

ربع (MTU) لقنللى صقألا دحلا ةدحو نيوكت SD-WAN ةكبش يف IP ISE لوكوتورب SDA رشن تايلمعل

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[ةلكشملا فصو](#)

[ةيجيضوت ايجولوبوط](#)

[SD-WAN فاوخل SDA دح - MTU ةوجف 1: يدحتلا](#)

[1: يدحتلل ل](#)

[ةدحو تانايب رورم ةكرح - \(MTU\) لقنللى صقألا دحلا ةدحو طغض 2: يدحتلا](#)
[SD-WAN ةكبش ةيشغت ربع \(ISE\) نيذختلا](#)

[فيبلغتو ةمزللا لكيه ةلومح](#)

[ISE IP MTU ل يقاب تسالا نيوكتلا 2: يدحتلل ل](#)

[\(CLI\) لالغ نم لاثم\) ISE نيوكت](#)

[يارقلا](#)

[عجارملا ويرىاعملا](#)

ةمدقملا

(MTU) لاسرالا ةدحول صقألا دحلا لكاشم اهب رثؤت دق يتلا ةيفيكللا دنتسملا اذه حضوي SDA. عقاوم ليصوتل SD-WAN مادختسا دنع SDA يف ةيئزجلا ةئزجتلا ىلع

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيذل نوكت ناب Cisco يصوصت:

- Cisco (SDA) جم انربب فرعملا لوصولا
- Cisco (SD-WAN) جم انربب يف ةدحمل ةعساوولا ةقطنملا تاكبش
- Cisco (ISE) نم ةيوهلا تامدخ كرحم

ةمدختسملا تانوكملا:

ISE و SDWAN و SDA ىلى دنتسملا اذه يف ةدراولا تامولعملا دنتست

عصاخ ةي لمعم ةئي ب ي ف ةدوجومل ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل عاشنإ م تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسمل اذه ي ف ةمدختسمل ةزهجال عي مج تأدب رما يأل لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتل دي ق ك تكبش

ةيساسأ تامولعم

مدع ةيقافتا نم ةدافتسالا يلع ديازتم لكشب ةثي دحل تاسسؤمل تاكبش لمعتو قستمل ذيفنتلاو ةقيقدلا ةقيقدلا ةيئزجلا ةئزجتلا ضارغل زيمي مل امم Cisco، نم SD-WAN فيظوت متي ام ابل اغ ،ةعزومل SDA عقاوم لي صوتل .تاسايسلل هذه ةيمهال ارظنو .ةعونتم ةيساسأ تاكبش ربع ةنسحمو ةنمأو ةعيرس لقن ةليسو رفوي عيزوتل باناج يل ،ةماهال (AAA) ةبساحمل او ضيوفتلاو ةقداصل مل تامدخ ISE رفوت ،ةينبل مكحتل مئاوقو (SGT) نامأل ةعومجم تامالع ،لاثمل ليلبس يلع) تاسايسلل يكيمانيدل (ليزننلل ةلباقلا (ACL) لوصول ي ف

نيوكب تايدحت يل يدؤي نأ نكمي ةلاعفل تاينقتلا هذه جم نأ ال ،اهتوق نم مغلرل يلعو لقن طاقن دنع (MTU) لقنلل ي صقأل دحل ةدحو عم لماعتل نإ .ةرثؤم اهنكلو ةقيقد لوانتت .لكاشمل هذه لثمل يسيئر لاجم وه SD-WAN ةكبش ةيشغت ربعو ةجرحل ةكبشلا امهنكمي (MTU) لقنلل ي صقأل دحل ةدحو قباطت مدعل ني عئاش ني هوي رانيس ةلاقمل هذه ةكبشلا تايلمع لي طعت

1. ةزهجاو SDA لو كوتوربل ةي دودحل دقعل ني ب (MTU) لقنلل ي صقأل دحل ةدحو ةوجف SD-WAN ةكبش ةفاح
2. ةطساوب اهؤاشنإ متي تال تانايبلا رورم ةكرحل (MTU) لقنلل ي صقأل دحل ةدحو دوي ق SD ةكبش ةصاخال WAN ةكبش ةيشغت زاي تجال ISE

تالكشم عنمل ةيمهال غلاب ارمأ حيحص لكشب (MTU) لقنلل ي صقأل دحل ةدحو ةاذاحم دعت ذيفنتو ةقوئومل ةقداصل مل نمضي امم ،ةتماصل طاقسالا تايلمع وأ ةمزحل ةئزجت هذه ةجلاعم ي ف لشفل يدؤي دقو .ماع لكشب ةكبشلا رارق تسا قيقحتو تاسايسلا ادهج كلهتسي امم ،تاسايسلا قيبطت تاقافخاو عطقتمل لاصلتالا كابرل ال تالكشمال اهلحو تالكشمال فاشكتسا ي ف اري ب ك

(MTU) لقنلل ي صقأل دحل ةدحو ةعئاشلا ضارغلأ

ريثك ي ف يدؤي امم ،ةفلتخم قرطب ةي ذاحمل (MTU) لقنلل ي صقأل دحل ةدحو رهظت نأ نكمي :اهصخيشت بعصي لئاسم يل نايحال نم

- هتظحال نمكمي امك :ةلهمل اءهتنا تالاح وأ ةعطقتمل RADIUS ةقداصل مل لشف تالاح يتل كلت ،لاثمل ليلبس يلع) ربكأ RADIUS مزح دلوت يتل تاسايسلل صاخ لكشب (ةعساو تاداهش وأ AV چاورأ يلع يوتحت
- ةلباقلا (ACL) لوصول ي ف مكحتل مئاوق مالتسا ي ف لشفت يتل ةيماهال طاقن متي ام ابل اغو :اهقيبطت وأ TrustSec (SGTs/SGACLs) تاسايس وأ (dACLs) ليزننلل ةري ب ك RADIUS مزح ي ف تاسايسلا هذه لقن
- يلع لاسرالا ةداعا تايلمع ببسب :مهيلع قدصل مل ءالمعل ةئي طب لمع ةسلج عاشنإ .تاقببطتلا ةقبط
- ISE تالجس ي ف ةظحال مل لباق RADIUS لو كوتورب ربع ةقئافل لاسرالا ةداعا تايلمع

