مراقبة الأحداث باستخدام عارض أحداث موحد على واجهة المستخدم الرسومية (GUI) لـ FMC

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

استكشاف

مثال لصفحة الحدث الموحد

مراجعة الأحداث

تخصيص الأعمدة

حفظ مجموعة الأعمدة

البحث عن حدث

حفظ البحث

الإطار الزمني

الوقت

تصدير الأحداث كقيم مفصولة بفاصلة (CSV)

معلومات ذات صلة

المقدمة

يصف هذا المستند استخدام عارض الأحداث الموحد على واجهة مستخدم رسومية (GUI) على مركز إدارة جدار الحماية (FMC).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الوصول إلى FMC باستخدام امتيازات المسؤول أو محلل الأمان
- FMC مع إصدار يساوي أو يزيد عن v7.0

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- مركز إدارة جدار الحماية الآمن لـ VMware الإصدار 7.2.5

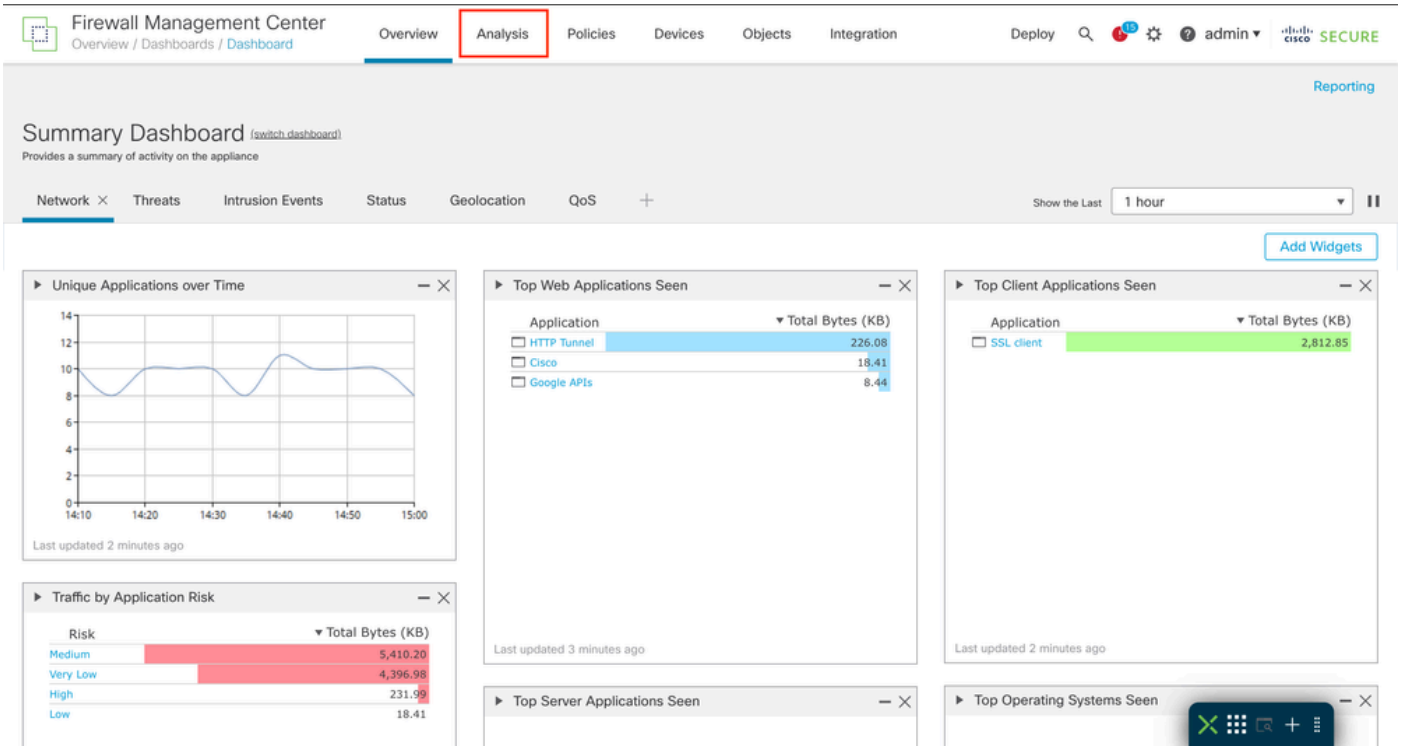
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت

شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

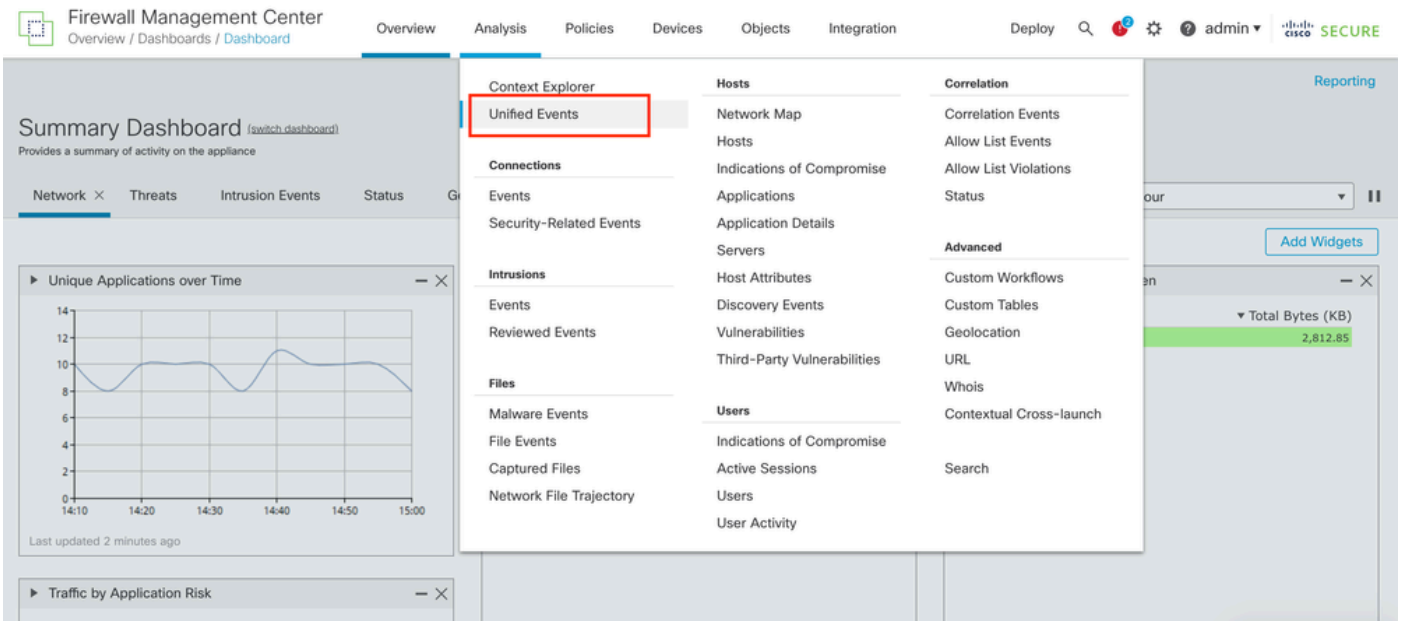
نستكشف

الخطوة 1. سجل الدخول إلى واجهة المستخدم الرسومية (GUI) ل FMC.

