رـيـظـنـلـاـ.

ـجـ نـيـعـتـوـ عـاـشـنـاـ جـ keyringـ IKEv2ـ profileـ.

```

crypto ikev2 proposal FLEXVPN_PROPOSAL
  encryption aes-cbc-256
  integrity sha256
  group 14
!
crypto ikev2 policy FLEXVPN_POLICY
  proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
  peer FLEVPNPeers
  address 192.168.0.20
  pre-shared-key local cisco123
  pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
  match identity remote address 192.168.0.20
  authentication remote pre-share
  authentication local pre-share
  keyring local FLEXVPN_KEYRING
  lifetime 86400
  dpd 10 2 on-demand
!
```



ةي طغت لالخ نم ىن دألا دحلا ىلا نـيوكـلـا زـيـمـلـا IKEv2 Smart Defaults FlexVPN لـلـقـتـ: حـيـمـلـتـ ىـلـعـ، ةـنـيـعـمـ IKEv2 Smart Defaults مـاـدـخـتـسـاـ تـالـاـحـ صـيـصـخـتـ كـنـكـمـيـ . مـاـدـخـتـسـاـ تـالـاـحـ مـظـعـمـ ةـسـرـامـمـلـاـ هـذـهـبـ يـصـوـتـ الـ Cisco نـأـنـمـ مـغـرـلـاـ.

تـانـاـيـبـلـاـ ةـيـاـمـحـلـ ةـمـدـخـتـسـمـلـاـ ةـئـزـجـتـلـاـ تـايـمـزـراـوـخـ وـرـيـفـشـتـلـاـ فـيـرـعـتـوـ Transport Set ءـاشـنـإـ دـ.

٥-- ءـاشـنـإـ IPsec profile.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
  mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
  set transform-set FLEXVPN_TRANSFORM
```

```
set ikev2-profile FLEXVPN_PROFILE
!
```

قفنلا ةهجاو نيوكتب مق .و.

```
!
interface Tunnel0
 ip address 10.1.120.10 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.20
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.10 255.255.255.0
!
```

نع نلعي نأ نكمي ، كلذ دعب . قفنلا ةهجاو نالعإلل يكيماني دلا هيجوتلا نيوكتب مق . ز . قفنلا ربع رمت نأ بجي يتلا ئرخألا تاكبشلا

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

هجوملا نيوكت: 2 ةوطخل

أ. IKEv2.

ريظنلا ةقداصمل ھمادختسإ متى a keyring لخدأو a keyring Pre-Shared Key . ب.

ج. ج عاشنإ keyring . IKEv2 profile نييعت و

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
 peer FLEVPNPeers
 address 192.168.0.10
 pre-shared-key local cisco123
 pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
```

```

match identity remote address 192.168.0.10
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!

```

دان ايبل ا ئيام حل ۋە مىختىمىلا تايىم زراو خەرى فېشىتلا فيرعت و ئاشندا.

اقبسم اهۋاشندا مت لېوحەت ۋە عومۇجىم و IKEv2 فېرعت فەلم نېيىعەت و ئاشندا.

```

!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
  mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
  set transform-set FLEXVPN_TRANSFORM
  set ikev2-profile FLEXVPN_PROFILE
!

```

نېوكتب مۇق. 9 Tunnel interface.

```

!
interface Tunnel0
  ip address 10.1.120.20 255.255.255.0
  tunnel source GigabitEthernet1
  tunnel destination 192.168.0.10
  tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
  ip address 192.168.0.20 255.255.255.0
!
```

نۇ نەلەپى نأ نەكمى ، كىلذ دىعە . قىفنلە ۋە جاونۇ نالعەلل يەكىمانى دىلا ھېجوتلا نېوكتب مۇق . 10 قىفنلە رېبىع رەمت نأ بېجي يەتلە يەخالا تاكبىشلى.

```

router eigrp 100
  no auto-summary
  network 10.1.120.0 0.0.0.255

```

قىقىحتىلا نەم قىقىحتىلا

- قىفنلە نأ نەم قىقىحتىلا و قىفنلە ۋە جاونۇ ئەللاج ۋە جارمەل رەمەل مىختىمىلا

ف يف up/up اح ظل.

<#root>

RouterB#

show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet1	192.168.0.20	YES	NVRAM	up	up
Tunnel0	10.1.120.11	YES	manual		

up

up

سا دختس م دخل رم م إكأتل show crypto ikev2 sa نيب نم آل ا لاصتالا عاشن ديكأتل جوجوملا تاهج.

<#root>

RouterB#

show crypto ikev2 sa

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvrif/ivrf	Status
2	192.168.0.20/500	192.168.0.10/500	none/none	

READY

Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/3139 sec

IPv6 Crypto IKEv2 SA

• ربع اهروم و تان ايبل رورم ةكرح ريفشت ديكأتل show crypto ipsec رم م دختسا لاصتالا عطق و نيمضتل تادادع ةدایز نم ققحتلا قيرط نع قفنل.

