

تاكبشلا عم عقوم ىلإ عقوم نم لاصتال Cisco Secure Access في ةلخادتملا ةيعرفلا

تايوتحمل

[عمدقملا](#)

[ةيساسال تابلطتملا](#)

[تابلطتملا](#)

[عمدختسملا تانوكملا](#)

[عدبلال لبقي](#)

[ريضحتلا او دادعلا](#)

[نئيوكتلا تاوطخ](#)

[Cisco نم نمالا لوصولا نئيوكت](#)

[ةيامحل رادج نئيوكت](#)

[قلص تاذا تاملول عم](#)

عمدقملا

Cisco نم نمالا لوصول ةلخادتملا ةيعرفلا ةكبشلا لح دنتسملا اذه فصلي

ةيساسال تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيذل نوكت نأ Cisco ي صوت

- Cisco نم نمالا لوصول ةرادإ
- هجوملا / ةيامحل رادج ةرادإ

كيذل نوكتي نأ Cisco ي صوت

- Cisco Secure Access ىلإ يرادإلا لوصول
- (هجوملا وأ ةيامحل رادج) IPSec ب ةصاخلا شبل او لابقتسالا ةدحو زاهج ىلإ يرادإلا لوصول

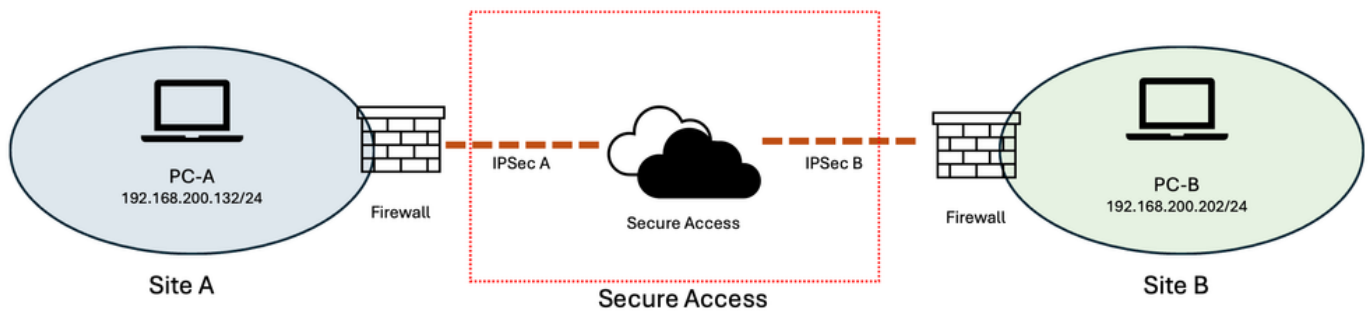
عمدختسملا تانوكملا

ةنعم ةي ءام ءانوكم وءارب ءاراءصا اىلع ءنءسملا اءه رصءق اىل

ةصاخ ةي لمعم ةئيىب اىف ءءوءوملا ةزهءال نم ءنءسملا اءه اىف ءءراول ءامولعمل ءاشنم ءنءا ءا (اىضارءفا) ءوسمم نىوكءب ءنءسملا اءه اىف ءمءءءسملا ةزهءال اىمء ءا ءب رما اىل لمءءملا رىءاءلل كمءف نم ءكاأءف ،لئغشءل ءىق ءءءبش

ءءبلا لبق

اهسفن ةي عرفل IP ءءبش امهل نافلءءم نائىعرف ناعقوم ءانه ،لاءملا اءه اىف IPSec قفن ربء Cisco نم نمال لوصولاب لاصءالا امءف مءى اىءلاو ،192.168.200.0/24 لصفنم



ةءبش لىل اىطىءءل مسرلا - ةروص

ءءوءوملا ءراوملا اىل لوصولا نم "فل ءقوملا" نم نىمءءءسملا نىءمء وه ءلء نم فءءلاو سءءلاب قاصءالا نمو "ءاب ءقوملا" اىف

رىضءءلا ءاءءالا

ءءاسم ءنءمء ،(192.168.200.0/24) ةي عرفل IP ءءبش سفن نامءءءسى نىءقوملا الء نال نىيىءمءى ،لءاءءل اءه لءل .نئىءقوملا نىب رشابملا لاصءالا ءلءاءءملا ناونءلا ءقوملء اىف ءراوملا لئءمءل نئىلءاءءم رىغ نئىءىرهظ نئىءىعرف نئىءبش