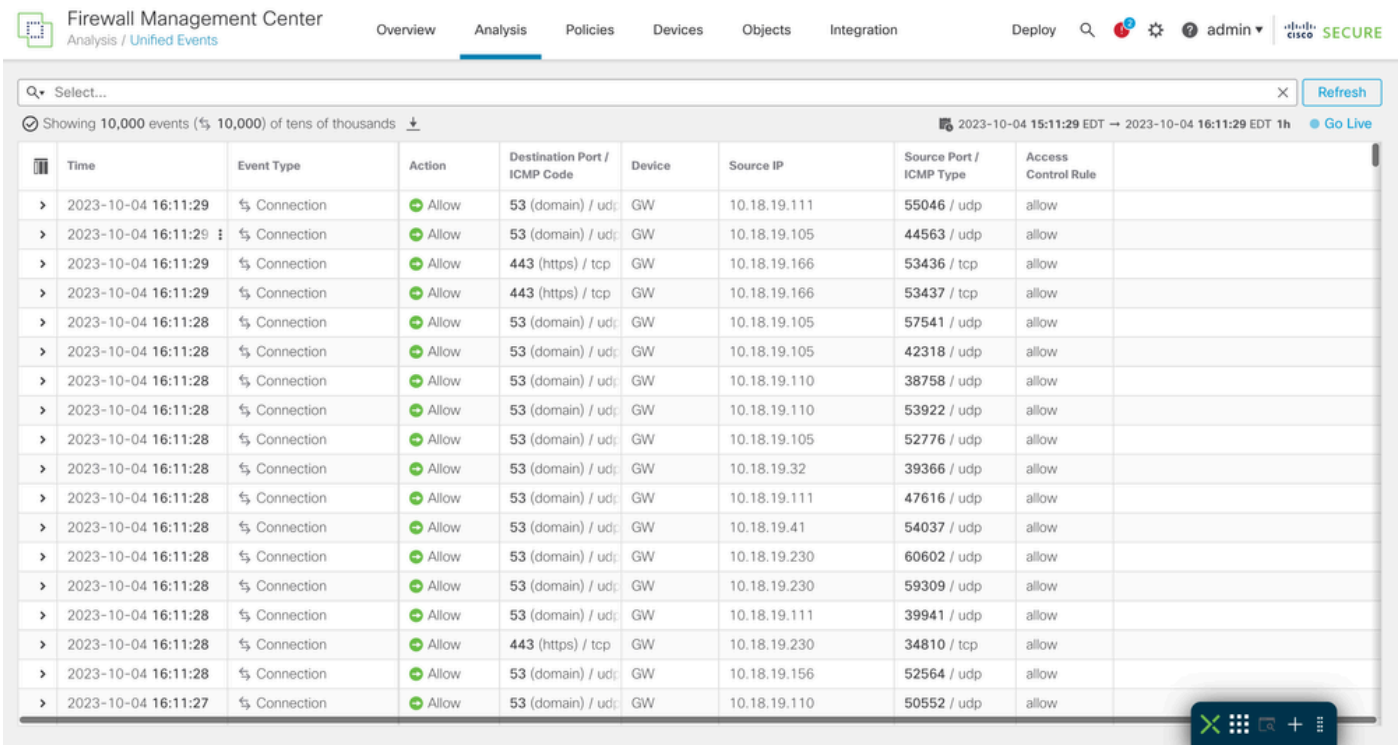
الخطوة 2. انتقل إلى علامة التبويب تحليل.



الخطوة 3. من القائمة المنسدلة، انقر فوق الأحداث الموحدة.