<#root>

RouterB#

show crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 192.168.0.20

```
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
current_peer 192.168.0.10 port 500
    PERMIT, flags={origin_is_acl,}

#pkts encaps: 669, #pkts encrypt: 669, #pkts digest: 669

#pkts decaps: 668, #pkts decrypt: 668, #pkts verify: 668

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.0.20, remote crypto endpt.: 192.168.0.10
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0x93DCB8AE(2480715950)
PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x89C141EB(2311143915)

    transform: esp-256-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 5578, flow_id: CSR:3578, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4607913/520)

    IV size: 16 bytes
    replay detection support: Y

status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x93DCB8AE(2480715950)

    transform: esp-256-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 5577, flow_id: CSR:3577, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4607991/3137)
```

```
IV size: 16 bytes
replay detection support: Y
```

```
status: ACTIVE(ACTIVE)
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

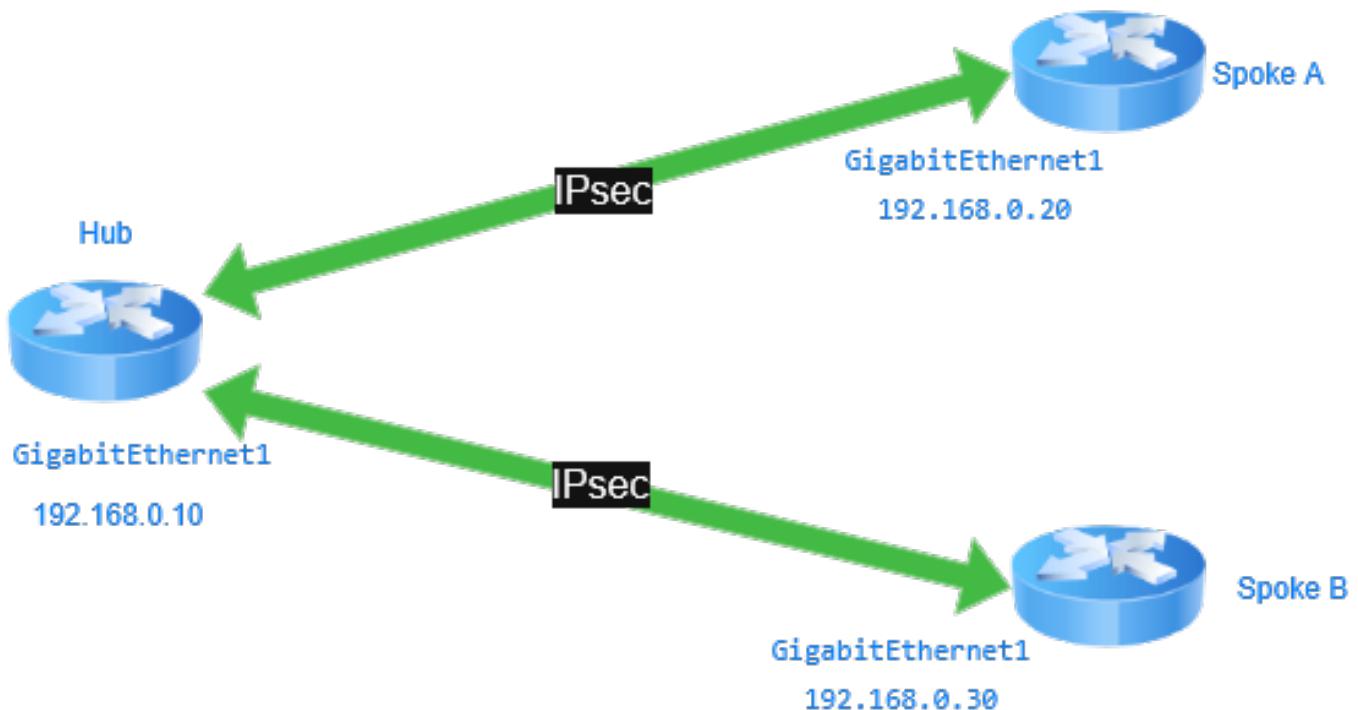
- رخآلا عقومل اع م EIGRP رواجت عاشن ديكأتل show ip eigrp neighbors رمألا مدخلتسأ.

```
RouterB#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
      H   Address           Interface      Hold Uptime      SRTT      RT0      Q      Seq
      0   10.1.120.10       Tu0            13  00:51:26    3        1470     0      2

```

FlexVPN ۋەينقتب Hub-and-Talk

نيوكتل اذه يزكرم زكرم ھجومب ۋەملكتم ۋەددىتم تاهجوم لصىتت، ططخم يف ۋەكپش يف. ھجوملاب اس اس أ ئىعرفلىا مداخلان اهيف لصىتت يىتلان تاهوي رانىسىلى يىلاتم عزوملار ئۆزۈمىي. لاصتا ئاعافك نىسحتل ئىكىمانىدىلار قافنالا نىوكت نكمى، FlexVPN، IKEv2 ھىجوت مىتىمكىو. سلس لاصتا نمىضى امم، ئىكەنلىك تاهجوملارلىك تاراسملارنىزوتل نىوكت مىتى فىكىو Talk و Hub نىب VPN لاصتا نىوكتلارنىزىشى، ططخملار يف هىلى ئراشىلا نم ديزملار ئافاضا ئىلع رداق هنأ امم، ۋەددىتم تاهبىج عم يكىمانىدىلاصتا عاشنالا عزوملار ئورفلار.



ل يطي طختلا مس رلا Hub_and_TALK_Diagram

عزملا نیوکت: 1: ۋوطخلار

أ. IKEv2.

ب. ماقبلا قداصلەمەمادختىسى مەتى a keyring لىخداو a Pre-Shared Key نیوکتىب.

