

ASA VPN لمج ةنزاوم ري دم باختنا ةيلمع

تايوت حمل

[ةمدقملا](#)

[ةيساس ال اابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساس ا تامولعم](#)

[ليمحتلا ةنزاوم ةيلمع](#)

[ري دم باختنا ةيلمع](#)

[ليغش تلا ةداعا تاهويراني س ري ذخت](#)

[ري دملا باختنا ةداعا ةيلمع](#)

[ةومجملا ماظن نم Director زاوج ةلازا تم](#)

[ةومجملا وضعب ةصاخلا Hello لئاسر ريلا Director زاوج بيحتسي ال](#)

[اهخالص او ءاطخ ال افاشكتسا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

ةصاخلا ةكبشلا لمج ةنزاوم وي راني س ي ري دملا راي تخا ةيلمع دننتمس م اذ ه فصي Cisco 5500-X ةلس لس نم (ASA) فيكتلل لباقلا نام ال زاوج مادختساب (VPN) ةيره اظلا

ةيساس ال اابلطتملا

تابلطتملا

دننتمس م اذ ه ةصاخ تابلطتم دجوت ال

ةمدختسملا تانوكملا

9.2 ةغصي ةيجمرب ضكري نأ cisco ASA 5500-X لىل ةقيثو اذ ه في ةمولعملا تسسا

لاخد ا م ت ه ن ال ارظن ،جمار بلا تارادص ا عي مج لىل اضي ا دننتمس م اذ ه قبطني :ةظالم
7.0(1) رادص ال ا في ةرم لوال ةزيملا

ةصاخ ةيلمع ةئيب في ةدوجوملا ةزهجال نم دننتمس م اذ ه في ةدراول ا تامولعملا ءاشن ا م ت
تناك اذ ا .(يضا رتفا) حوسم نيوكتب دننتمس م اذ ه في ةمدختسملا ةزهجال عي مج تا دب
رما ي ال لمحتملا ري ثاتلل كم ه ف نم دك ا ت ف ، ةرشابم كتك ب ش

ةيساس ا تامولعم

نبي فص نم لكشب ةكبشلا رورم ةكرح عيزوتل اهمادختسا م تي ةيلآ يه VPN لمج ةنزاوم
في ذخات الو ، طيس بلا عيزوتلا لىل دم تعت لامحال ةنزاوم . ةيضا رتفا ةومجم في ةزهجال

وأن يزاوج نم لامحالة نزاومة ومجم فالتت. ىرخا لمواع وأ جرخلا نم دافاتسالا لدعم رابتعالا لثامتم لكش بةزهجالا هذه نيوكت بجي الو، رثكأ وأ دحاويوناث زاهجوريدمو، رثكأ

للمحتال نزاومة مزرراوخ

للمحتال نزاومة مزرراوخ ىلع عماعة رظن ىلي اميف

- يدعاصت بيترتب يوناثلال عمومجمالماظن اعاضعأ نم عزورفم عمئاقب ريديلما زاهج ظفتحي .ة. ىلخالل IP نىوانل
- م تي ىتلا (ىوصقلا/ةطشلالا لمعالا تاسلج ددع) حىحص ددع ةبسنك للمحال باسح م تي .يوناث عمومجمالماظن وضع لك ةطساوب اهرىفوت
- IPSec نم (SSL) نم آلا لىصوتلا ذخأم ةقبطل VPN قفن هيجوت ةداعاب هجوملا زاهج موقى .ىرخالا ةزهجالا نم ةئاملال ىف دحاو ةبسنب ىلعأ نوكى ىتح، الو للمل لقا هب زاهج ىلا
- عمومجمالماظن اعاضعأ مكي ام دنع طقف هسفن ىلا ههيجوت ريديلما زاهج دىعي .ريديلما زاهج نم ةئاملال دحاو ةبسنب ىلعأ ةيوناثلا

ةيوناثلال عمومجمالما نم نىوضعو دحاو ريديم عم كلذ ىلع لاثم ىلي اميفو

- بسنلال مكي بي رقت م تي و، ةئاملال ىف رقص هت بسن للمحتال دقعل مكي ادبت .ةئاملال ىف فصن برقا ىلا ةيوناثلا
- دحاو ةبسنب ريديلما زاهج نم ىلعأ للم اعاضعأ مكي ىدل ناك اذا لاصتالا ريديلما زاهج ذخأي .ةئاملال ىف
- ىذلا ىطايتحالل خسنلا زاهج لبق نم ةسلجال ذخأ م تي، لىصوتلاب ةرادلا زاهج مكي مل اذا .ةيوناثلا لمحتال لقا ىلع اىلح ىوتحي
- خسنلا زاهج ىلوتىس ف، لمعالا لمحل ةيوناثلا ةبسنلا سفن اعاضعأ لك ناك اذا .تاسلجال نم ردق لقا بةسلجال ىطايتحال
- لمعالا تاسلج ددع سفسن بولمعالا لمحل ةيوناثلا ةبسنلا سفن اعاضعأ مكي مل ناك اذا . IP نىوانل نم ردق لقا بةسلجال ىطايتحالل خسنلا زاهج ىلوتىس ف

ريدم باختنال ملىم

ماظن ةكبش ىلع (VPN) ةيرهاظلا ةصاخلا ةكبشلالا لمحتال نزاوم ريديلما رايتخا ةلىممع ارجا م تي :ةجراخلا ةكبشلالا ىلع ةلدابتملانا اىبالا نم ناعون كانه .ةجراخلا عمومجمالما

- م تي ىذلا عمومجمالماظنل IP ناوئعل (ARP) ناوئعل لىلحت لوكوتورب مزح لدابت م تي . IP ناوئعل اهللسرا م تي ىتلا ARP مزح ددعل ىصقألا دحل .هجومال فاشتكال همادختسا :وه ريديلما فاشتكال عمومجمالماظنل

1 + (ةيولوالا - 10)

رم اوألا رطس ةهجاو رمأ نم priority ىعرفلا رمالا ىف لالحا وه امك ةيولوالا نىوكت م تي، انه . (CLI) vpn load-balancing

- ذفنملا مقرر دي دحت متي Hello. ةباجتسإ/ب ل ط لئاسرل ج راخلا لىل UDP مزح لدابت متي .