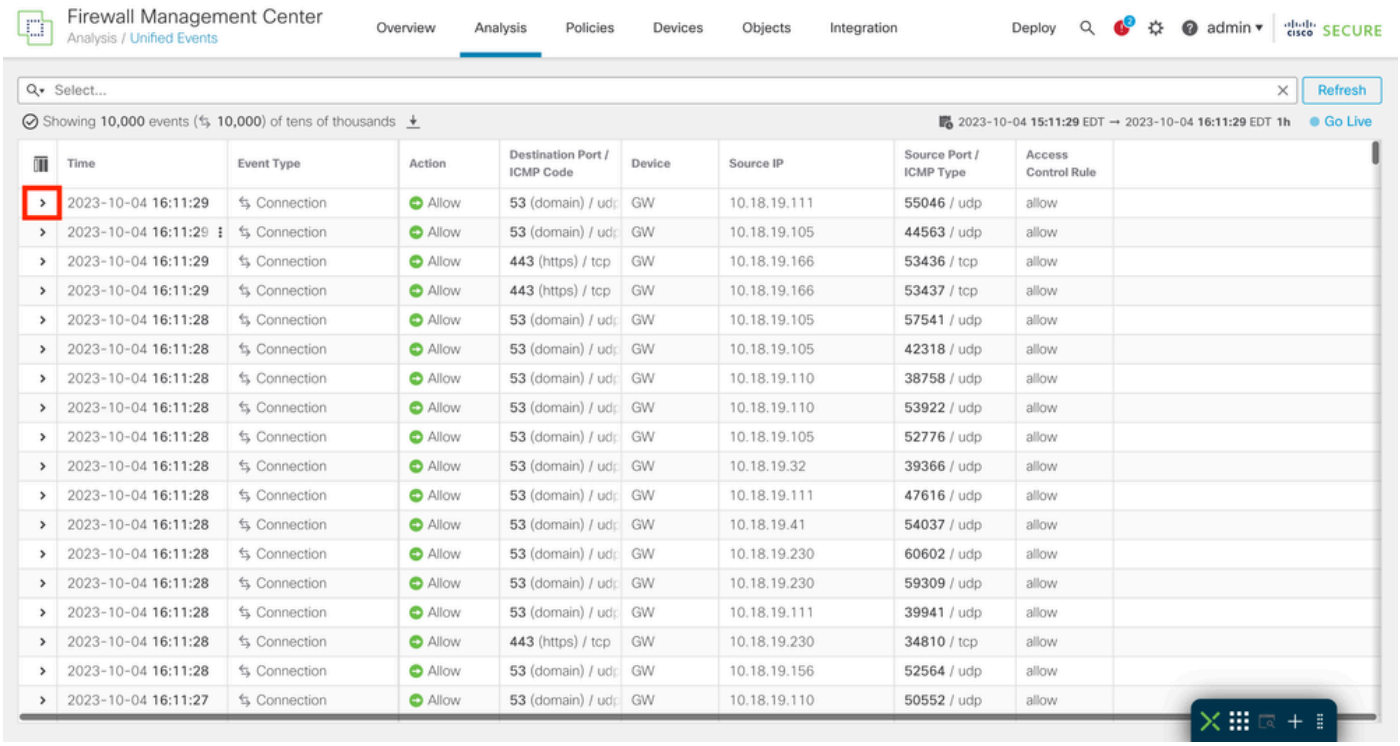


مثال لصفحة الحدث الموحد

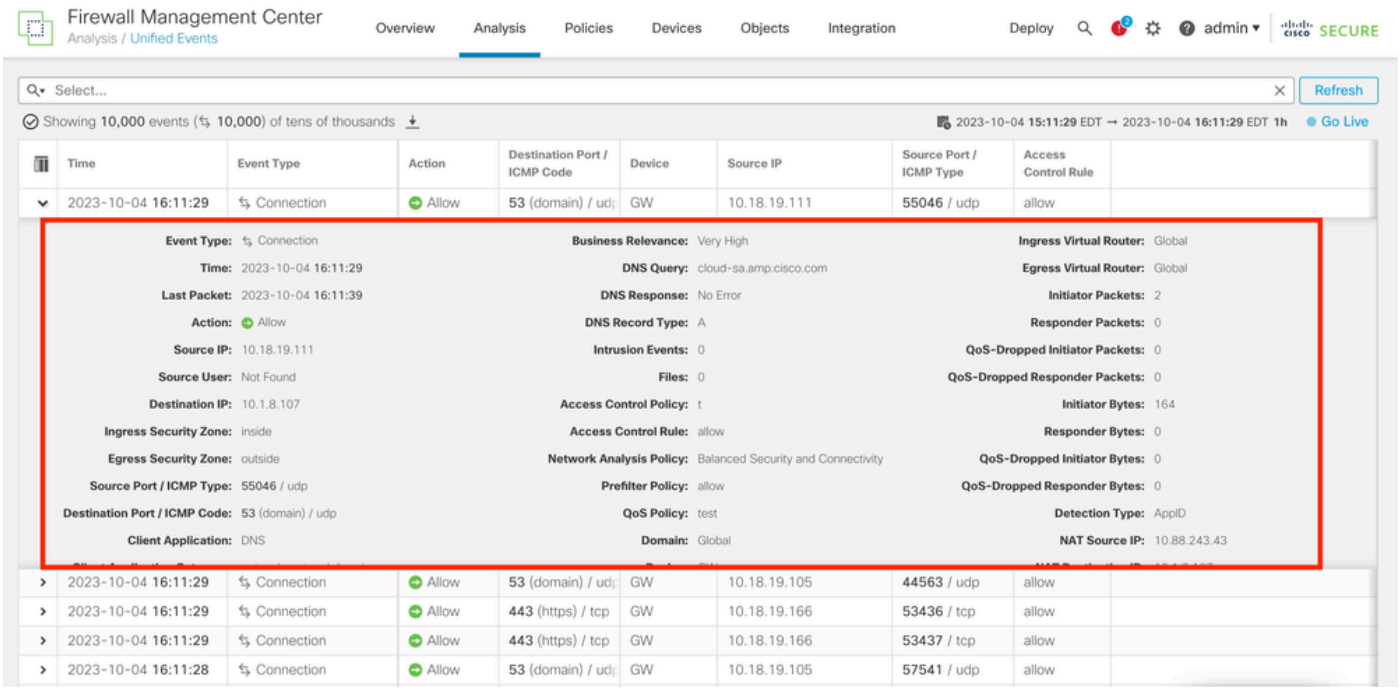


مراجعة الأحداث

الخطوة 1. انقر فوق أيقونة > .

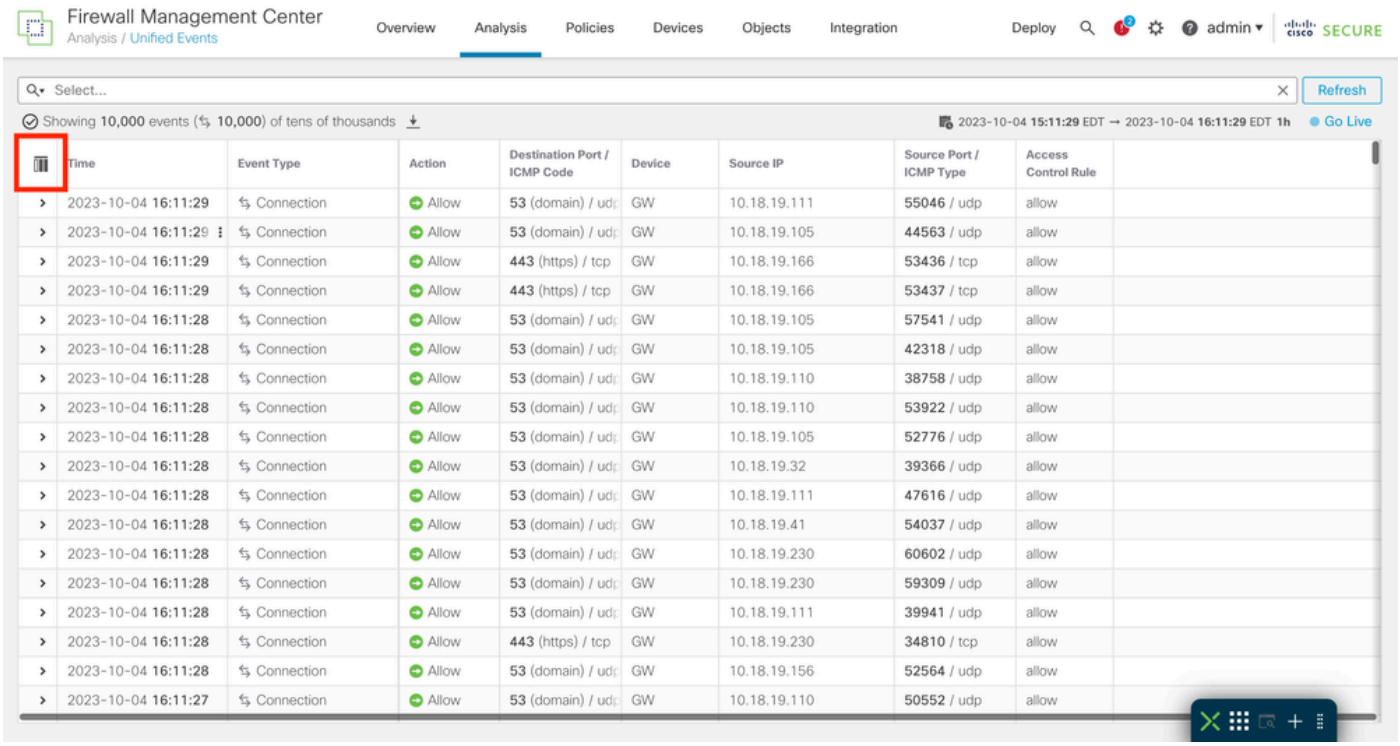


الخطوة 2. يتم عرض المعلومات التفصيلية للحدث.