```

crypto ikev2 proposal FLEXVPN_PROPOSAL
  encryption aes-cbc-256
  integrity sha256
  group 14
!
crypto ikev2 policy FLEXVPN_POLICY
  proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
  peer FLEVPNPeers
  address 0.0.0.0 0.0.0.0
  pre-shared-key local cisco123
  pre-shared-key remote cisco123
!
```

قىباشلا ضيوفت ئامدۇچ دەجىن ئامىدۇچ ئامسەل ئەملا FlexAuthl دەجىن ئامسەل ئەملا زاھىجلا نیوکت نەم تاسايىسلا دەجىن يېتلىك.

```

!
aaa new-model
```

```
aaa authorization network FlexAuth local
!
```

متي. 10.1.1.2 ىلإ IP address pool اونع يوتحي، مسFlexPool ناو نعFlexPool ديدحتب مق. د. تاونقلاب ةصالخلا قفنلا ةهجاوي لاإ اقلت IP ناو نع نيعتل عمجتل اذه مادختسا.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

ددحت. 10.10.1.0/24 ةكبش لـ FlexTraffic اهتمست متي ةيسايق IP لوصو ةمئاق ددح.. لوصولل FlexVPN تاهبج ىلإ اعفد متي يتلا تاكبشلا هذه لوصولا يف مكحتلا ةمئاق قفنلا ربع اهيلا.

```
!
ip access-list standard FlexTraffic
 permit 10.10.1.0 0.0.0.255
!
```

يف IP نيوانع عمجتو لوصولا ةمئاق ىلإ ۀراش إلأ ممت.

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

اهنييعتو AAA و keyring ليوخت ةعومجم IKEv2 profile عاشناب مق.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

تانا يبلا ئامحلا ئاملا ئازجتلا تاي مزراوخ وري فشتلا فيرعت ئاشنإ Transport Set.

اقبس م ئاشناب مقتاح IKEv2 profile نيي عت و ئاشنإ مقت ام Transport Set.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
  mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
  set transform-set FLEXVPN_TRANSFORM
  set ikev2-profile FLEXVPN_PROFILE
!
```

قيبطتو ك اول ا عجم IP unnumbered address ئاج هج اولا نيوكتب مق ط virtual-template 1 as type tunnel.

```
!
interface virtual-template 1 type tunnel
  ip unnumbered loopback1
  tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
  ip address 10.1.1.1 255.255.255.255
!
```

ب ثدحتلا مقت يذلا نيوكتلارا 2: ووطخلا

ا IKEv2 س اي س و حر تقم ديدحت.

ىلع ئقادص ملل 5 مادختسا مقت ياقبس م كرتشم حاتفم لخ دأو حيتافم ئاقلخ نيوكتب مق ب عزوملا.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
  encryption aes-cbc-256
  integrity sha256
  group 14
!
crypto ikev2 policy FLEXVPN_POLICY
  proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
  peer FLEVPNPeers
  address 0.0.0.0 0.0.0.0
  pre-shared-key local cisco123
  pre-shared-key remote cisco123
!
```

ةامسملا ةكبشلا ضيوفت ةمئاق ددح مث ،ةرصلأا هجوم ىلع AAA تامدخ نيكمنتب مق. FlexAuth نيوكت ةسأيس نيوكتب مق ،كلذ دعب .يلحملأا زاهجلأا نيوكت نم تاسأيسلا ددحت يتلا عورفلأا ىلإ تاراسملاو IP ناونع عفدل عضولا.

```
!
aaa new-model
  aaa authorization network FlexAuth local
!
```

10.20.2.0/24. اهتيمست متي يتلا ةيسأيق FlexTraffic لوصو ةمئاق ددح . د اذه ةطساوب اهتكراشم ممت يتلا تاكبشلا ٥ه (ACL) لوصولا يف مكحتلا ةمئاق ددحت قفنلا رباع رمتل ثدحتلا.

```
!
ip access-list standard FlexTraffic
  permit 10.20.2.0 0.0.0.255
!
```

يف لوصولا ةمئاق نيعت متي IKEv2 Authorization Policy.

```
!
crypto ikev2 authorization policy SpokePolicy
  route set interface
  route set access-list FlexTraffic
!
```

اهنيعتو AAA و ليوخت ةعومجم keyring عاشنا.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local FLEXVPN_KEYRING
  aaa authorization group psk list FlexAuth SpokePolicy
!
```

تانايبلأا ةيامحل ةمدختسملا ةئزجتلأا تايمزراوخ وريفسشتلا ديدحت ولقنو ةعومجم عاشنا . و اهؤاشنا مت يتلا لقnela ةعومجم و IKEv2 فيرعت فلم نيعت و IPsec فيرعت فلم عاشنا . اقبسم

```

!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
  mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
  set transform-set FLEXVPN_TRANSFORM
  set ikev2-profile FLEXVPN_PROFILE
!