(NAD) ةكبشال ىلإ لوصول ةزهجأ ىلع وأ

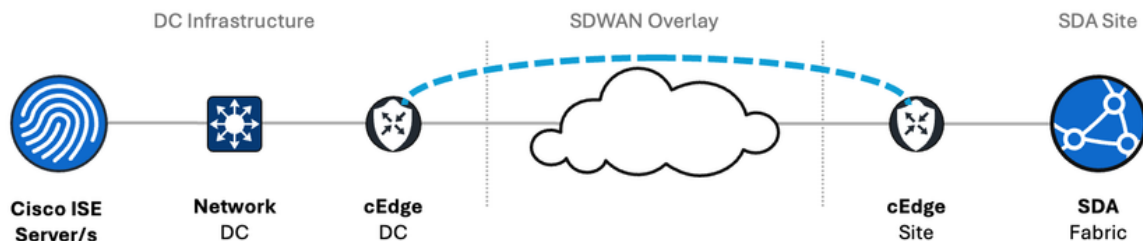
- ISE يف اهؤارج مت يتال ةسايسال تاريغت رشن متي ال دق: قستمال ريغ جهنل رشن ةديعلال SDA عقاوم يف NADs عيمل ىلإ تباث لكشب
- ىلع) ةريبك مزح لسرت يهو ISE طاقنال رهظت نأ نكمي: ةمزحل طاقنال تاضقانت ةباحتسا دجوت ال نكلو، (DF) ةئزجت مدع تب ةعومجم عم (تيا ب >1450، لاثمل ليبس SD-WAN Cisco Edge وأ NAD هجوم نم ICMP ل "ةبولطمال ةئزجتال" أطخ وأ ةقباطم
- هجوم (DC) تانايبال زكرم لولخدل ةهجاو ىلع هتظحال م تمت: مزحل طاقسإ تادادع ةدايز ىلع وأ SDA عقاومل ةهجومال ISE نم اهيلع لوصول متي يتال رورمل ةكرحل Cisco Edge يسكعل هاجتإل يف رورمل ةكرحل SDA دودح هجاوت يتال Cisco Edge SD-WAN هجوم ةهجاو

ةلكشمال فصو

تاسسؤملل ةيجذومن رشن ةيلمع
ةعئاشال تاسسؤملل ايجولوبوط دحأ انه لمأتنلو

- ةلصتم، ةيميلقا رواح وأ (DC) يزكرم تانايب زكرم يف رشنال متي: Cisco ISE مداوخ DC ةكبشل ةيساسال ةينبال
- تالوحم وأ ةيساسال DC تالوحم نمضتي: رمتسمال رايتلل ةيساسال ةينبال ISE مداوخ اهب لصتت يتال ةيمجتال
- Cisco DC Edge تاهجوم موقت: جماربال قيرط نع ةفرعمل WAN ةكبش ني مضت، لاثمل ليبس ىلع) ةيساسال لقن ةكبش ربع (IPsec ةداع) SD-WAN قافنأ ءاشناب، ةديعلال SDA عقاوم يف Cisco Edge تاهجوم ىلإ (Internet، MPLS)
- ةيلحمل SDA ةينبال ةديعلال عقاومال يف Cisco Edge تاهجوم لصتت: SDA عقوم، ةيلحمل ةكبشال يف مكحتال تادحوو دودحل دقعو ةينبال ةفاح دقع نمضتت يتالو فاطمال ةياهن يف ةياهنل طاقنو، ةيكلسالل (WLCs)

ةيجيضوت ايجولوبوط



SD-WAN فاولح SDA دح - MTU ةوجف 1: يدحتل

يئاقولتلا ليغشتلا لالخ نم اهقيبطت متي ام ابلاغ يتلا، Cisco نم SDA ميمصت ئدابم عمجمل يوتسم يلغ (MTU) لقنلل يصقألا دحلا ةدحو زيزعتو، (LAN) ةيلحملا ةكبشلل نم ةيدودحلا دقلا كلذ نمضتو. ةينبلا ةزهجأ عيمج يلغ (ةمخض تاراطا) تياب 9100 ةعسب ةجيتنو. ةينبلا لخاد ةعافكب Ethernet jumbo تاراطا لقن نمضيو Catalyst 9000 ةلسلسلا ةدحو يلغ ايضارتفا SDA دودح ةدقع يلغ SVI وأ 3 ققبطلا ليصوت ةهجاو نييعت متي، كلذل هذه ربكألا (MTU) لقنلل يصقألا دحلا.

ةيضارتفا ةداع نوكت، Catalyst 8000 ةلسلسل لثم، SD-WAN ةفاح ةزهجأ نإف، سكعل يلغ تاهجاو لل يسايق اذهو. تياب 1500 ةميقب ةهجاو لل (MTU) لقنلل يصقألا دحلا ةدحو يلغ تاراطا لمعد نوكتي ثيح، (ISPs) تنرتنالا ةمدخ يرفوم لثم ةيجراخلا تاكبشلاب ةلصتلم نكمم ريغ وأ عئاش ريغ مچحل ةريبك.

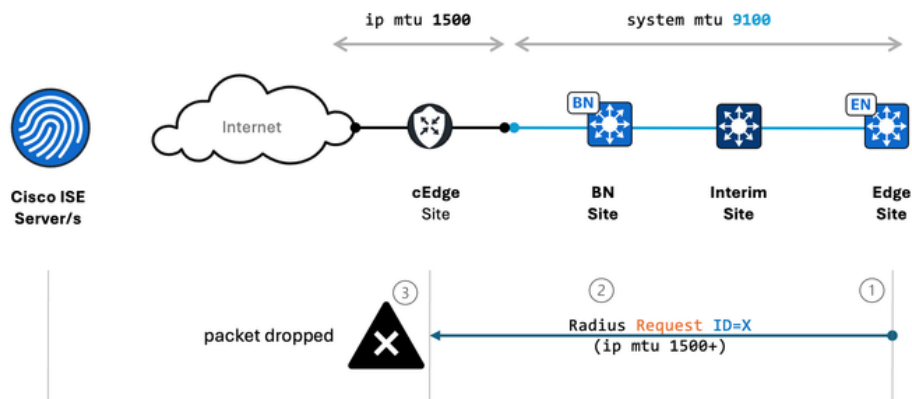
نم ربكأ IP ةمزنح لاسرلا لواحي SDA دح: لمحتملا لشفلا نم ةرشابم ةطقن توافتلا اذه قلخيو يصقألا دحلا ةدحو لاهل مالتسالا ةهجاو نيوكت مت يتلا SD-WAN ةفاح يلغ تياب 1500. تياب 1500 تاذا (MTU) لقنلل.

رشن تايلمع يف عئاش أطخ وه (MTU) لقنلل يصقألا دحلا ةدحو قباطت مدع نم عونلا اذه ايدحت رثكأ رمألا اذه لعجي امو. نيوكتلا ءانثأ هنع يضاعتلا لهسلا نم نوكتي ام ابلاغو SDA Catalyst تالوحم يلغ RADIUS تابلط ءاشنإ ةيفيكب ةقلعتملا ةدحمل تايكولسل نأ وه هذه روهظ يف ببستت نأ نكمي Cisco IOS-XE® جمانرب لغشت يتلا 9000 switches ةجرحو ةدحم فورظ يف طقف تالكشمل.