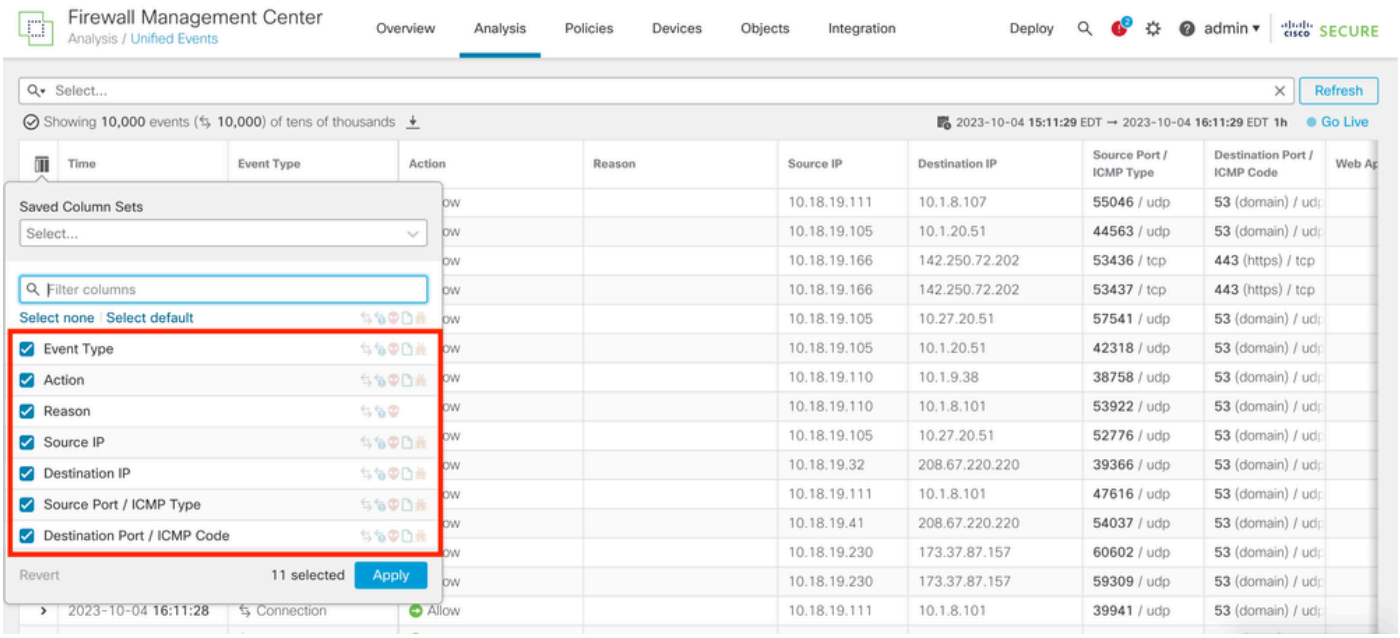


تخصيص الأعمدة

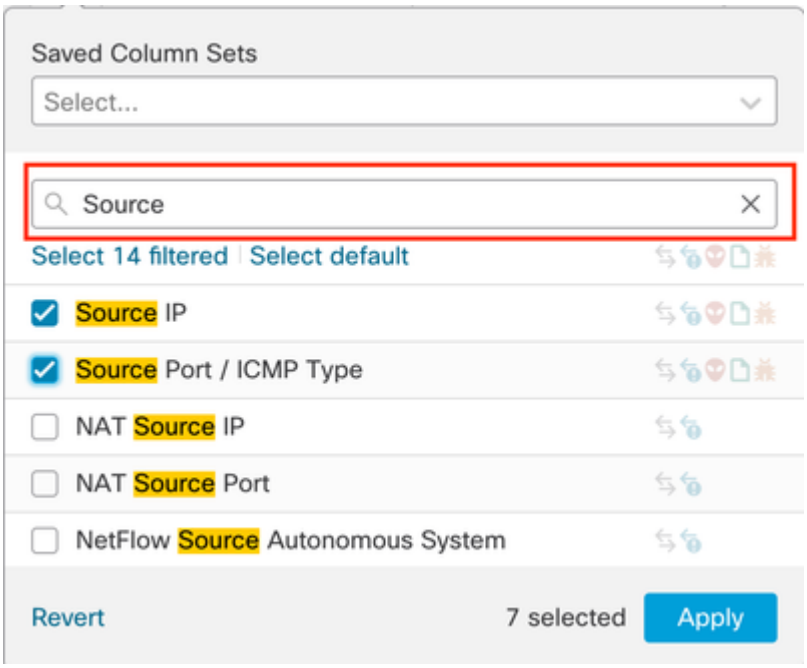
الخطوة 1. انقر على الرمز  .



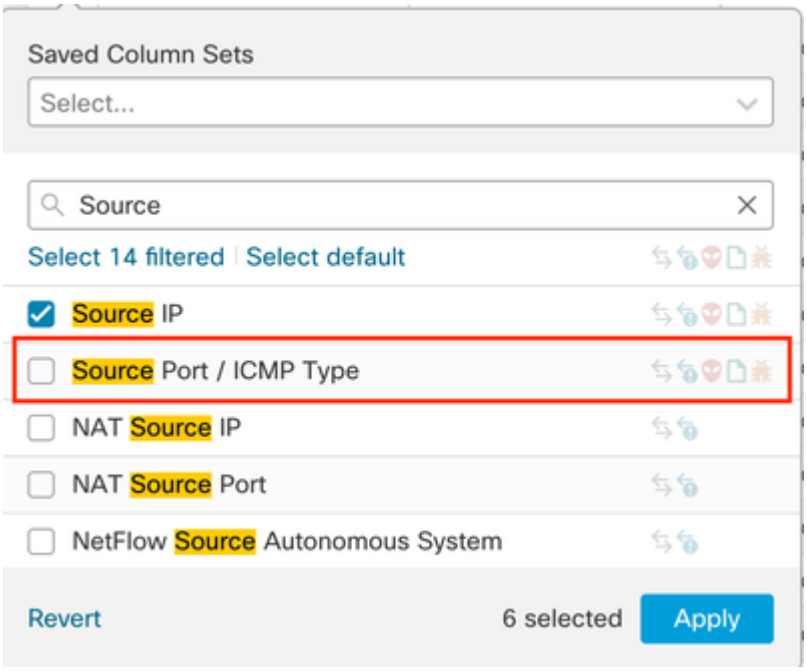
الخطوة 2. حدد حقول الحدث التي تريدها في الجدول.



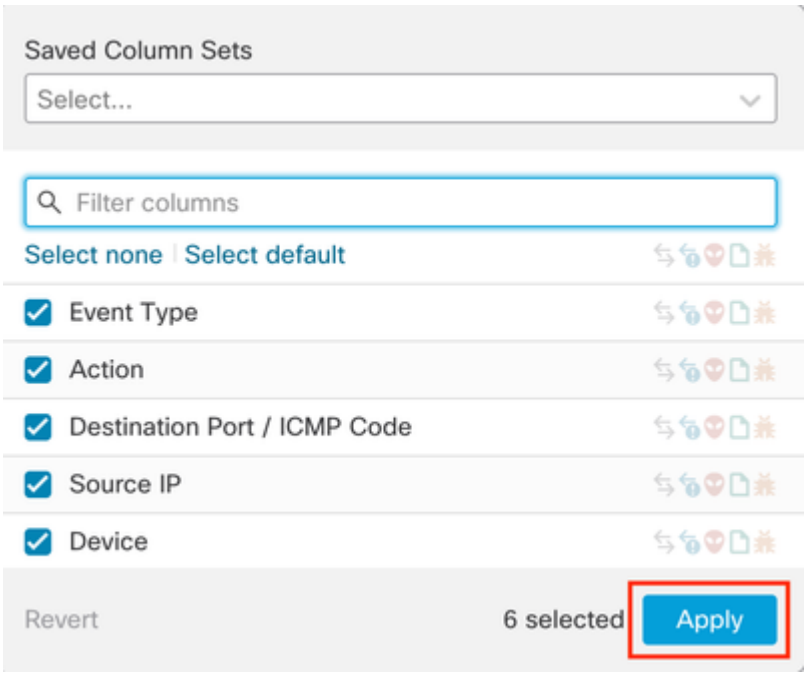
الخطوة 3. (إختياري) ابحث عن الحقل لتسهيل التنقل.



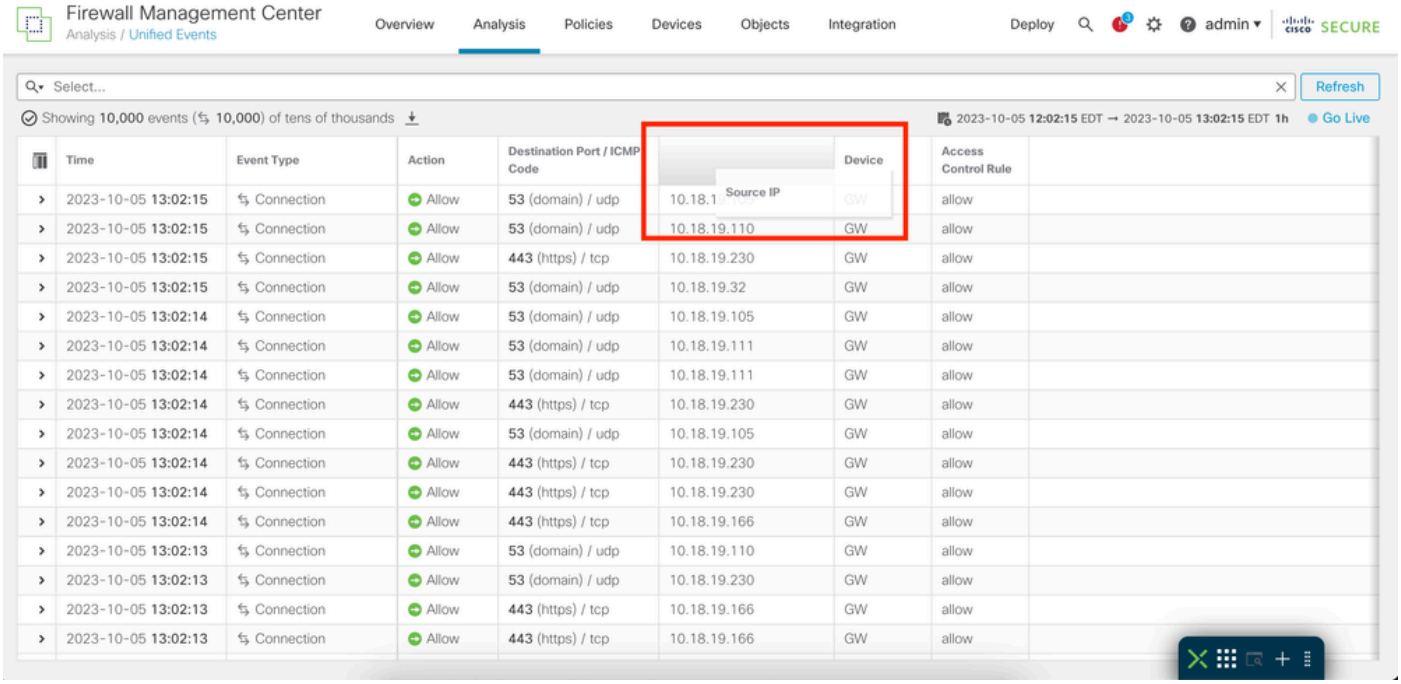
الخطوة 4. انقر فوق حقل حدث لتعطيله أو تمكينه.