```

لکشی وہ نأ عمجمتلا نم تلن نوکی يأ، ناونع ضوافت نم ئيصالخ عم نراق قفنلا تلکش ج. رصلالا ىلع.

```

!
interface tunnel 0
  ip address negotiated
  tunnel source GigabitEthernet1
  tunnel destination 192.168.0.10
  tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
  ip address 192.168.0.20 255.255.255.0
!

```

ڇھصلالا نم ڦڻھتلار

لوصولاو يرهاظلا بلاقلا او Tunnel عضولالا ڦعجارمل show ip interface brief رمألا مڌتسا يرهاظلا:

- تقلخ. ڦيادع يهولفسألل/ىلعألل ڦلاح ىلع يرهاظلا بلاقلا ڦوتحي، لصولا ڇھول ىلع Virtual-Access ڦلاح يدبيو رصلالا عم ليصوت سسُؤي نأ لک ل Talk up/up.
- عضو up/up يدبيو ناونع قفنلا نراق تملتسا، لالا ىلع Talk.

<#root>

FlexVPN_HUB#

show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet1	192.168.0.10	YES	NVRAM	up	up
GigabitEthernet2	10.10.1.10	YES	manual	up	up
Loopback1	10.1.1.1	YES	manual	up	up
virtual-Access1	10.1.1.1	YES	unset	up	up
<<<<< This Virtual-Access has been created and is up/up					
Virtual-Template1	10.1.1.1	YES	unset	up	

```

FlexVPN_Spoke#
show ip interface brief

Interface          IP-Address      OK? Method   Status      Protocol
GigabitEthernet1  192.168.0.20   YES NVRAM    up          up
GigabitEthernet2  10.20.2.20    YES manual   up          up
Tunnel10          10.1.1.8      YES manual   up          up <<<<<

```

The tunnel interface received an IP address from pool defined

- ملكتمل او ةرصلا نيب نمآل ا لاصتالا عاشن ديكأتل show crypto ikev2 sa رمألا مدخلتسا.

<#root>

```

FlexVPN_HUB#
show crypto ikev2 sa

IPv4 Crypto IKEv2 SA

Tunnel-id Local           Remote          fvrf/ivrf      Status
1           192.168.0.10/500 192.168.0.20/500 none/none

READY

```

Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/587 sec

IPv6 Crypto IKEv2 SA

- رباع اهروم و تانايبل رورم ڈكوح ريفشت ديكأتل show crypto ipsec رمألا مدخلتسا.
لاصتالا عطقو نيمضتلابا تايلمع تادادع ةدائيز نم ققحتلا قيرط نع قفنلابا.

<#root>

```

FlexVPN_HUB#
show crypto ipsec sa

interface: Virtual-Access1

Crypto map tag: Virtual-Access1-head-0, local addr 192.168.0.10

protected vrf: (none)

```

```
local ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
current_peer 192.168.0.20 port 500
    PERMIT, flags={origin_is_acl,}

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.0.10, remote crypto endpt.: 192.168.0.20
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0xAFC2F841(2948790337)
PFS (Y/N): N, DH group: none
```

inbound esp sas:

spi: 0x7E780336(2121794358)

```
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 5581, flow_id: CSR:3581, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-h
```

sa timing: remaining key lifetime (k/sec): (4607998/3010)

```
IV size: 16 bytes
replay detection support: Y
```

status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xAFC2F841(2948790337)

```
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 5582, flow_id: CSR:3582, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-h
```

sa timing: remaining key lifetime (k/sec): (4607998/3010)

```
IV size: 16 bytes
replay detection support: Y
```

STATUS: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

- مداخلة إلى تاراسملاء عفد نم ققحتلل show ip route رمألا مدخلتسأ:
 - ةعومجم ٥٥ جاوناي ب ببسن IKEv2 نيوكت تالو مح رب 10.1.1.1/32 ل راسملاء عفد مت.
 - ةرصلان يوكت يف تاراسملاء.
 - ةرصلان يوكت يف تاراسملاء عومجم FlexTraffic.

<#root>

```
FlexVPN_Spoke#show ip route
<<< Omitted >>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
      s     10.1.1.1/32 is directly connected, Tunnel0    <<<<<
      C     10.1.1.8/32 is directly connected, Tunnel0
      s     10.10.1.0/24 is directly connected, Tunnel0  <<<<<
      C     10.20.2.20/32 is directly connected, GigabitEthernet2
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
      C     192.168.0.0/24 is directly connected, GigabitEthernet1
      L     192.168.0.20/32 is directly connected, GigabitEthernet1
```

- اهنع نلعملاء تاكبشنلاب لاصتنالا نم ققحتلل ping رمألا مدخلتسأ.