لاءملا لئببس اىلع

• 10.30.30.0/24 :ءقوملا

• 10.40.40.0/24 : ب عقومال

• 192.168.200.0/24 : نيعقومال الك يف ةيلعفل ةيعرفال ةكبشال

دراومال رمتست امنيب عقوم ل كل ةديرف ناو نع تاحاسم ةيرهافل ةيعرفال تاكبشال رفوت
ةدوجومال 192.168.200.0/24 نيوانع مادختسإ يف ةيلعفل

مدختسمال موقى B، عقومال يف دوجوم دروم ىلإ لوصولاب A عقومال يف مدختسم موقى ام دنع
نم الدب (10.40.40.0/24) B عقومال ةيرهافل ةيعرفال ةكبشال لال خ نم درومال ىلإ لوصولاب
ةلخادتمال 192.168.200.0/24 ناو نعل ةحاسمل رشابمالم مادختسال

يتال (D-NAT) ةدحاو ىلإ ةدحاو ةهجو (NAT) ةكبش ةهجاو ةقاطب ةزيم Cisco Secure Access رفوي
هل D-NAT ناو نع قاطن. ةلباقملا ةيقيقحلال نيوانعل ىلإ ةيرهافل نيوانعل ةمجرت انه كم
ةيلعفل ةيرهافل تاكبشال دعت، لاثملا اذه يف. ةيلصلال ةيعرفال ةكبشال مجح سفن
ةيقيقحلال ةيرهافل IP نيوانع نيوب دحاو ىلإ دحاو طيخت رفوي امم، 24/ ةيعرف تاكبش

للا ثمل لىبس ىلع

10, 40, 40, 202 → 192, 168, 200, 202

امم، 192.168.200.202 ىلإ 10.40.40.202 ل هجومال A عقومال نم ابلاط D-NAT مجرتي، يلاتلابو
الك مادختسإ نم مغرلا ىلعل B عقومال يف لباقملا درومال ىلإ لوصولاب بلطلل حمسي
ةيساسال ةيعرفال IP ةكبش سفنل نيعقومال

ىلع ظافحل عم عقوم ل كل ةلخادتم ريغ ةيضارتفا ناو نع ةحاسم عاشنا ىلع جهنلا اذه لمعي
نيوانعل ةيضارتفال نيوانعل نيوب ةقسانتم ةقالع رفوي امك. دراوملل ةيلالحال IP ةنونع
اهالصل ءاطخال فاشكتساو ةرادلال مةفلل لهسا نيوكتل لعجي امم، ةيقيقحلال

نيوكتل تاو طخ

ويرانيسلا اذه قيقحت بلطتي، Cisco نم نمآال لوصولا دويقوي لالحال ميمصتلل ارطن
نم نمآال لوصولا IPsec قافنا فلخ ثبلالو لابقتسال ةدحو ةزهجأ نم لك ىلع نيوكتل
Cisco.

لوصولل IPsec قفن عاشناب موقى يذال هجومال وأ ةيامحل رادج وه ثبلالو لابقتسال ةدحو زاهج
رادج موقى نأ بجي، Cisco Secure Access يف D-NAT نيوكت ىلإ ةفاضلابل Cisco نم نمآال
ةدئاعال رورملا ةكرحل (S-NAT) ردصم لل NAT ذيفنتب اضيأ ثبلالو لابقتسال ةدحو ةيامح

نيمسق نم نيوكتل نوكتي كلذل

1. لصفنم لكشب قفن ةكبش لكل ذفنم نمأي cisco في NAT (D-NAT) ةياغ لكشي
2. إلى عجار رورم ةكرح عجري نأ نمضي نأ ةيامحل ناردج ىلع NAT (S-NAT) ردصم لكشي
ةحاسم ناو نع ىلعفل

Cisco نم نمآلا لوصولا نيوكت

ةكبشلا تالاصتإ > لاصلتالا إلى لقتنا Cisco، نم نمآلا لوصولا ةرادإ لخدم نم: 1 ةوطخلا
ةكبشلا قفن تاعومجم بيوبتلا ةمالع ددحو

مدختسي يذلل عقوملل IPsec قفنب ةنرتقملا ةكبشلا قفن ةعومجم ريحتب مق: 2 ةوطخلا
ةلخادتملا ةيعرفلا ةكبشلا