الخطوة 5. انقر فوق تطبيق.

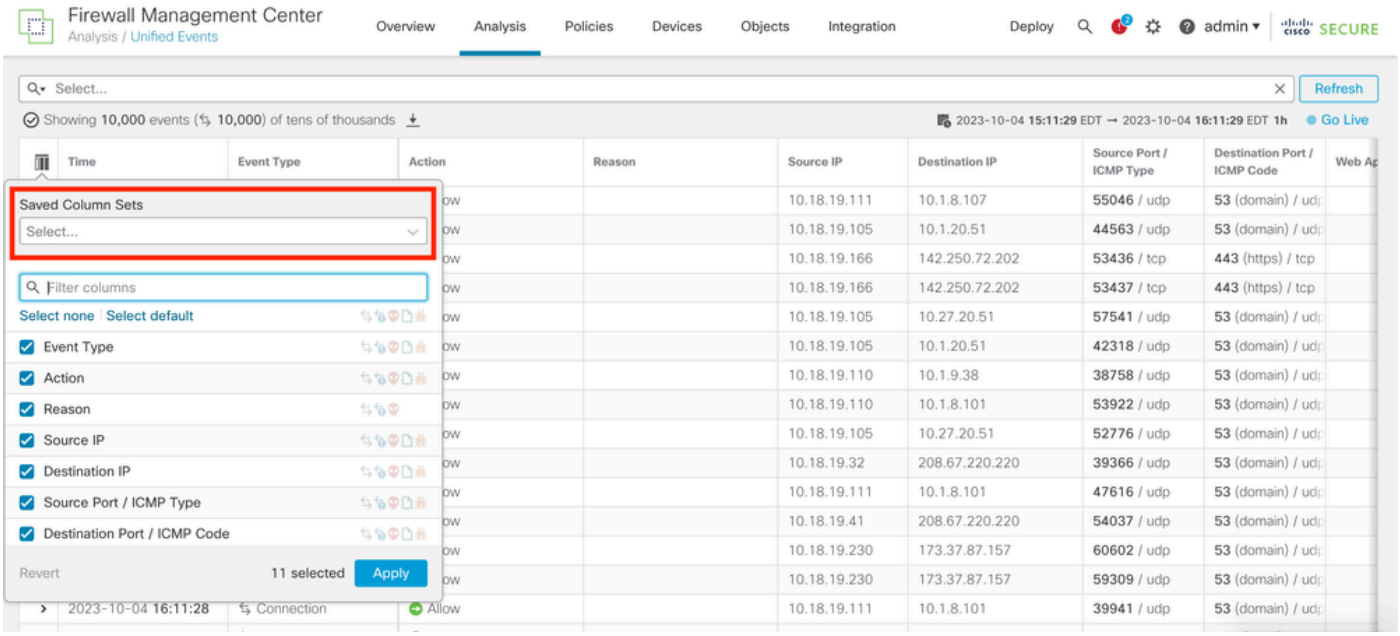


الخطوة 6. (إختياري) يمكنك إعادة وضع الأعمدة بسحب كل واحدة إلى موقع مختلف.

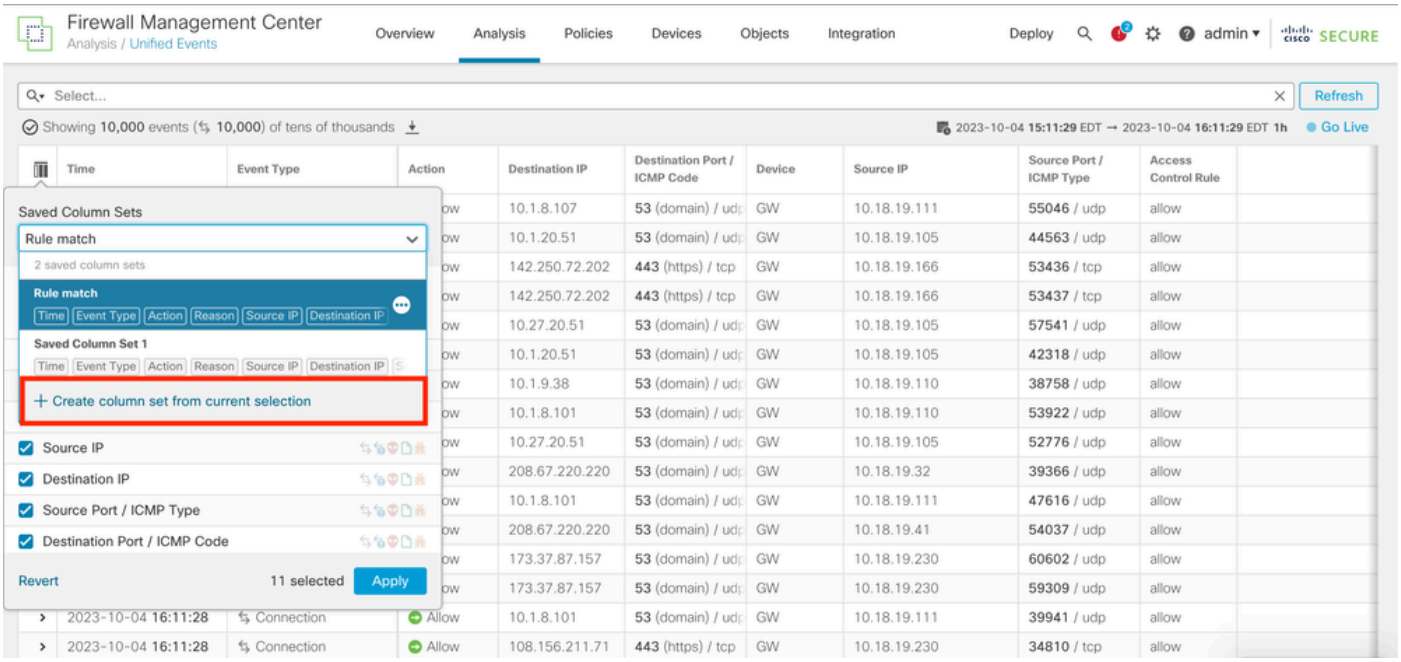


حفظ مجموعة الأعمدة

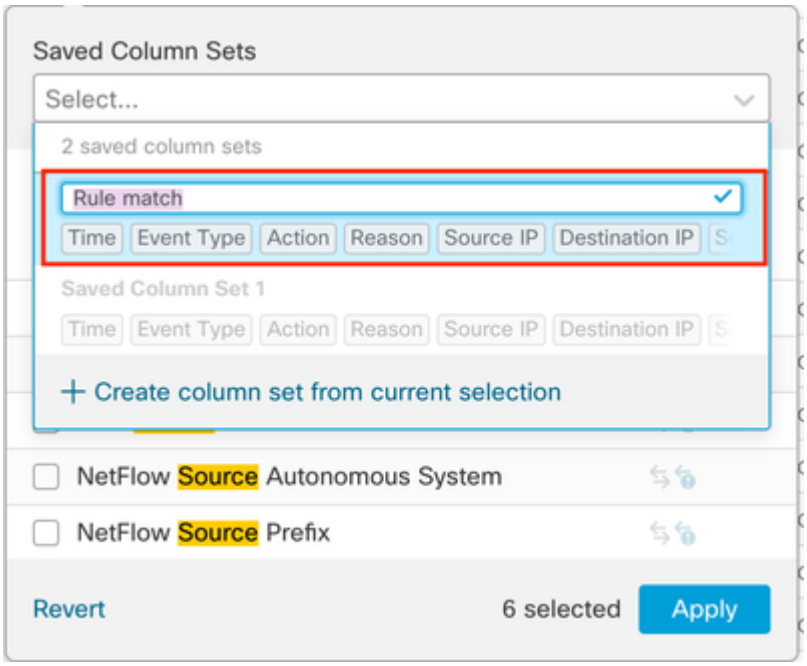
الخطوة 1. انقر فوق مجموعات الأعمدة المحفوظة.