<#root>

```
FlexVPN_HUB#
ping 10.20.2.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
FlexVPN_Spoke#
```

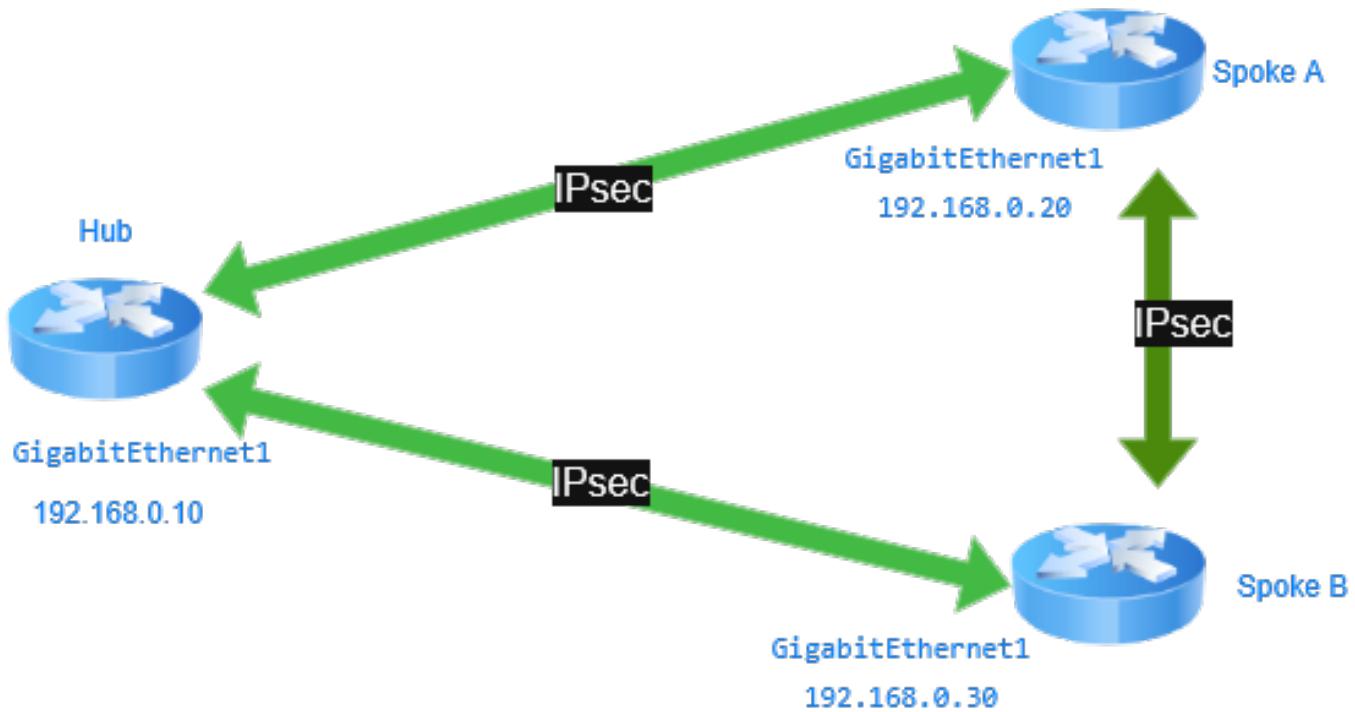
```
ping 10.10.1.10
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

ثدحتي يذلا FlexVPN ىلإ ثدحت

(مالكلاب لاصتالا) ئينقت تاذ ئيفيصوت و ئيروحم ئكبش يف FlexVPN ئكبش لمعن ئيرهاظلا ئصالخا ئكبش لل نمآل او ريوطتلل لباقل او يكيمانيدلا لاصتالا نيكىمت ىلع نع مالعتسالاب تاملكلل NHRP حمسى ثىج ئيزكرم مكحى ئطقنىك ئرصلالا لمعي و (VPN). لاعفلالا لصاوتتلل IPsec قافنأ ربعة ئرشابم ئداحم حيثى امم، ئرخأ IP نيowanعل ئرصلالا ريخأتلا ليلقتو.

نيسحت، ئيناكما ئداحم ىلإ ئرشابم لقان رطخي نأ رمألا تلمعتسا، ئرصلالا ىلع ip مەل حمسىت، دافصىللا ىلع. تانايىبلالا ىوتسم رورم ئكرح ئرصلالا زواجتب رورملالا ئكرح قفت ئىقلت دعب ئرخألا ديداخألا عم يكيمانيدل كشب ئرشابم قافنأ ئئيەتبا ئدايىقلالا، ئدحتل او زكرملالا نىب رورملالا ئكرح ىلإ يطيطختلارىشى. ئرصلالا نم ھيجوتلار ئدعا، ئداحم ىلإ ئدحتي و.



_talk_talk_diagram

عزملا نىوكت: 1 ئوطخلالا

تافیصوتو IKEv2 تاسایس فیرعت.

عورفل ا قداصمل ھمادختس! متي a keyring Pre-Shared Key a لخداو نیوکتب مق. ب.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
    encryption aes-cbc-256
    integrity sha256
    group 14
!
crypto ikev2 policy FLEXVPN_POLICY
    proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
    peer FLEVNPees
    address 0.0.0.0 0.0.0.0
    pre-shared-key local cisco123
    pre-shared-key remote cisco123
!
```