لثمل اذه في

• A عقوملل ةكبشلا قفن ةعومجم = IPSec-A

• B عقوملل ةكبشلا قفن ةعومجم = IPSec-B

ةبولطملا ةكبشلا قفن ةعومجم ل ةرواجملا ثالثلا طاقنلا تاذ ةمئاقلا قوف رقنا: 3 ةوطخلا
ريحت ددحو

ناو نع ةمچرت نيكم تب مقو هيچوت بيوبتلا ةمالع ددح، ىرسىلا ةمئاقلا نم: 4 ةوطخلا
لعللاب ةنكمم نكت مل اذا (NAT) ةكبشلا

تانييت ةفاضإ رقنا، ةهچولل NAT تانييت تحت: 5 ةوطخلا

ةكبش قفن ةعومجم لكل D-NAT تانييت نيوكتل لودجلا اذه مدختسأ: 6 ةوطخلا

IPSec قفن - B عقوملا	IPSec قفن - A عقوملا	
→ عقوملا إلى نمآلا لوصولا 10.30.30.0/24 لىلصألا CIDR 192.168.200.0/24 مچرتملا CIDR	→ عقوملا إلى نمآلا لوصولا 10.40.40.0/24 لىلصألا CIDR 192.168.200.0/24 مچرتملا CIDR	NAT-1 ةياغلا
نمآلا لوصولا → عقوم 192.168.200.0/24 لىلصألا CIDR	نمآلا لوصولا → عقوم 192.168.200.0/24 لىلصألا CIDR	NAT-2 ةياغلا

CIDR مجرتم ال 10.40.40.0/24		CIDR مجرتم ال 10.30.30.0/24																																
Destination NAT Mappings <table><thead><tr><th>Name</th><th>Direction</th><th>Original CIDR</th><th>Translated CIDR</th><th></th></tr></thead><tbody><tr><td>> Site-B-1</td><td>Site → Secure Access</td><td>10.30.30.0/24</td><td>→ 192.168.200.0/24</td><td>⌵ ⌶</td></tr><tr><td>> Site-B-2</td><td>Secure Access → Site</td><td>192.168.200.0/24</td><td>→ 10.40.40.0/24</td><td>⌵ ⌶</td></tr></tbody></table>		Name	Direction	Original CIDR	Translated CIDR		> Site-B-1	Site → Secure Access	10.30.30.0/24	→ 192.168.200.0/24	⌵ ⌶	> Site-B-2	Secure Access → Site	192.168.200.0/24	→ 10.40.40.0/24	⌵ ⌶	Destination NAT Mappings <table><thead><tr><th>Name</th><th>Direction</th><th>Original CIDR</th><th>Translated CIDR</th><th></th></tr></thead><tbody><tr><td>> Site-A-1</td><td>Site → Secure Access</td><td>10.40.40.0/24</td><td>→ 192.168.200.0/24</td><td>⌵ ⌶</td></tr><tr><td>> Site-A-2</td><td>Secure Access → Site</td><td>192.168.200.0/24</td><td>→ 10.30.30.0/24</td><td>⌵ ⌶</td></tr></tbody></table> Rows per page 30 < 1 >		Name	Direction	Original CIDR	Translated CIDR		> Site-A-1	Site → Secure Access	10.40.40.0/24	→ 192.168.200.0/24	⌵ ⌶	> Site-A-2	Secure Access → Site	192.168.200.0/24	→ 10.30.30.0/24	⌵ ⌶	
Name	Direction	Original CIDR	Translated CIDR																															
> Site-B-1	Site → Secure Access	10.30.30.0/24	→ 192.168.200.0/24	⌵ ⌶																														
> Site-B-2	Secure Access → Site	192.168.200.0/24	→ 10.40.40.0/24	⌵ ⌶																														
Name	Direction	Original CIDR	Translated CIDR																															
> Site-A-1	Site → Secure Access	10.40.40.0/24	→ 192.168.200.0/24	⌵ ⌶																														
> Site-A-2	Secure Access → Site	192.168.200.0/24	→ 10.30.30.0/24	⌵ ⌶																														
D-NAT نيوكت - IPsec B ق فن عقوم		D-NAT نيوكت - IPsec A ق فن عقوم																																


 ةذفان روهظ دنع .ظفح ىلع رقنا ،ةكبش ق فن ةعومجم لك تادادع| نيوكت دعب :ةظحالمةكبشال ق فن ةعومجمل هسفن ءارجال راركت .رييغتال ديكتأل Update لخدأ ،ديكتألال ىرأل