ةقداصم ةيلمع ءانثأ اهؤاشنإ متي يتلا RADIUS تابلط زيمرت متي، لاثملا ليبس يلغ (SMD)، لمعل تاسلج ةرادا جمانرب ةيلمع ةطساوب اهتجلاعم متت يتلاو ئيئاهنلا مدختسملا تابلط ءاشنإ متي، كلذ نم ضيقللا يلغو. تياب 1396 رادقمب مزحل ةئزجتلا اثبات ازيمرت يلغ لوصول يف مكحتلا ةمئاق لثم، TrustSec تاسايس دادرستاب ةقلعتملا RADIUS Cisco Internetworking Operating System (IOSd) جمانربل ةيعرفلا تانوكمل ةطساوب، (SGACL) نامألا ةعومجم بنجت اهنكميو (MTU) لقنلل يصقألا دحلا ةدحو عم قفاوتم تادحو لا هذهو. (IOSd) System (IOSd) يلغ لصي ام ةداع) ماظنلل (MTU) لقنلل يصقألا دحلا ةدحو اهمجج زواجتي مل ام مزحل ةئزجت (تياب 9100).

(MTU) لقنلل يصقألا دحلا ةدحو قباطت مدعب ةقلعتملا لكاشملا حبصت، كلذل ةجيتنو م. ادختسالا ديق Cisco TrustSec (CTS) نم ليزننلا تاسايس نوكت امدنع طقف ةحضاو راودألا يلغ ةدنتسملا لوصول يف مكحتلا مئاقو ةعومجم فلتخت دق، كلذل يلغ ةفاضلاب يألغ ءانب مدختسملا ةقداصم ءانثأ SDA ةفاح زاهج ةطساوب اهليزنت متي يتلا (RBACL) موقوي، ةيلمعلا ةسرامملا يف. يرخلأا زيميتملا تامالعل لعفلاب ةدوجوم SGACL تاسايس تاسايسلا تاعومجم نم طقف ةلخادتملا ريغ ءانجألا ليزنتب لوحملا.

حوارتت، ةقسانتم ريغو ةعقوتم ريغ جئاتن يلغ تايكولسل هذه يدؤت نأ نكمملا نم، اعمو مچج يلغ ادامتعا، تاسايسلل ةلمتكملا ريغ تاليزننلا يلغ ةتماصل تاقافخالا نيب ماظنلا فورظو، (SGACL) ةيساسألا ةينبلا يلغ لوصول يف مكحتلا ةمئاق ةسايس يلغ (MTU) لقنلل يصقألا دحلا ةدحو قافاتا يف تالالخال، فاطملا ةيانه يفو، ةيلحالا راسملا.



ISE وحن (تياب 1600، لاثم لاي بس ىلع) ڤري بك RADIUS ةمزن هيجوت ةداعاب SDA دودح موقت
ثدحي ام اذو، SD-WAN ةفاح ربع

1. تياب 1600 تا ذ IP ةمزن، 9100 MTU ةهجاو عم، SDA دودح لسرت.
2. اهب ةصاخلا 1500 MTU ةهجاو ىلع ةمزال هذه Cisco Edge SD-WAN هجوم لبقتسي.
3. هجوم ناف، هذه RADIUS مزح ىلع (DF) ةئزجتال مدع تب ةدحو نييغت متي مل اذا، كلذ عمو. ريبكت "متي هنال ةطاسبب لوخدلا دنع اهطاقساب موقبي نأ نكمي SD-WAN Cisco Edge لصي ال. اهنويكت متي تي ةهجاو لل (MTU) لقنلل ىصقألا دحلا ةدحو ىلإ ةبسن "اهمجح تاجالعمل هذه ةئزجت رابتعالا في عضبي نأ نكمي شي IP هيجوت ةداعا قطنم ةلحرم ىلإ (DF تب حمسي ناك اذا).

تالكشمل افاشكتساب قلعتت ةريطخ عاوص تابون ثودح ىلإ تاماصل طوقسلا اذ يڭوي
SD-WAN/ISE ىلإ SDA) هاجتالاب قلعتت ةلكشمل ناواميس ال، اهجالصاو

زكرم تالوحم في (MTU) لقنلل ىصقألا دحلا ةدحو في لثامم قباطت مدع ثدحي نأ نكمي
ىلع) مچجال ڤريبكت تاراطال معدل ةداع اهنويكت متي يتلاو، ةيفرطال وأ ةيساسال تانايبلا
مت اذا، كلذ عمو. ةيلخادلا تانايبلا رورم ةكرح ةءافك نيسحتل (MTU 9000+)، لاثم لاي بس
مت يذل SD-WAN Edge Router هجومب ةصاخلا LAN ةكبش ةهجاو ىلإ رورملا ةكرح ميسلست
1500، لاثم لاي بس ىلع) ةيسايقلا (MTU) لقنلل ىصقألا دحلا ةدحو مادختساب هنيوكت
رورملا ةكرحل ةصاخو، مزحلا طاقساب تايلمع وأ ةئزجتال ىلإ اذ قباطتال مدع يڭوي دق، (تياب
SD-WAN ةينب ىلإ DC ةكبش نم ةقفدتال.

1: يدحتلل لح

SDA دودح ليصوت ةهجاو ىلع IP لوكتورب ربع (MTU) لقنلل ىصقألا دحلا ةدحو ةاذامب مق
تياب 1500 ةداع، SD-WAN Cisco Edge Router ةهجاو عم (SVI وأ ةيدامل).

(SDA دح ةدقع ىلع) نيوكتال لاثم:

<#root>

!

```
interface Vlan3000 // Or your physical handoff interface, for example, TenGigabitEthernet1/0/1
description Link to SD-WAN cEdge Router
ip address 192.168.100.1 255.255.255.252
```

ip mtu 1500

```
// Align with SD-WAN cEdge receiving interface MTU  
!
```

Catalyst 9000 دودج ىلع ةئزجتال: مهم رابتعإ

يوتسم يف ةيلصلأل IP مزحل IP ةئزجت، SDA دح دقعك، Catalyst 9000 Series تالوحم معدت لوكوتورب ب ةصاخال (MTU) لقنلل ىصقأل دحل ةدحو ضفخ ببستي ال. ةزهجال تانايب لىل ةدنتسمال ةئزجتال ببسب عادأل ضافخنا يف 1500 لىل ميلستال ةهجاو ىلع تنرتنإل لولول موقى. اهب رمت وأ اهليلجاتحت يتال دودحل نم أشنت يتال رورمل ةكرحل جماربال ليجست لبقةافكب (حضاو DF تب ناك اذإ) تياب 1500 نع اهمجج ديزي يتال IP مزح ميسقتب ةيزكرمل ةجلالعمل ةدحو ىلع طغضال نود، ةددحمل ةهجاوال هذه.

فلغي VXLAN ةئزجت دناسي ال ماع لكشب حاتفم 9000 ةزافح ةدام نأ طحال ي نأ مهم وه، اهمم ويرانيس ىلع رثوي ال هنا ريغ رورمل ةكرحل ةيمهال غلاب ارمأ ديدحتال اذه دعي. رورم ةكرح لخد ةداع يجرالخال ISE و SDA دودح ني ب RADIUS لاصتا ثدحي ثيح، فوصومال RADIUS ةقداصم VXLAN ةكبش تايشغتل (MTU) لقنلل ىصقأل دحل تارابتعا). (يلصلأل IP هيچوت) ةدعاقال (Cisco) نم ةلصلال تاذ SDA ميمصت ةلدأ يف لصفم، دقعمو لصفنم عوضوم يه.