FlexAuth ةامسمل ا كبسلا ضيوفت ةمئاق ددح مث ، عزوملا هجوم ىلع AAA تامدخ نيكمنتب مق. c. عضولا نیوکت ةسایس نیوکتب مق مث ، يلحملا زاهجلانیوکت نم تاسایسلار ددحت يتلا عورفل ا ىلإ تاراسمل او IP ناونع عفدل FlexVPN.

```
!
aaa new-model
    aaa authorization network FlexAuth local
!
!
```

FlexPool 10.1.1.2 نیوانعل ا ىلع يوتحي IP address pool، ئىمسىم ناونع ديدحتب مق. د. تاونقلاب ةصالخا قفنل ا ٽهوجاول ا ايئاقلت IP ناونع نييعتل عمجمتل ا اذه مادختس! متي

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

FlexTraffic اهتيمست متي يتلا ةيسياقل ا IP لوصو ةمئاق ديدحتب مق ..-0.0.0.0/8. ئيل اهعفد متي يتلا تاكبسلا هذه (ACL) لوصولا يف مكحتل ا ةمئاق ددحت كلذل ، وجوملاب ةلصتملا ئرخألا عورفلاب ةصالخا تاكبسلا كلذ يف امب FlexVPN، تاكبسلا اولاؤ عزوملا لالخ نم تاكبسلا هذه ئيل ا لوصولا متي هنأ تالوحمل ا فرعت.

```
!
ip access-list standard FlexTraffic
    permit 10.0.0.0 0.255.255.255
```

!

يُف اهنِي ييُعَت IP address pool مُتي و لوصول ا ةمئاق.

!

```
crypto ikev2 authorization policy HUBPolicy
  pool FlexPool
  route set interface
  route set access-list FlexTraffic
```

!

اهنِي ييُعَت و AAA و keyring لِي و خَتَ و مَجْمَعِي IKEv2 profile عَاشَنَا و.

!

```
crypto ikev2 profile FLEXVPN_PROFILE
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local FLEXVPN_KEYRING
  aaa authorization group psk list FlexAuth HUBPolicy
  virtual-template 1
```

!

تَانِيَابْلَا ةِيَامِحْلَة مَدْخَلَة سَمْلَا ةِيَزْجَتَلَا تَايِمِزْرَاوَخَو رِيَفْشَتَلَا فِيَرَعَتَو Transport Set عَاشَنَا ز.

قَبَاس عَاشَنَا ح. IKEv2 profile و Transport Set نِيِيُعَت، IPsec profile عَاشَنَا ح.

!

```
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
  mode tunnel
```

!

```
crypto ipsec profile FLEXVPN_PROFILE
  set transform-set FLEXVPN_TRANSFORM
  set ikev2-profile FLEXVPN_PROFILE
```

!

قِيَبَطَتِبْ مَقْوِيَّه جَأَوَكْ ةَهَجَأَوَلَا عَجَارْ نِيِوكَتِبْ مَقْ. IP unnumbered address IPsec profile virtual-template 1 as type tunnel.

عِم رِشاَبِم لِاصَتِا عَاشَنَابْ مَدَوْخَلَا مَالِعَاءَلْ يِرَهَاطَلَا بَلَاقَلَا ip nhrp redirect اهتاكَبَشِىلِ لَوْصَوْلَى عَوْرَفَلَا.

!

```

interface virtual-template 1 type tunnel
  ip unnumbered loopback1
  ip nhrp network-id 1
  ip nhrp redirect
  tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
  ip address 10.1.1.1 255.255.255.255
!

```

نیوکت نع ثدحت: 2 ۋەطخلا

تافیصوتو IKEv2 تاسایس فىرعت.

عورفلار ئۇچداشىملىك مادختسى مىتى a keyring Pre-Shared Key لىخ داۋ نیوکت بىمۇق.

```

crypto ikev2 proposal FLEXVPN_PROPOSAL
  encryption aes-cbc-256
  integrity sha256
  group 14
!
crypto ikev2 policy FLEXVPN_POLICY
  proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
  peer FLEVNPeers
  address 0.0.0.0 0.0.0.0
  pre-shared-key local cisco123
  pre-shared-key remote cisco123
!
```

FlexAuth ئامسەملە ئەكباشلا ضىوفت ئەمىئاقدىچىم دىجىمە ، ئەرسىلە جومىلىع AAA تامىخ نىكەمتبىمۇق. نیوکت ئەسایس نیوکت بىمۇق ، كىلذىدۇب . يىلەملا زاھىجلا نیوکت نم تاسایسلىدا دىجىت يىتلە عورفلار ئىلە تاراسەملارو IP ناونۇ عەفدىل عضۇلما.

```

!
aaa new-model
  aaa authorization network FlexAuth local
!
```

FlexTraffic 10.20.2.0/24. اهتىمىست مىتى يىتلە ئەسایق IP لۈوصۈ ئەمىئاقدىچىم دىجىمە . عەطقىملا اذە ئەتساوب اهتكاراشم مەتت يىتلە تاكباشلا ھەزەلۈنىڭلە يىف مەكتەلە ئەمىئاقدىجىت قىفنەلە رېبىع رەمتلە.

```

!
ip access-list standard FlexTraffic
```

```
permit 10.20.2.0 0.0.0.255
```

```
!
```