9023 لىل يضا رتفا وهو cluster port load-balanced ي عرفل رمال ي ف

ام لاسرلا لواح اهنإف ، لىمحتلا ةنزوم زاهج ةسمخ يه ةيولول وأل تناك اذا ، لاثملا لىبس لىل ع اذا . ةعومجملا ماظنل IP ناووع ك لىتم ي رىدم زاهج ي انك اذا ام ةفرعمل ARP مزح تس لىل لىص ي نأ لبق ةي ناث 15 رظتني و ARP لئاسر نم دىزم ي لىسري ال ASA نإف ، رىدم زاهج فاشتكام ت UDP Hello. ةباجتسإ مادختساب هجوملا زاهج بىجتسي كلذ دعب .

لىغشتلا ةداعإ تاهوي رانيس رىدحت

لامحال ةنزوم ةعومجم ماظن ي ف ASA ي تدحو مادختساب لىغشتلا ةداعإ ةلاح ي ف

- لىغشتلا ةداعإ لبق رىدملا ناك ASA-2 وأ ASA-1 امإ .
- ASA-1 ديهمت ةداعإ مت .
- اقباس رىدملا وه نكي مل نإ رىدملا ASA-2 حبصي .
- ديهمتلا ةداعإ دعب وضعك ةعومجملا لىل ةطاسبب ASA-1 مضمني .

زهجال ةي ج راخلا ههجال لىصوت متي ثيح لوحمل نيوكتب لامحال ةنزوم ةي مزراوخ رثأت دق ي ف ةعرفتملا ةرجشلا ةي مزراوخ ببستت دق ، لاثملا لىبس لىل ع . اضيأ ةعومجملا ماظن لوحملاب لصتملا زاهجال ديهمت ةداعإ دنع لاصتالا رىخأت .

ةي لمعلا عيرست لىل ع [spanning-tree port fast](#) رمال دعاسي : حىملت .

ةنكمم لمح ةنزوم هي دل ي ذل او اذ ي دح هلىمحت ةداعإ تمت ي ذل ASA لواح ي دق ، تالاحل ضعب ي ف لىل لوصول عىطتسي ال هنأل (لعللاب دوجوم رىدملا زاهج ناك اذا ي تح) ةرادال زاهج حبصي نأ فشتم هجوم ضراعت كانه نوكي ام دنع . لوحمل ي ف لاصتالا رخأت ببسب لىل لىدملا زاهج ضفخنم (MAC) طئاسولا لىل لوصول ي ف مكحت ناووع عم ASA نإف ، ARP مداصتل ةجيتنك رىدملا زاهج رود نع ي نغتسي لىل ع MAC ناووع عم ASA لىل امنيب ، زوفي .

رىدملا باختنا ةداعإ ةي لمع

ةرادال زاهج باختنا ةداعإ ي ف ناببستت ني تلاح كانه .

ةعومجملا ماظن نم Director زاهج ةلازا تمت

ةعومجملا ماظن اعاضع اعىم لىل ثب ةلاسر لاسرلا متي ، ASA ي ف ةزىملا لىطعتب موقت ام دنع اقباس اهفصومت ي تلالا [باختنالا ةي لمع](#) اعرجا متي و ، رىغتملا مالعال

ةعومجملا وضعب ةصاخلا Hello لئاسر لىل Director زاهج بىجتسي ال

رمال قرغتسي ، ةعومجملا ماظن وضعب ةصاخلا "ابحرم" ةلاسرل ةرادال زاهج بىجتسي مل اذا لاسرلا متي . ادوجوم دعي مل رىدملا نأ فاشتكال ةي ناث 20 لىل ع ASA ةعومجم ماظن وضع ةعومجملا ماظن اعاضع اقلتي مل اذا . (نىوكتلل ةلباق رىغ) ناووسمخ لك Hello لئاسر ةي باختنالا ةي لمعلا لىغشت متي سىف ، "ابحرم" لئاسر عبرا دعب ةرادال زاهج نم ةباجتسإ .

اهحال صإو ءاطخأل فاشكتسا

رمأ طبضي تنأ لمعتسي نأ لبق ءدام cisco [رمأ Debug](#) [ىلع مهم ءمولعمل](#) تلحأ: ءظالم

ماظنل ءاطخأ فاشكتسا تالواحم عم ءءي فم هذه ءاطخأل احيصت رمأو نوكت نأ نكمي
اهحال صإو:

- **debug fsm 255** - ءمءل ءاا اءه مءءتسا - **no debug all** رمأل
طيشننل ءاغلإل
- **debug vpnlb 3** ءمءل ءاا - **debug vpnlb 3** ءمءل ءاا
in order to ءرأ ءرم رمأ
- **debug vpnlb 4** ءمءل ءاا - **debug vpnlb 4** ءمءل ءاا
in order to ءرأ ءرم رمأ

ءلص تاذا ءمولعم

- [لئمءل ءنزاوم مهف](#)
- [Cisco Systems - ءاءنءس ملأو ىنقءلأ معءلأ](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لالحل وه
ىل إأمءءاد ءوچرلاب ةصوء و تامچرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إلل دن تسمل