هجوم لقن ىل SDA ةقاطب دودح يف (MTU) لقنلل ىصقأل دحل ةدحول ةيقابتسال ةاذحمل يرورض رما Cisco نم SD-WAN ةفاح.

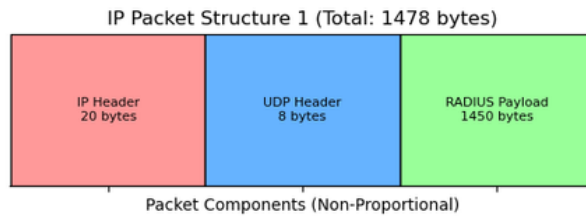
رورم ةكرح - (MTU) لقنلل ىصقأل دحل ةدحو طغض: 2 يدحتال SD-WAN ةكبش ةيشغت ربع (ISE) نيزختال ةدحو تانايب

ذفانم وأ، (NIC) ISE ةكبش ةهجاو ةقاطب لثم، ةيدرفال ةيدامل تاهجاوال نييعت مت اذإ ىتح تياب 1500 ةعس IP لوكوتوربل (MTU) لقنلل ىصقأل دحل ةدحو ىلع هجومال تاهجاو وأ، لولول هذه كلهتستو. ةماعال نيمصتال تايلمع مدقت اهسفن SD-WAN ةيشغت نإف، ةيسايق ىصقأل دحل تادحو ددع للقي امم، تياب 1500 غلابال دحل نم اعزج ةيفاضال تاقفنال (ISE) روظنم نم "ةلومحل" ةيلصلأل IP ةمزحل رفوتمل لاعفال (MTU) لقنلل.

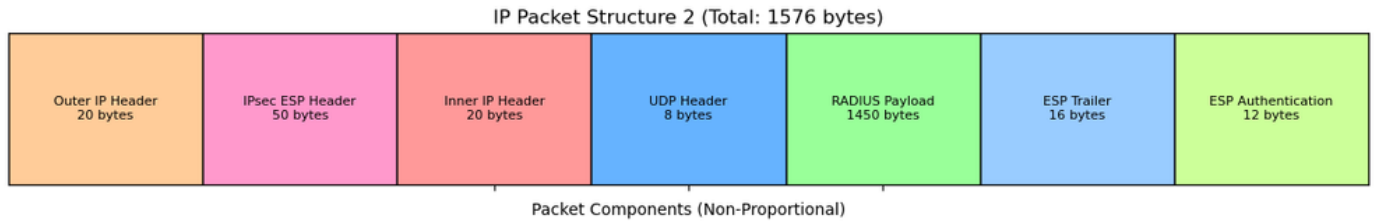
فيللغتو ةمزحل لكيه ةلومح:

(RADIUS لىل لوصول لوبق ةمزح، لاثمل لىبس ىلع) ISE مداخل نم IP ةمزح لاسرا متي ام دنع ممتو SD-WAN ةيشغت زاتجت اهنإف، SDA عقوم يف (NAD) ةكبشال لىل لوصول زاهج لىل رورمل UDP ربع ام بر، قفنال عضو يف IPsec عئاشال نيمصتال سدكم نمضتي. اهفيلغت NAT (NAT-T).

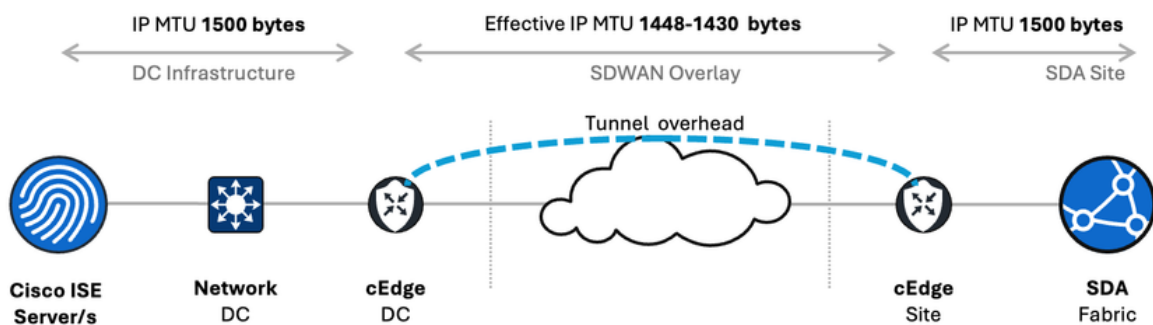
- (ةيلخادل ةمزحل) ISE نم ةيلصلأل ةمزحل:
8 ةعس UDP لوكوتورب + تياب 1450 نم ةلومح تاذ RADIUS ةمزح، لاثمل لىبس ىلع
تياب 1478 = تياب 20 ةعس يللخد IP لوكوتورب + تياب



- UDP ل NAT-T: نيمضت عم ام بر، قفالن عضو في IPsec ESP رابتعالا في عض



- ققداصم ال تايلآو ددحم ال IPsec تارفش ىلع ءانب فيللاكتل يلامجإ فلتخي نأ نكمي
يجزومن باسح. (اهمادختسا مت اذا GRE لثم) ىرخألا ةيشغتل تازيمو:
 - تياب 20 (IPv4): يجرالخ ال IP سار
 - تياب 8 (NAT-T ل UDP ربع ESP ناك اذا) UDP سار
 - تياب ~8: ESP ناونع
 - (انكمم كلذ ناك اذا) تياب ~16: ESP IV (ل AES-CBC، لاثم ال ليبس ىلع)
 - تياب ~12-16: HMAC-SHA256 عا طتقا مت، لاثم ال ليبس ىلع) ESP ققداصم
 - لصي ام، ىلعأ نوكت نأ نكمي) تياب ~52-70: ةعئاشلا ةردقم ال IPsec تافورصم
(تارايخل عيجم مادختساب رثكأ وأ ابيرقت تياب 80 ىلإ).



حبصت، تياب 1500 ىلعفل طابترالاب ةصاخلا (MTU) لقنلل ىصقألا دحل ةدحو تناك اذا - تياب 1500 ISE: نم ةيلصلأا IP ةمزحل ةرفوتم ال (MTU) لقنلل ىصقألا دحل ةدحو SD. ةكبشب ةصاخلا WAN ةكبش ربع ةماع تافورصم.
تياب $1500 - 70 = 1430$ ، لاثم ال ليبس ىلع.