يـف لـوصـولـا ةـمـئـاق نـيـيـعـت مـتـيـ.

```
!
```

```
crypto ikev2 authorization policy SpokePolicy
  route set interface
  route set access-list FlexTraffic
!
```

اهـنـيـيـعـتـو AAA وـلـيـوـخـتـو keyring عـاـشـنـا .5.

```
!
```

```
crypto ikev2 profile FLEXVPN_PROFILE
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local FLEXVPN_KEYRING
  aaa authorization group psk list FlexAuth SpokePolicy
  virtual-template 1
!
```

تـانـاـيـبـلـا ةـيـامـحـلـا ةـمـدـخـتـسـمـلـا ةـئـرـجـتـلـا تـايـمـزـرـاـخـو رـيـفـشـتـلـا فـيـرـعـتـو Transport Set عـاـشـنـا .9.

اهـؤـاشـنـا مـتـ يـتـلـا لـقـنـلـا ةـعـوـمـجـمـو IKEv2 فـيـرـعـتـو IPsec فـيـرـعـتـو ، فـلـمـ نـيـيـعـتـو ، g. اـقـبـسـمـ.

```
!
```

```
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
  mode tunnel
!
```

```
!
```

```
crypto ipsec profile FLEXVPN_PROFILE
  set transform-set FLEXVPN_TRANSFORM
  set ikev2-profile FLEXVPN_PROFILE
!
```

مـتـ يـتـلـا Virtual-Template1 VTls دـدـحـ . يـرـهـاـظـلـا بـلـاـقـلـا وـ tunnelinterface tunnel0 tunnel shortcuts . اـضـيـأـ معـدـلـ اـهـؤـاشـنـا .

لـكـشـبـ ةـرـشـابـمـ قـافـنـا عـاـشـنـا نـمـ اـهـنـيـكـمـتـلـ تـالـوـحـمـلـا يـلـعـ ip nhrp shortcut . اـدـانـتـسـا يـخـأـلـا تـالـوـحـمـلـا يـلـا يـكـيـمـانـيـدـ .

```

!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.20 255.255.255.0
!

```

نیوکتلایف ثدحت: 3 ۋەطخلا B

تافیصوتو IKEv2 تاسایس فىرعت.

عورفلار ئۇچداشىملىك مادختسى! مىتىي a keyring Pre-Shared Key لىخداو نیوکتب مق ب.

```

crypto ikev2 proposal FLEXVPN_PROPOSAL
encryption aes-cbc-256
integrity sha256
group 14
!
crypto ikev2 policy FLEXVPN_POLICY
proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVNPees
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

قايسىمىلا ئېنىشلىكا ضىوفت ئەمئاق ددح مىت، عزومىلا ھجوم ىلۇ AAA تامىخ نىكمىت بمق. FlexAuth عضولالا نیوکت ئاسایس نیوکتب مق مىت، يىلەملى زاھىجلا نیوکت نىم تاسایسلىدا ددحت يىتلە عورفلار ئىلە تاراسىملىك او IP ناونع عىفادىل.

```

!
aaa new-model
 aaa authorization network FlexAuth local
!
```

حامسل او اهتيمست مت ي يتلا ئيردنكس إلاب ئصالا IP لوص و ئومئاق ديدحت بمق. دمتت يتلا تاكبشلارا مكحولى يف مكحولى ئومئاق ددخت 10.30.3.0/24. ئوكبشلل قفنلاربع رمتل عطقملارا اذه ئطساوب اهتكراشم.

```
!  
ip access-list standard FlexTraffic  
permit 10.30.3.0 0.0.0.255  
!
```

يىف لوصولارا ئومئاق ئىلا ئراشىلا مىتت IKEv2 Authorization Policy.

```
!  
crypto ikev2 authorization policy SpokePolicy  
route set interface  
route set access-list FlexTraffic  
!
```

اهنېيۇتىو و AAA keyring ئۈچۈن ئەنلىك ئەمچەنە.

```
!  
crypto ikev2 profile FLEXVPN_PROFILE  
match identity remote address 0.0.0.0  
authentication remote pre-share  
authentication local pre-share  
keyring local FLEXVPN_KEYRING  
aaa authorization group psk list FlexAuth SpokePolicy  
virtual-template 1  
!
```

تانايىبلارا ئاماحل ئەم دختسەملە ئۆزجىتلارا ئايىمىزراوخ و رىفشتىلارى فىرىعتىو ئاشنە.

قىباسى ئاشنە و ئەنلىك ئەمچەنە IKEv2 profile IPsec profile و ئەنلىك ئەمچەنە Transport Set.

```
!  
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac  
mode tunnel  
!  
crypto ipsec profile FLEXVPN_PROFILE  
set transform-set FLEXVPN_TRANSFORM  
set ikev2-profile FLEXVPN_PROFILE  
!
```

دنسی نأ تقلخ نوکی نأ tunnel interface AND virtual template. ددح Virtual-Template1 ل dVTIs نیوکت مقت. ح NHRP shortcuts. tunnel0 اونعک tunnel virtual-template.

لکشب ۋرشابم قافنأ عاشنأ نم اهنيكمتل تالوحملارىل ع ip nhrp shortcut رمألا نیوکت متى ئەرچىوت ئەداعا لىاسرىلى ادانتسا ئىخالا تالوحملارىل يكىمانىد.