ةيماحل رادج نيوكت

ةيعرفال IP تالكبش ةجلاعم في لالاح ديدحت دوجو ببسب بولطم ةيماحل رادج نيوكت .ةكبشال قافنأ ءاعومجم فلخ ءلخادتمال

ملسي نأ ناونع تلمعتسا ةياغل ،مداق طبر ىلع Cisco Secure Access D-NAT زجني امدنع ءكرحل ايئاقلت ءلباقملا ةيسكعلا ءمجرتلال ءارجا متي ال ،كلذ عمو .دروم ةياغلا ىلإ طبرلل اذه ءلخادتملا ةيعرفال ءكبشال وييرانيس في ءارجال رورم

ةيماحل رادج ىلع NATed ردصم ايودي ءعجترملا رورم ءكرح نوكت نأ بجي ،كلذل ءجيتنو

يرهاظل IP ناونع مادختساب ءارجال رورم ءكرح ءهوجلل مداخال ىري نأ وه بولطملا يساسأل رملال مداخلل ىلعفل IP ناونع نم ال دب ،لصلال في هيلإ لوصولاب ليمعلا ماق يذلا

لاثم

يلي ام ضارتاب

- 192.168.200.132 A: عقوملا ليمع
- 192.168.200.202 ب: عقوملا بيومداخ
- 10.40.40.0/24 B: عقوملل يرهاظل ةيعرفال ءكبشال
- 10.40.40.202 ب: يولل مداخل يرهاظل ناونعلا

مادختساب (ب) عقوملا بيومداخ ىلإ لوصولاب (أ) عقوملا في ليمعلا موقي
<https://10.40.40.202>

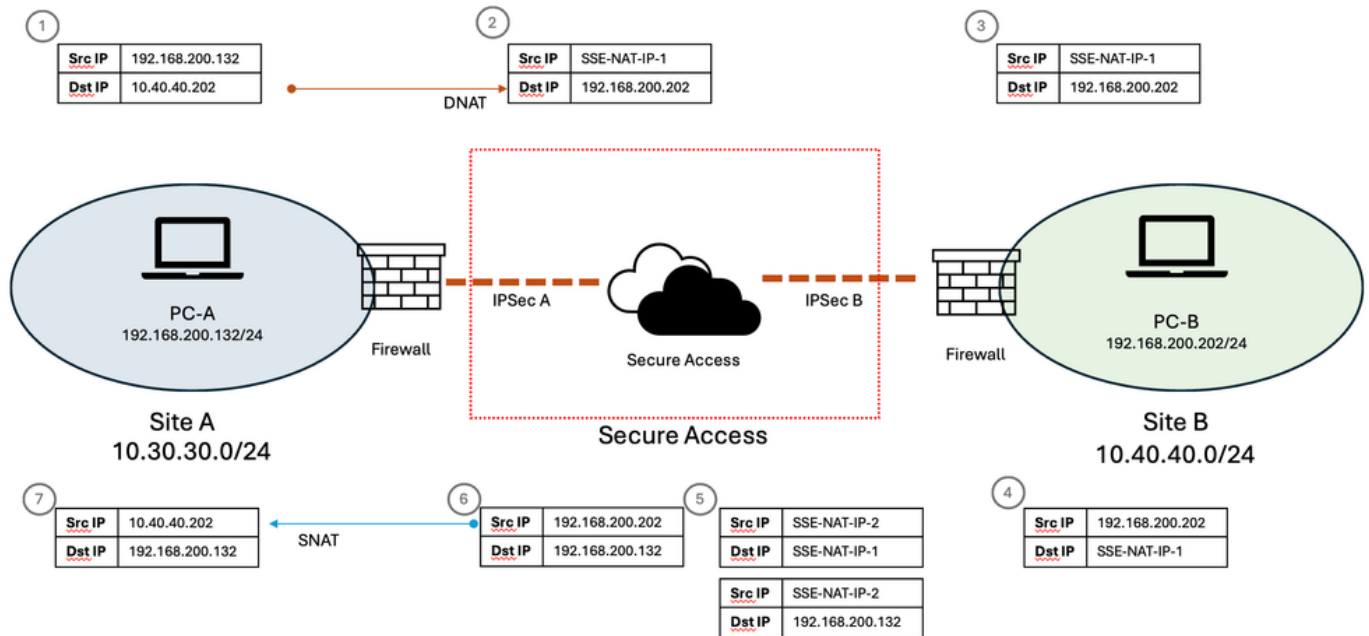
Cisco Secure Access ل D-NAT 10.40.40.202 → 192.168.200.202