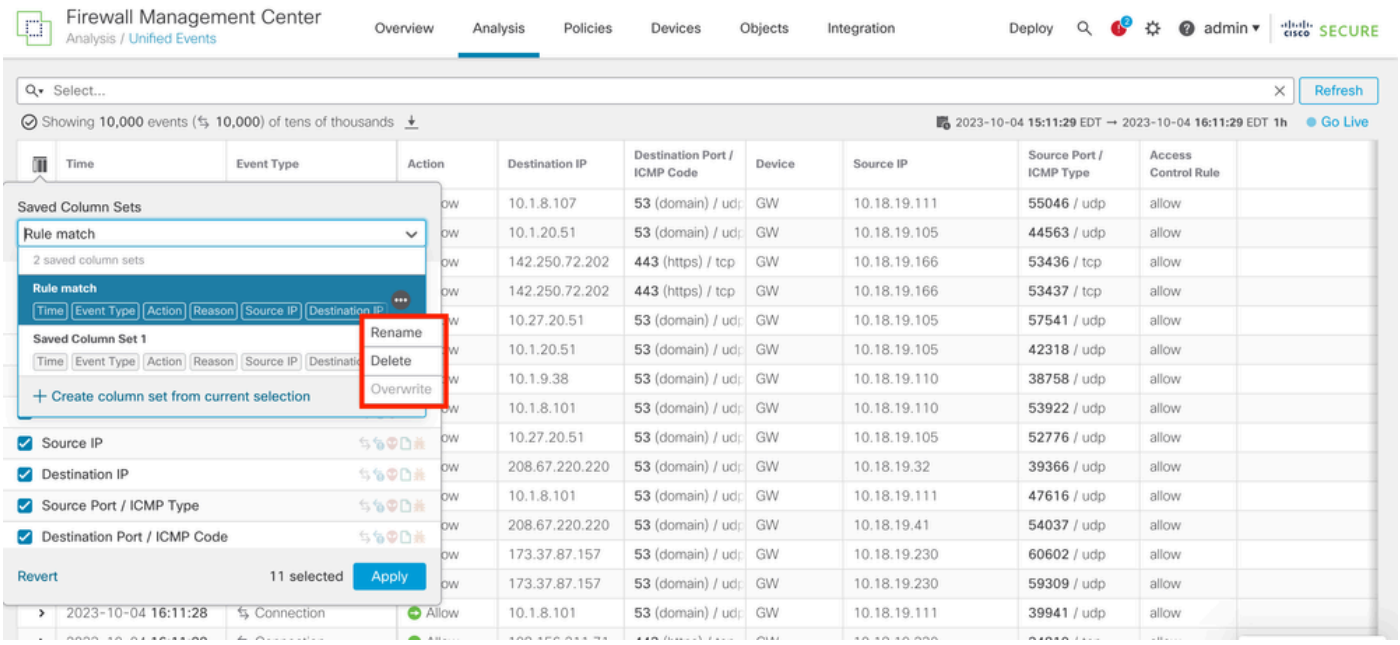
الخطوة 2. انقر فوق إنشاء مجموعة أعمدة من التحديد الحالي.



الخطوة 3. (إختياري) قم بتغيير اسم مجموعة الأعمدة.

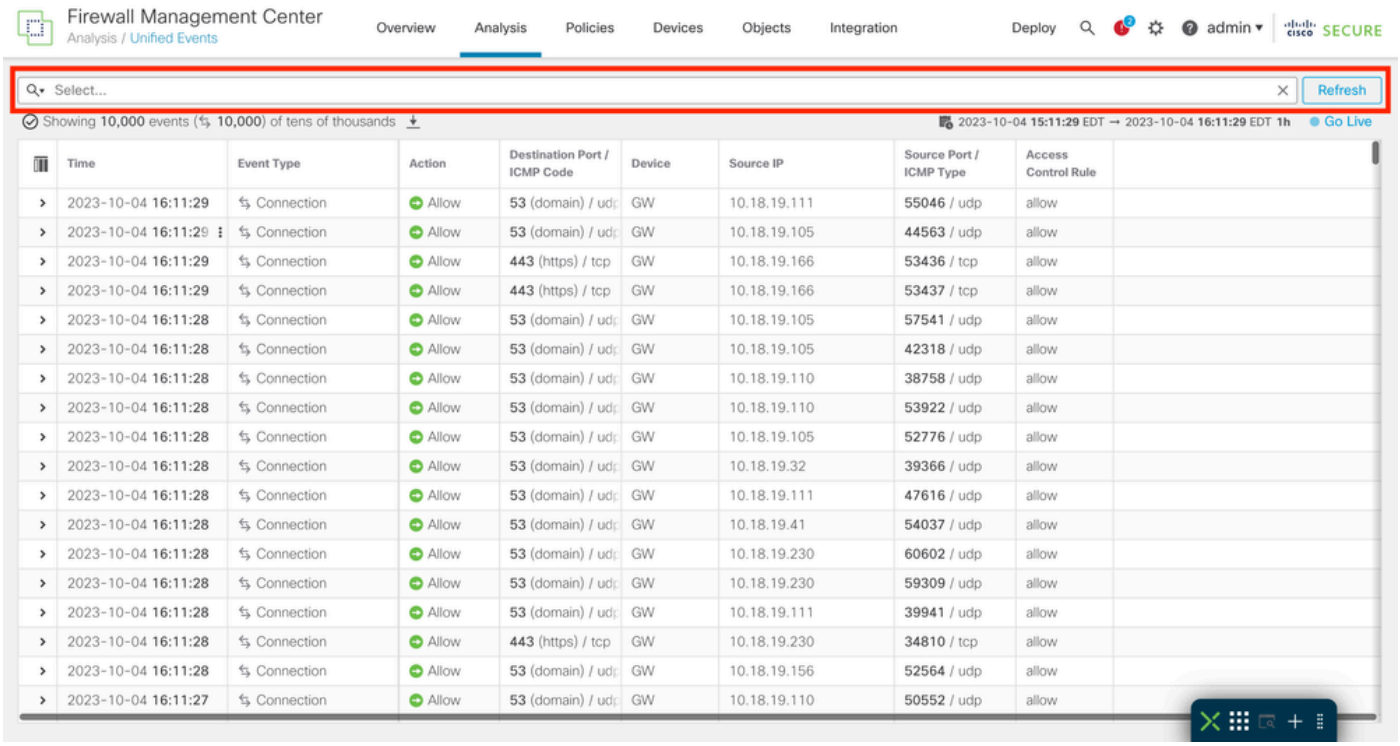


الخطوة 4. يمكنك تحرير مجموعة موجودة بالنقر على البيضاوي (..).