```
!
interface tunnel 0
    ip address negotiated
    ip nhrp network-id 1
    ip nhrp shortcut virtual-template 1
tunnel source GigabitEthernet1
tunnel destination 192.168.0.10
tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
    ip unnumbered tunnel0
    ip nhrp network-id 1
    ip nhrp shortcut virtual-template 1
tunnel source GigabitEthernet1
tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.30 255.255.255.0
!
```

ۆحصىلا نم ققحتلا

لوصول او يرهاظلا بلاقلا او Tunnel عضولارىجا رمألا مدختسا: ئەباطخلاب رشابم لاصتا كلانه، نآل او يرهاظلا

- عاشنأ متى. ئەداع يەولفسا/ىل ع يرهاظلا بلاقلا يوتحى، تالوحملارىل "يرهاظلا لوصولا" up/up.

<#root>

FlexVPN_Spoke#

show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet1	192.168.0.30	YES	NVRAM	up	up
GigabitEthernet2	10.20.2.20	YES	manual	up	up
Tunnel0	10.1.1.12	YES	manual	up	up
Virtual-Access1	10.1.1.12	YES	unset	up	up
Virtual-Template1	10.1.1.12	YES	unset	up	down

- زاھج لک نیب نمآلا لاصتالا عاشن| دیکأتل show crypto ikev2 sa رمآلا مدخلتسا.
 - ربع اهروم و تانایبل رورم ڈکرھ ریفشت دیکأتل show crypto ipSec رمآلا مدخلتسا.
 - لاصتالا عطقو نیممضتلہ تايلمع تادادع ڈایز نم ققحتلہ قیرط نع قفنلہ.
 - عورفلہ نیب رورملہ ڈکرھ ھیجوت ڈداعا نم ققحتلہ show ip nhrp رمآلا مدخلتسا.
- <#root>

```
FlexVPN_Spoke#
```

```
show ip nhrp
```

```
10.1.1.10/32 via 10.1.1.10
    Virtual-Access1 created 00:00:13, expire 00:09:46
    Type:
```

```
dynamic
```

```
, Flags: router nhop rib nho
    NBMA address: 192.168.0.30
```

```
10.30.3.0/24 via 10.1.1.10
```

```
Virtual-Access1 created 00:00:13, expire 00:09:46
Type:
```

```
dynamic
```

```
, Flags: router rib nho
    NBMA address: 192.168.0.30
```

ةثداحملہ یلإ تاراسملہ عفد نم ققحتلہ show ip route رمآلا مدخلتسا:

- تاراصتخاب ناطبتری و نیدیج نیقیرطب Virtual-Access1 ڈھجاوپ ناراسملہ نرتقیو NHRP.
- ڈیلاتلہ ڈوطلخلا زواجت یلإ٪ فرعلہ ریشی.

<#root>

```
FlexVPN_Spoke#sh ip route
```

```
<<< Omitted >>>
```

```
Gateway of last resort is 192.168.0.1 to network 0.0.0.0
```

```
S*   0.0.0.0/0 [1/0] via 192.168.0.1
    10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
S     10.0.0.0/8 is directly connected, Tunnel0
S     10.1.1.1/32 is directly connected, Tunnel0
```

```
s %   10.1.1.10/32 is directly connected, Virtual-Access1
```

```
C     10.1.1.12/32 is directly connected, Tunnel0
C     10.20.2.20/32 is directly connected, GigabitEthernet2
```

```
s %   10.30.3.0/24 is directly connected, Virtual-Access1
```

```
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C      192.168.0.0/24 is directly connected, GigabitEthernet1
L      192.168.0.30/32 is directly connected, GigabitEthernet1
```

- اهنع نلعمل ا تاکبشلاب لاصتالا نم ققحتلل ping رمألا مدخلتساً.

```
<#root>
```

```
FlexVPN_Spoke#
ping 10.30.3.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.3.30, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

اهحالص او عاطخألا فاشكتسا

مدخلتساً. اهحالص او نيوكتل ا عاطخأ فاشكتسا ال اهمادخلتسا لـ نـ كـ مـ يـ تـ اـ مـ وـ لـ عـ مـ مـ سـ قـ لـ اـ اـ ذـ رـ فـ وـ يـ مـ دـ خـ تـ سـ اـ . قـ فـ نـ لـ اـ ضـ وـ اـ فـ تـ ةـ يـ لـ مـ عـ عـ اـ طـ خـ اـ حـ يـ حـ صـ تـ لـ رـ مـ اوـ لـ اـ هـ ذـ هـ

```
debug crypto interface
```

```
debug crypto ikev2
debug crypto ikev2 client flexvpn
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ikev2 packet

debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message
debug crypto ipsec states
```

متى يتلا تالاصتالا عاطخأ فاشكتساً يف NHRP عاطخأ حيحصت تاييلمع دعاست نـ كـ مـ يـ

```
debug nhrp
debug nhrp detail
debug nhrp event
debug nhrp error
debug nhrp packet
debug nhrp routing
```

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).