ةلاعفل MTU مزحل زواجت دنع كولسل:

1. (DF Bit Anomaly شرح) ةم زح عاشناب ISE موقى:

- نىيىعتب ISE زاهجب صاخلا لىساسلا Linux لىغشت ماظن موقى، يضا رتفا لكشب يواست و نم رغصأ أشنت يتل مزحلل عىمجل IP سار نىب (Do Not Fragment (DF (تىاب 1500، لاثملا لىبس ىلع) IP MTU اهنىوكت مت يتل ةهجالول لكشب (هب صاخلا لىغشتلا ماظن لال خ نم) ISE لمعى DF تب اذه نم ضرغلل MTU فاشتكا ةىلمع نىسحتل لوالا ماقملا يف DF تب نىيىعت ىلع يقاب تسلا PMTU ملعتب ISE ل حمسى اذهو. اقحالا هفصو متي يتل او، (PMTUD) راسملل اهب ةصاخلا ةهجالولاب صاخلا MTU نم رغصأ تناك اذا ةهجو ىلا ايكىمانىد ةىلعفلل ةهجالول زواجتت IP ةم زح لاسرا ىلا ISE جاتحا اذا: ةهجالول MTU نم ربكألا مزحلل كولس. هب صاخلا Linux لىغشتلا ماظن ىلع دمتعى كولسل نإف، IP MTU هل ةنوكملا كلت ىلع (DF=0 دادعا) DF تب حمسو قىبسملا طبرلا ةئزجتب OS موقى، اىجذومن ال، لىغشتلا ماظن ىوتسم ىلع ةفىظو نع ةرابع ةئزجتلا اذه. ةجتانلا اعزجالا هسفن ISE قىببطت زمر ةطساوب ةرشابم اههيجوت متي دادعا) ISE ل يضا رتفاللا كولسل اذه فلتيخي: ةكبشلا ةزهجا نم حاتفم زىيىمت (MTU) لقنلل ىصقألا دحلا ةدحو لخد ةمئالما ةأزجمل ريغ مزحلل ىتح DF=1 ةكبشلا ةزهجا نم دىدعلا نع طوخلم لكشب هب ةصاخلا ةهجالولاب ةصاخلا تب ةدحو نىيىعتب ةكبشلا ةزهجا موقت ام ابلاغ. (تالو حمل، تاهجوملا) ةىديلقنلا ماىقنلل حىرصل لكشب اهنىوكت مت اذا ال اهل سرت و اهنىوكت يتل مزحلل ىلع DF تب ةعومجم ىلع لعفلاب يوتحت اههيجوت ةداعا مت يتل مزحلل تناك اذا و، كلذب اذا يضا رتفا لكشب ةئزجتلاب حمست اهنإ. اهطرتشت ةنىعم تالو كوتوربل و DF، (DF=0 و) ةىلاتلا ةوطخلل MTU زواجتت ةم زحلا تناك اهل نوكتى ام ابلاغ رورم ةكرح NAD ىلا ISE ثيح، قسانتلا مدع اذه: دىقعت ىرتي ماق اذا ال DF=0 اهل نوكتى نأ نكمى ISE ىلا NAD رورم ةكرح امنىب، اىضا رتفا DF=1 ءانثأ دىقعتلا نم ةىفاضا ةقبط مدقوى نأ نكمى - (ام ببسل اهنىيىعتب NAD ل ةئزجتلا تاىكولس ةطحالم نىسندنهملل نكمى. اهحالا صاواطاخألا فاشتكتسا رورملا ةكرح قفدت هاجتإ بسح PMTUD تالعا فتو ةفلتخمل

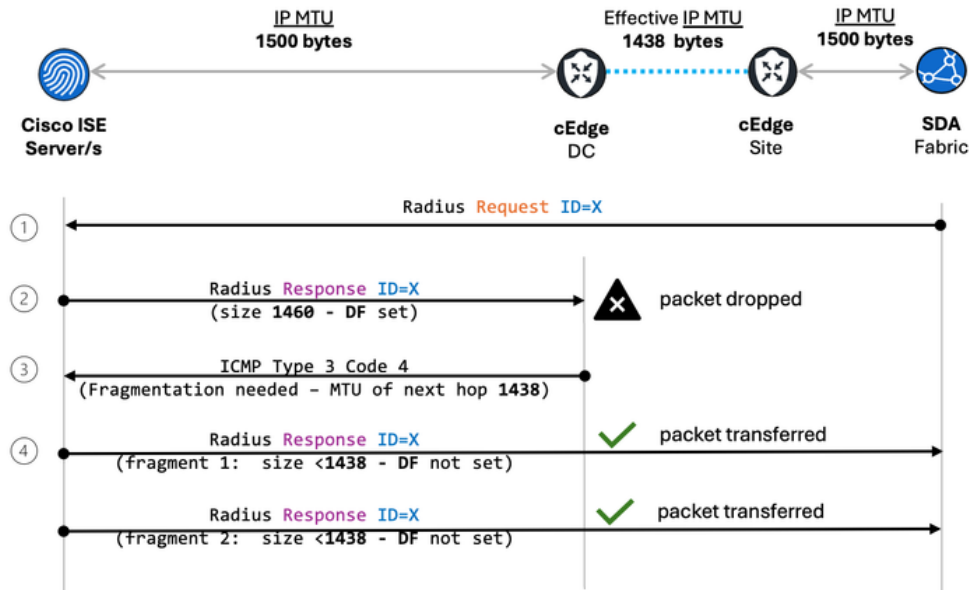
2. ISE نم IP ةم زح Cisco نم DC ةفاح هجوم ملتسى: (Cisco (DC ةفاح هجوم ىلا ةم زحلل لصت

3. نىمضت Cisco Edge هجوم لواحي: Cisco Edge هجوم ةطساوب MTU نم ققحتلالا نىمضتلا SD-WAN. قفنل ةم زحلا

- دحلا ةدحو ةىفاضا ال SD-WAN ةلسبك ةىلمع ةمىق ةىلصألا ةم زحلل تزواجت اذا ىلع Cisco Edge هجومب ةصاخلا ةرداصللا ةىداملا ةهجالول (MTU) لقنلل ىصقألا ةىلصألا ةم زحلل ىلع DF تب ةدحو نىيىعت متو، (تىاب 1500، لاثملا لىبس ةم زحلا ةئزجت ىلع Cisco نم ةفاحلا هجوم لمعى ال بجىف، ISE نم (ةىلخادل) ةىلخادل.
- ةم زحلا طاقساب Cisco Edge هجوم موقى نأ بجى.
- يتل ةهجالو "ICMP ةلاسراضى Cisco Edge هجوم لسرى نأ بجى، مساح لكشبو ةرم (4 زمرا، 3 عونلا) DF تب ةعومجمو ةبولطملا ةئزجتلا - اهىلا لوصول رذعتي ةوطخلل (MTU) لقنلل ىصقألا دحلا ةدحو ىلا ةراشلال، (ISE) ردصملا ىلا ىرخأ (قفنلل ةلاعفل (MTU) لقنلل ةىطمنلا ةدحو) ةىلاتلا.