192.168.200.202. ىل ع بيولا م داخ ىل ا ةمزال لصت م ث

ب يولا م داخ دلي ، ةيامل رادج ىل ع يفاضل NAT نودب . ةدئاعال رورم ا ةكرح ي ف ةلكشمال ثدحت
ردصمالم اذختساب ةباجتسال
192.168.200.202

10.40.40.202 : ةهوجلابل لاصلتال ليمعال ادب ، كلذ عمو

عم ليمعال ىل ا مدقمالم ردصمالم اناونع قفاوتي شيحب عاجرال رورم ا ةكرح ةمجرتمزلي ، كلذل
192.168.200.202 → 10.40.40.202 يرهاظالم اناونعالم



ةكبشال قفدت - ةروصلال

هاجتاب جورخال عم رورم ا ةكرح ىل ع ردصمالم NAT ذيفنتب ةيامل رادج موقوي ، كلذ قيقحتل
ةكبشال قفدت عومجم

192.168.200.0/24 → 10.40.40.0/24 وه بولطمالم نييعتال نوكي ، لاثمالم لىبس ىل ع

ةلباقمالم يرهاظالم نيوانعالم او ةيقيقحالم نيوانعالم نيبي ةيسكع ةقالع عاشنل ىل ا اذه يدؤي
امل.

دحاو ىل ا دحاو طخ

ةكبش لل دحاو ردصم ىلإ دحاو ردصم ل (NAT) ةكبش لل ةهجاو ةقاطب معدى ةيماحل رادج ناك اذا
قاطن (NAT) ةكبش لل ةهجاو تاقاطب نم ةدحاو ةدعاق لثمت نأ نكمي ف ،اهلمكأب ةيعرفل
لمالك 24 / نىوانعلا

للاثلما لىبس ىلع

مجرتم ردصم	يقيقح ردصم
10.40.40.0/24	192.168.200.0/24

192.168.200.202 → 10.40.40.202 و 192.168.200.203 → 10.40.40.203 لثمت تانيي عت كلذ نع جتنىو

اهلمكأب ةيعرفل ةكبش لل ربع رخآو درف نيب ةقالعلا سفن قيبطت متي

ةفيفخ ةمصو نودب ةيماحل ناردي

لك نيوكت مزلتي ،اهلمكأب ةيعرفل ةكبش لل دحاو ىلإ دحاو ردصم NAT ةيماحل رادج معدى مل اذا
يدرف لكشب بولطم نييعت

بىولا مداخل ،لاثلما لىبس ىلع

- 192.168.200.202 :ردصم ال IP
- ةكبش لل قافنأ ةعومجم :ردصم ال ةهجاو
- لخاد :رورم ال ةكرح هاجتإ
- 10.40.40.202 :مجرتم ال ردصم ال IP

192.168.200.202 → 10.40.40.202 يه ةجتانل ةمجرتللاو

ةيرهاظلا ةيعرفل ةكبش لل ربع لوصول بلطتي دروم لك ىلع هسفن جهنل قيبطت نكمي

للمعل نأو ةيرهاظلا ةنونعلا ماطن ب ناطفتحي لاصلتال نم نيهاجتال الك نأ نمضي اذهو
لاصلتال عاشن دنع هم دختسا يذل يرهاظلا IP ناونع سفن نم ةباجتسال ىقلتى

ةلص تاذا تاملولعم

Cisco : نم ةكبش لل قفن ةعومجم نيوكت / نمآلا لوصول NAT طيخت
<https://securitydocs.cisco.com/docs/csa/olh/168842.dita>

Cisco: نم نـم آلا لوصولا ةكبش قفنة ومجم هيچوتو نيوكت عجرم
<https://securitydocs.cisco.com/docs/csa/olh/118900.dita>

Cisco: نم ةسسـالـا تانايـبـلا عمج واهـالـصـاو نم آلا لوصولا ءاطخأ فاشكتسأ ليلد
<https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html>

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م ج ر ت
م ل ا ع ل ا ا ح ن ا ع م ج 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 ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ط 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 م ج ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م ج ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م ج ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م 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 د ن ت س م ل ا