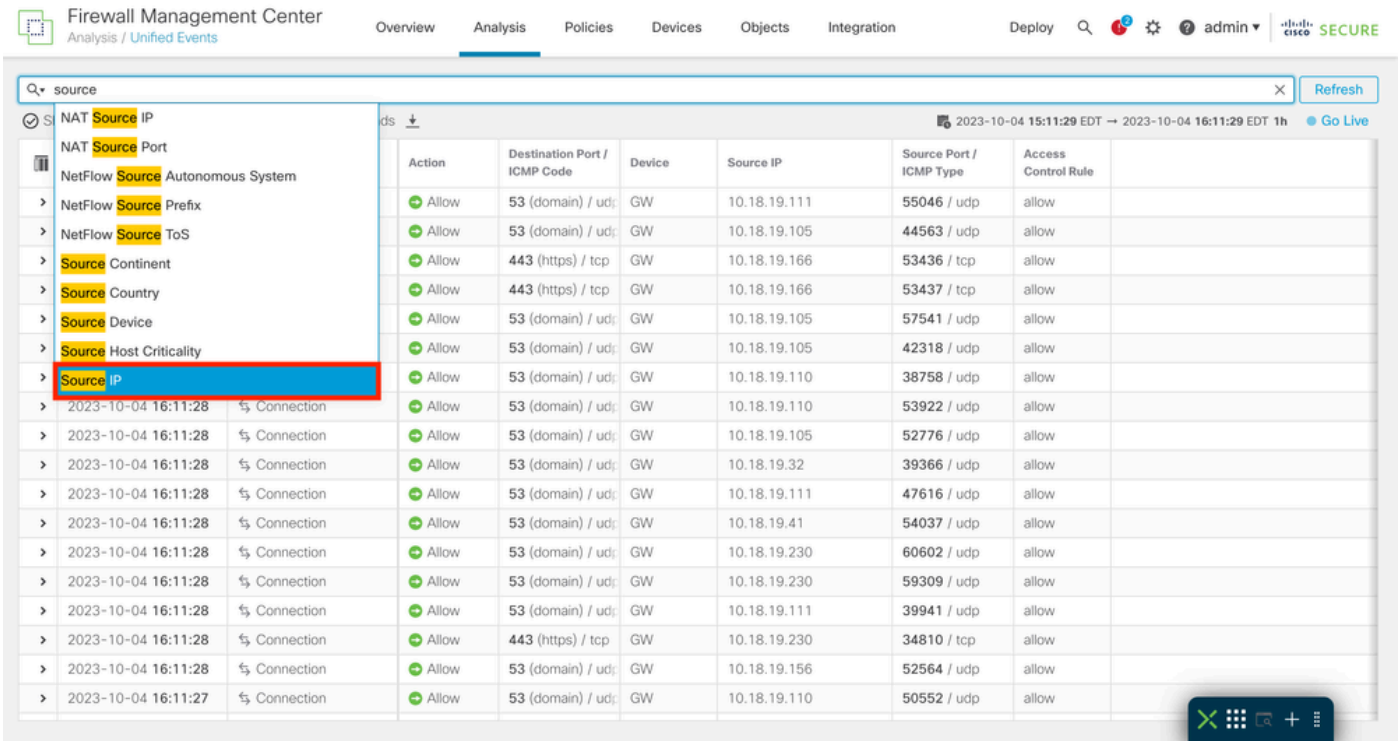


البحث عن حدث

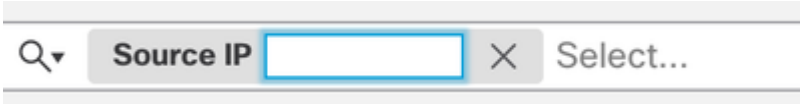
الخطوة 1. لبدء البحث عن أحداث معينة انقر فوق تحديد.



الخطوة 2. حدد الحقل الذي تريد تطبيق عامل التصفية فيه.

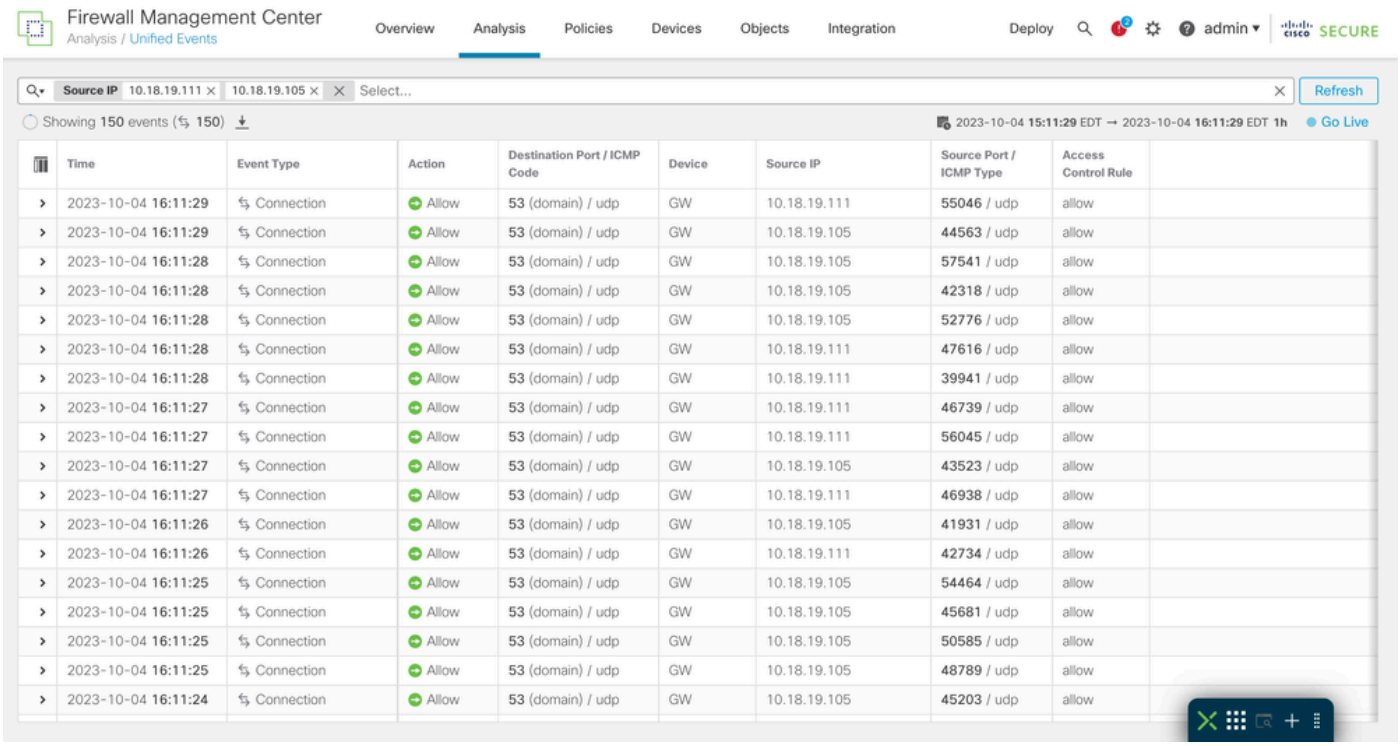


الخطوة 3. اكتب القيم المطلوب إستخدامها كعامل تصفية.