4. ةلاسرى قلت دنع: (PMTUD) راسملل (MTU) لقنلل ىصقألا دحلا ةدحو فاشتكا ةىلمع لىلقنل (لىغشتلا ماظن ردصم) ISE موقى نأ بجى، ICMP نم هذه "ةبولطملا ةئزجتلا" اتقؤم تامولعمل هذه نىزخت هئاش نمو. دحمل ةهجالو راسمل هب صاخلا PMTU رىدقت اثىدح ةفشكمل PMTU ةدحو بسانت رغصأ مزح يف تانابلا لاسرا ةداعاو

PMTUD: ةىلمعل لىطىطخت مسر



PMTUD راهني شېح

ةيخانل نم لشف في نأ نكمي هنكل ،ةيرظنللةيخانل نم ايوق "يبعشال دशल" ربتعي
ةيلعمل:

- لئاسر رطحب نامأل تاسايس وأ ةطيسوللةيخانل ناردج موقت امابل اغ ICMP ةيفصت ISE. لىل لوصول نم "ةبولطملةئزجتال" ةلاسرعنمي امم، ICMP.
- Cisco Edge Router CoPP تاهجوم مدختست Cisco Edge Router CoPP ءجوم ىلع (CoPP) مكحتل ىوتسم ميظنت ICMP أطخ لئاسرءاشنإ. اهبةصاخال (CPU) ةيزكرمللةجالعمل ةدو ةيخانل Router CoPP مچحل تاذ مزحل نم ديدعل عم وأ ليقثلل لمحل تحت. مكحتل ىوتسم ىلع ةمههم يه ISE ىقلتى ال ICMP ءاشنإ طاقسإ وأ لدعمل ديدحتب CoPP موقى نأ نكمي ،دئازل ادبأ تاطحالمل.
- هنإف ،"ةبولطملةئزجتال" ICMP ةلاسر ISE ملتسي مل اذا :تماصلال طوقسال تالاح تب ةعومجم مادختساب ةريبك مزحل لاسرإ يف رمتسيو .راسمل ديقتل كردم ريغ لظي تالاح لىل كذيدؤي Cisco. ةفاح ءجوم لخدم لالخنم تمصب اهطاقسإ لىل يدؤي امم ، DF (RADIUS لاثمل لىبس ىلع) تاقيبطتل ىوتسم ىلع لاسرلال ةداعإو ةلهمل ءاهنتا.
- (ال RADIUS لىل لوصولل ةلباقال ةريبكل مزحل نوكت ISE تامدخ ىلع ريثأتل (AVP) قاطنللةعساو تاحيملتال (dACLs) لقنل لىل لوصول يف مكحتل مئوق لمحت رهاظمل لمشت .صاخ لكشب ةساسح (بىقرل تامولعم
 - ةلماكل وأ ةعطقتمللةقداصلال لشف تالاح.
 - SGT جمارب وأ ةكبشلال لىل لوصول تاسايس ىقلتت ال يتللةياهنل طاقنل ءحصلال.
 - NADs و ISE نب ةلشاف وأ ةلماك ريغ جهنللةنمازم.

ISE IP MTU ل يقابتسالال نيوكتال: 2 يدحتلل ل

ISE. لثم ةيويحل تامدخل للصفأال وه يقاب تسالال جهنللا دعي، PMTUD ةيوقووم مدعل ارظن لىل ISE ةكبش تاهجاو لىل IP لوكوتورب ربع (MTU) لقنلل لىصقأال دحلل ةدحو نيوكتب مق نأ نمضى اذهو. SD-WAN ةكبش ةيشغتل عقوومل لىصقأال دحلل نم لكشب بعوتست ةميق ةيشغتل زاتحتل ادج ةريبك اهتعي بطب نوكت يتلاو (DF تب ةعومجم عم) IP مزح ئشنى ال ISE (DF=1) اذ هراطح متي يذلاو طيسو زاهج ةطساوب ةئزجتلا لىل ةجالحا نودب SD-WAN.

اهب لىصوم ال ISE IP لوكوتورب (MTU) لقنلل لىصقأال دحلل ةدحو دادعإو باسح

1. اذه غلبى، يچذومن لكشب: ةيساسأال ةيدامال (MTU) لقنلل لىصقأال دحلل ةدحو عاشنإ. راسمال لوط لىل ةيسايقلا تنرتي ةكبش تاهجاو لىل 1500 مقرلا.

2. SD-WAN نيمصت تافورصم نم لىصقأال دحلل ديدحت:

- مت يتلا ةماعلا تاقفنلا لىلامجال طفحتمل ريذقتلا وأ قيقدل باسحلاب مق SD (IPsec، GRE، VXLAN، MPLSoGRE، امو) لكذلى عجا. ماقرا لىل لوصحلل نيرومول قئاثلولى عجا. اهترتخا يتلا تارايلالو تالوكوتوربلا لوح ةقيد

نوكمل	لىلأال (تياابل)	تاطحالم
(MTU) لقنلل لىصقأال دحلل ةدحو ةيساسأال ةيدامال	1500	ةيلعف تاطاوترا لىل ةيسايق تنرتي
نع ةفرعمل WAN ةكبش: هنم اهورطم ةيفاضال جماربلا قيرط		
سأر (IPv4) يجرال IP	20	
سأر (NAT-T) UDP	8	UDP في ESP نيمصت مت اذ
سأر ESP	~8-12	
ESP IV (لىل لىبس لىل، AES-CBC)	~16	ريفشتلل ةيمزراوخ عم فلتخي
لىل لىبس لىل (ع ESP ةقداصم، SHA256)	~12-16	لىل لىبس لىل (ع ةقداصم ةيمزراوخ عم فلتخي (ضعبل تب-96، لىل لىل)
(اذهو، GRE) رخأ تايشغت	ريغت	SD-WAN نيمصت سدكم نم اعزج ناك اذ ةفاضل كيدل
ةردقمال ةماعلا تاقفنلا عومجم	تيا ب 68 - 80+	ةيلمعل ةلصلل تاذ تانوكملل عيمج عومجم كب ةصاخال رشنل
(MTU) لقنلل لىصقأال دحلل ةدحو لىل لىل راسمل	~1432 - 1420 تيا ب	ةيدامال (MTU) لقنلل لىصقأال دحلل ةدحو ةردقمال فيللكتل لىلامجا - ةيساسأال

3. هب لىصوم ال ISE IP MTU نيوكتب:

- لىل لىبس لىل (بوسحمل لىل لىل راسمال (MTU) لقنلل لىصقأال دحلل ةدحو ذخ (لىل لىل نم تيا ب 1420، لىل لىل).
- L2 سوور باسحل (تيا ب 20-70، لىل لىل لىل) يفاضل نامأ شماه حرطا. تقوؤم نزخم ريفوتل وأ ةبوسحمل رىغ ةيوناثل.
- لكشب (PMTU) راسمال MTU فاشتكأ عارجل Cisco SD-WAN لثم لولحل نكمي ةقيد 20 لك اياقلا ةيلالآل هذه لمعت. عقوم لىل عقوم نم قفن لك لىل ةصاخال (IP) تنرتنل لوكوتورب ربع (MTU) لقنلل لىصقأال دحلل ةدحو رابتخال ةجيتنو. عقوم لك في ةيلالال لقنل فورطل اقفو ايكيمانيد اهل يدعتو قفنلاب عقوومال ني ب (MTU) لقنلل لىصقأال دحلل تادحو مي قفلتخت نأ نكمي، لكذل تقولل رورم عم ريغتت نأ نكمي و.

- اھب ىصوملاو ەنمآلا IP لوكونورب ربع (MTU) لقنلل ىصقألا دحلا ەدحو نوكت
تياپ 1400 و 1350 نيب تاهوي راني سلا ەذە لثم ي ISE تاهجاو

تياپ 1350 غلبت ي تال IP لوكونورب ربع (MTU) لقنلل ىصقألا دحلا ەدحو نوكت ام ابلاغ
ەياغلل ەيوق ەياذب ەطقن

ISE نيوكت (CLI لال خ نم لاثم):

ەكبش ەهجاو لكل Cisco ISE زاھب ەصاخلا (CLI) رماوالا رطس ەهجاو ىل رمالا اذە ذيفنت م تي
ەبسانم.

```
<#root>
```

```
!  
interface GigabitEthernet0 ! Or the specific interface used for RADIUS/SDA communication
```

```
ip mtu 1350
```

```
!
```

ISE IP MTU: تاريغي غتل ەماھلا ەي لي غشتال تارابتال

- اذە بلاطي ISE ەهجاو ىل ip mtu رمالا قيبطت درجمب: ەمدخلال لي غشت ەداعا بولطم
بجي و ەمدخلال ىل رثوي ريغي اذە ISE قيبطت تامدخ لي غشت ەداعا ب مدختسملا
ىل لوصحلل ەي مسرل Cisco ISE قئاثو عجار. ططخم ەناي ص راطا اناثا ەتلودج
تاءارجال لي صافت.
- (MTU) لقنلل ىصقألا دحلا ەدحو لي دعت قيبطت بجي: ISE دقع عيج ىل قيبطت
PAN، ەي ساسألا (PAN) رشنال ي ISE دقع عيج ىل تباث لكشب اذە IP لوكونورب
SD-WAN ەكبش ربع NAD ەزھاب لصتت ي تال (PSN) ەسايسلا ەمدخ دقع، ەيونال
عقوتم ريغ كولس ىل ەقسانتملا ريغ MTU تاداعا ي دؤت.
- ي قيقد لكشب ريغي غتال اذە رابتخاب مق، چاتنال ي قيبطتال لب ق: لماش صحف
عونتم مزح ماھجا عم لاصتال رابتخا لثم تاودأ مدختسا. رايطلا وأ ربتخملا رشن ەي لمع
: ەياھن ىل ەياھن نم MTU ەجلاعم نم ققحتلل تب-DF طبض متو
 - Linux لي غشتال ماظن ىل دنست ي تال ەمظنالا

```
ping
```

```
-s
```

```
-M do
```

تتباث صارقأ تاكرحم 8 + ةلومحل = IP ةمزح مچح يلامچا. ICMP ةلومح مچح s ددحي - :ةطحالما
(تياپ 20 ةعس IPv4 لوكوتوربل HDR ةتباث صارقأ كرحم + ICMP)

- Windows:

ping

-f -l

(. ICMP ةلومح مچح ددحي - :ةطحالما)

- Cisco IOS/Cisco IOS-XE® جمانرب

ping

size

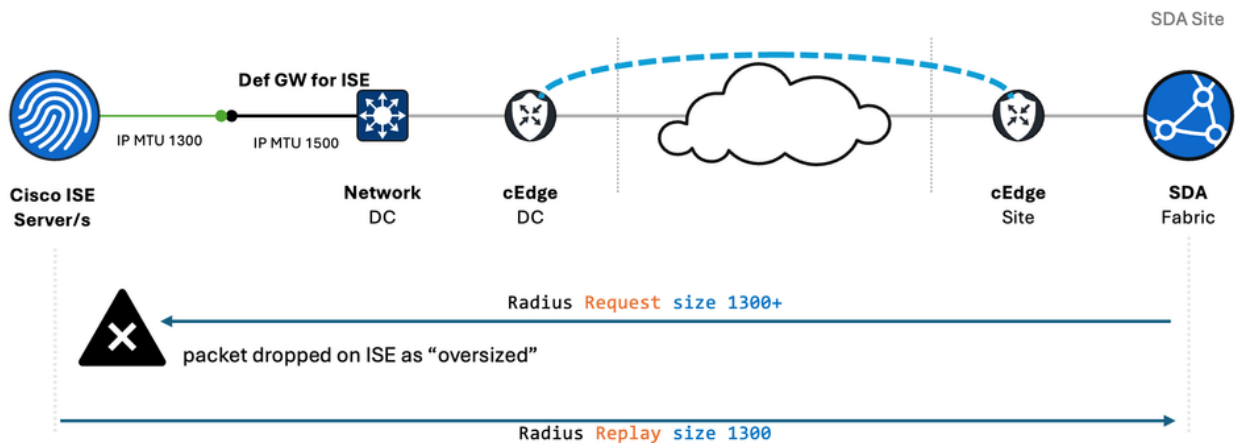
df-bit

- ربح (MTU) لقنلل ىصقألا دحلا ةدحو ةميق طبض دنع - ISE ل ىلوالا هيچوتلا ةطقن - تانايبلا زكرم يي ىلوالا هيچوتلا ةطقن نيوكت نم دكأت، ISE ةهجاو ىلع IP لوكوتورب ةدحو ةميق مادختساب اضيا - ISE ةيعرفلا ةكبشلاب ةطبترملا 3 ةقبطلا ةهجاو ةصاخو IP لوكوتورب ربح (MTU) لقنلل ىصقألا دحلا مدع يدؤي شح، 1 Challenge يي ءحضوملا كلت لثم تالاح ثودح عنم ىلع دعاسي اذهو ةلماعمب (ISE) ةيوهلا تامدخ كرحم مايق ىلا (MTU) لقنلل ىصقألا دحلا ةدحو قباطت اهتالفاو مچحلا ةريبك اهنأ ىلع ةدراولا مزحلا (MTU) لقنلل ىصقألا دحلا ةدحو ىلع يوتحت ISE ةهجاو تناك اذا، لاثملا ليبس ىلع ةدحو مادختساب ءنوكم ىلوالا هيچوتلا ةطقن لظت نكلو، (1300، لاثملا ليبس ىلع)

إلى إلسررمال مزحلإ نإف، 1500 غلبت يتلإ ةيضارتفالا (MTU) لقنلل ىصقألا دحلإ متي وامتئزت متي ال تياب 1500 نم رغصأ انهكلو تياب 1300 نم ربكأ نوكت يتلإ ISE 1. يدحتلإ يف حضوم وه امك — ISE ةطساوب انه صللختلإ مزل اذإ ةئزتلا ءارجإ ىلع ةرداق ىلوالأ هيجوتلإ ةطقن نأ نم دكأت، كلذل ىلإ ةفاضلإاب ءادلأ ضافخنا ىلإ يدؤي ال كلذب مايقلا نأو، رمالأ.

- الك يفو، هلمكب لاسررالا راسم ربع (MTU) لقنلل ىصقألا دحلإ ةدحو ثي دحتب مق ىصقألا دحلإ ةدحو ةاعارم مهمال نم، ISE ىلع IP MTU تادادعإ ثي دحت دنع - نيهاجتالا ةمبيق ةاذحم مت مل اذإ. نيهاجتالا الك يفو، هلمكب لاسررالا راسم ربع (MTU) لقنلل ىصقألا دحلإ ةدحو عم ISE ىلع انه نوكت مت يتلإ (MTU) لقنلل ىصقألا دحلإ ةدحو لكاشم أشنت نأ نكميف، ىلوالأ ةوطخل ةباوبل 3 ةقبطلا ةهجاو ىلع (MTU) لقنلل #1. يدحتلإ يف حضوم وه امك ةلثام.

ةصاخلا (MTU) لقنلل ىصقألا دحلإ ةدحو ةعس ضفخ مت اذإ، لاثمل لىبس ىلع (MTU) لقنلل ىصقألا دحلإ ةدحو لظت امنيب تياب 1300 ىلإ ISE رادصلإاب مزحلإ طاقسإ نكميف، ةيضارتفالا ةباوبل ىلع ةنوكم تياب 1500 ةعس ةيضارتفالا عئاش لكشب اهؤاشنإ متي يتلإو، مچحلإ يف تياب 1500 ىلإ 1300 نم حوارتت يتلإ اهمج مخضتل ارطن ISE ليغشتلإ ماظن ةطساوب، ةكبشلل ةزهجأ ةطساوب.



(MTU) لقنلل ىصقألا دحلإ ةدحو تاريغيغت خسن نم امئاد دكأت، ةلكشمال هذه بنجتل ةزهجألا عيمج ىلع اهسكع، للاثم لكشبو، ىلوالأ ةوطخل ةباوب ىلع ISE ىلع قسانت ىلع ظافحلإ ىلع اذه دعاسيو. 3 ةقبطلا عطقم سفن لخاد ةيفرطلل ةفيضمال ريغ مزحلإ طاقسإ تالاح عنمو ةيانه ىلإ ةيانه نم (MTU) لقنلل ىصقألا دحلإ ةدحو ةعقوتمل.

رارقلا

Cisco ISE مداوخ ىلع IP لوكوتورب ربع (MTU) لقنلل ىصقألا دحلإ ةدحو تادادعإ ميظنت نإ يتلإ لقنلل ةقبط ىلع (MTU) لقنلل ىصقألا دحلإ ةدحو ةلاعفل دودحل مادختساب ىلإ SDA دودح دنع (MTU) لقنلل ىصقألا دحلإ ةدحو ةاذحمو SD-WAN نيضمضت ةيلمع اهضرقت رارقتسإ نامضل يساسأ بلطتم لب ةيصوت درجم سيل SD-WAN نم Cisco Edge هجوم لقن نأ نم مغرلا ىلع. ةأزجمل ةثي دحلإ تاسسؤمل تالكبش يف اهئادأو اهتيقو وثومو AAA تامدخ ةلقرع نكمي هنأ لا، ةمهم ةيلآ نع ةرابع راسم لل (MTU) لقنلل ىصقألا دحلإ ةدحو فاشتكا يف مكحتلإ ىوتسم ميظنت وأ ICMP ةيفصت لثم لماوع ةطساوب ةيلمعل اهتيللاعف

SD-WAN تائيپ

ىلع IP لوكوتورب ربع (MTU) لقنلل ىصقألا دحلا ةدحول ىقاباتسا نيوكت عارجا لالځ نم ةكبشلا ىسدنهمل نكمي، (تياپ 1400 ىل 1350 نم، لاثملا لىبس ىلع) ةيوهلا تامدځ كرحم (MTU) تاطحما ةددعتم ةدحولاب ةطبترملا مزحلا طاقسإ تالاح رطځ فيفخت اهي سدنهمو يويح رمأ اذهو. اهب وُبنتلل ةيلباقو ةنورم رثكأ ةكبش تايلمع ىل ىدؤي امم، ريبك لكشپ ةئزجتلا قيسنتب ISE موقوي شيح Cisco نم SDA قيبطت رشن تايلمع ىف صاخ لكشپ ىلع دمتعت ام ابلاغ يتلاو، ةيكيما ني دل تاسايسلا ذيفنتو ةروطتملا ةريغصلا رابتځال او داځلا طيځتلا دعي. ةلمحتملا ةريبكلا مكحتلا ىوتسم لئاسرل حجنانلا ميلستلا اهلځو رشنلا ةيلمع حاجنل ايساسأ الماع ISE دقع عيمج ربع قسانتملا نيوكتلاو لماشلا تالځشملا نم.

عجارملاو ريياعملا

Cisco قئاثوو ةيمسررلا ريياعملا عجار، قمعأ مهف ىلع لوصحلل

ل: ددعلا ديحت تاودأ

- (MTU) لقنلل ىصقألا دحلا ةدحو راسم فاشتكا: RFC 1191 رايعملا
- ةئزجتلا مدع تب كلذ ي ف امب، IP سآر ددحي - (IP) تنرتنإلا لوكوتورب: RFC 791 رايعملا (DF).
- ميهافم نمضتتو، IPv6 مادختسا مت اذا ةلص تاځ) IPv6 تافصاوم: RFC 8200 رايعملا (PMTUD ةلثامم).
- (VPN) ةكبشلا لځاد يققنلا لاصتالا عم ةئزجتلاو MTU لكاشم: RFC 4459 رايعملا - VPN تائيپ ي ف ةعئاشلا MTU لكاشم ةرشابم جلاعت

Cisco قئاثوو

- دحلا ةدحو تايصوت لوح تامولعم ىلع لوصحلل Cisco: SDA ميمصتو رشنلا ةلدأ ةيودحلا دقعلا تانيوكتو ةيقيلل (MTU) لقنلل ىصقألا
- ةماعلا فيللكتلا لوح ليصافت ىلع لوصحلل Cisco SD-WAN: ميمصتو نيوكتلا ةلدأ PMTUD تارابتعاو، قفنلا ةهجاو (MTU) لقنلل ىصقألا دحلا ةدحو، نيضمضتلا ةيلمعل SD-WAN ةينب لځاد
- ماظنلاب ةصاخ ليصافت ىلع لوصحلل Cisco Catalyst 9000 Series لوحمل نيوكت ةلدأ ةئزجتلا تاناكمإو (MTU) لقنلل ىصقألا دحلا ةدحو تادادعإ لوح ايساسألا
- لوح تامولعم ىلع لوصحلل: رماوأل رطس ةهجاو ةلدأو Cisco نم ةيوهلا تامدځ كرحم ريځم ip mtu. رماو ةمدځلا ليغشت ةداعإ تاريثأت كلذ ي ف امب، ةهجاو نيوكت

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 چ 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 ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ 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 چ 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 چ 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 چ 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