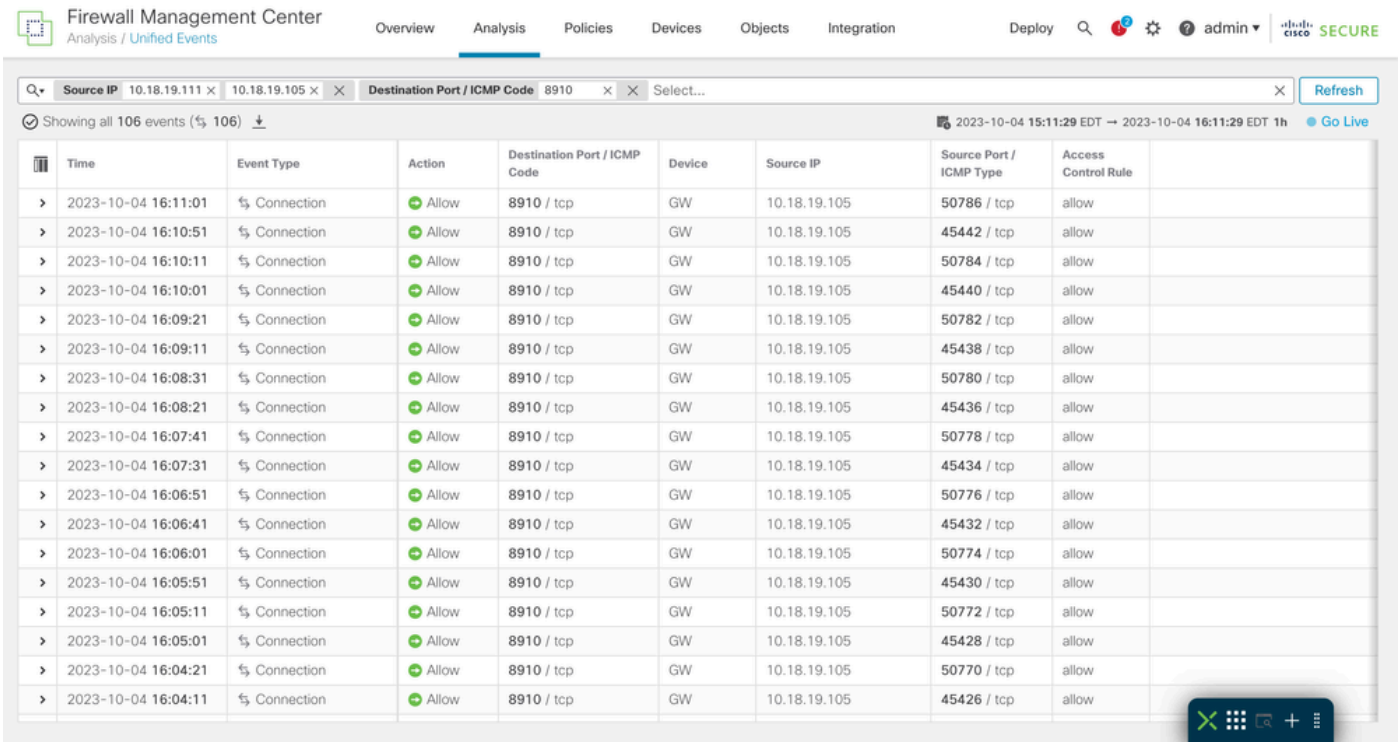


الخطوة 4. انقر فوق تطبيق، لتكوين عامل التصفية.

الخطوة 5. (إختياري) يمكنك إضافة قيم متعددة إلى كل مرشح.



الخطوة 6. (إختياري) أضف العديد من عوامل التصفية حسب الحاجة.

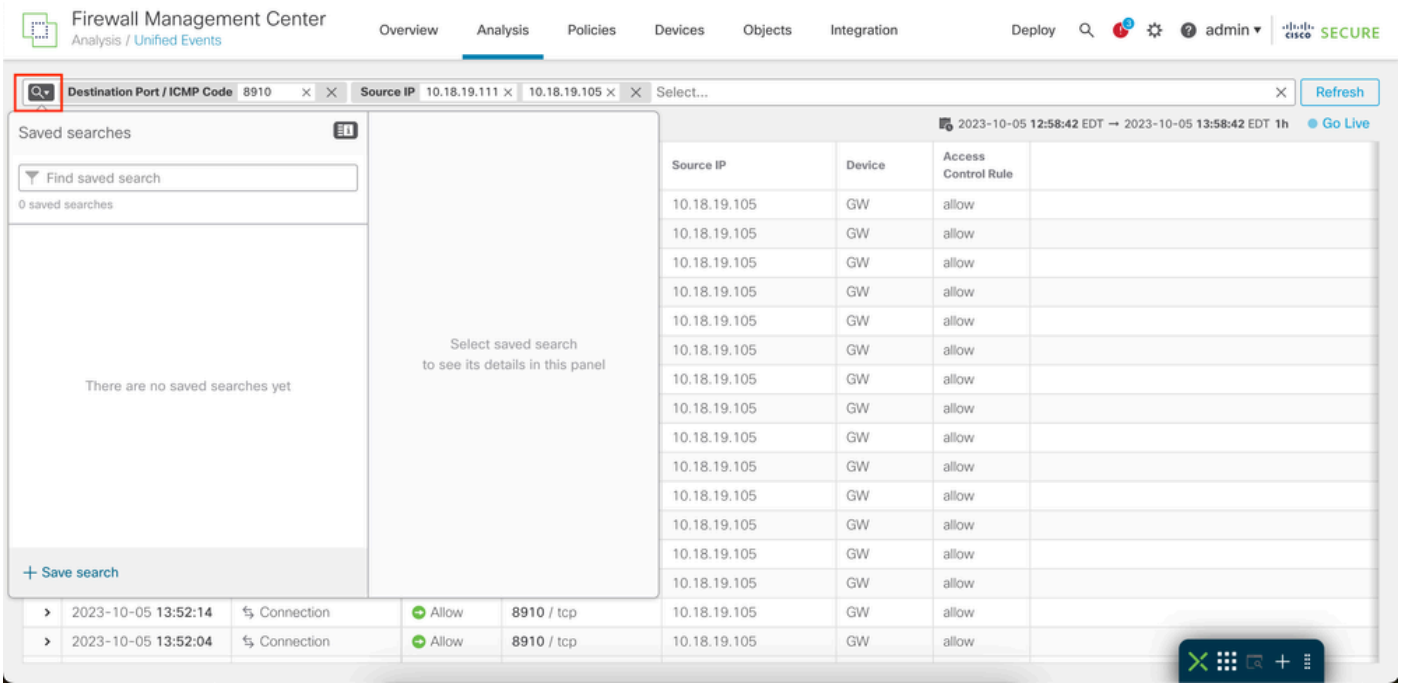


تلميح: يمكنك إستخدام المشغلات (>،<، !، وهكذا) أثناء كتابة القيم.

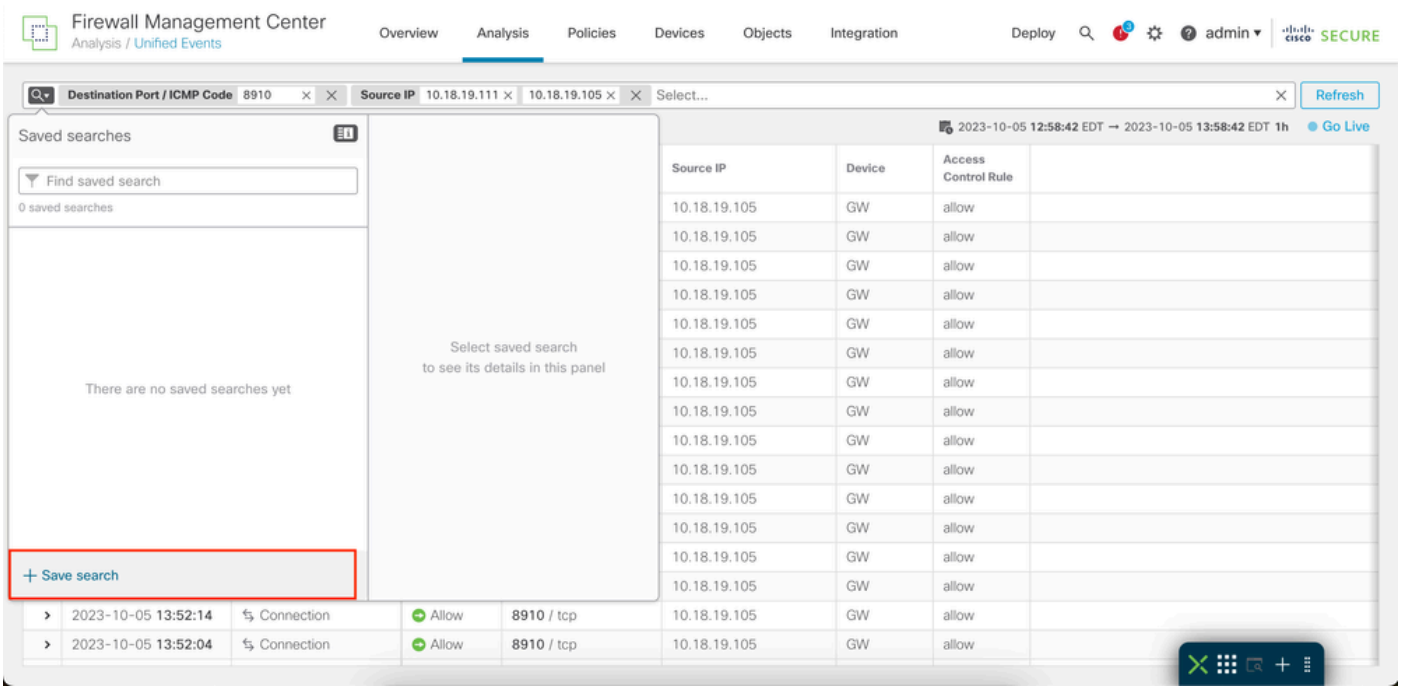
حفظ البحث

من الممكن حفظ عمليات البحث بحيث يمكنك إعادة إستخدام عوامل التصفية التي قمت بإنشائها.

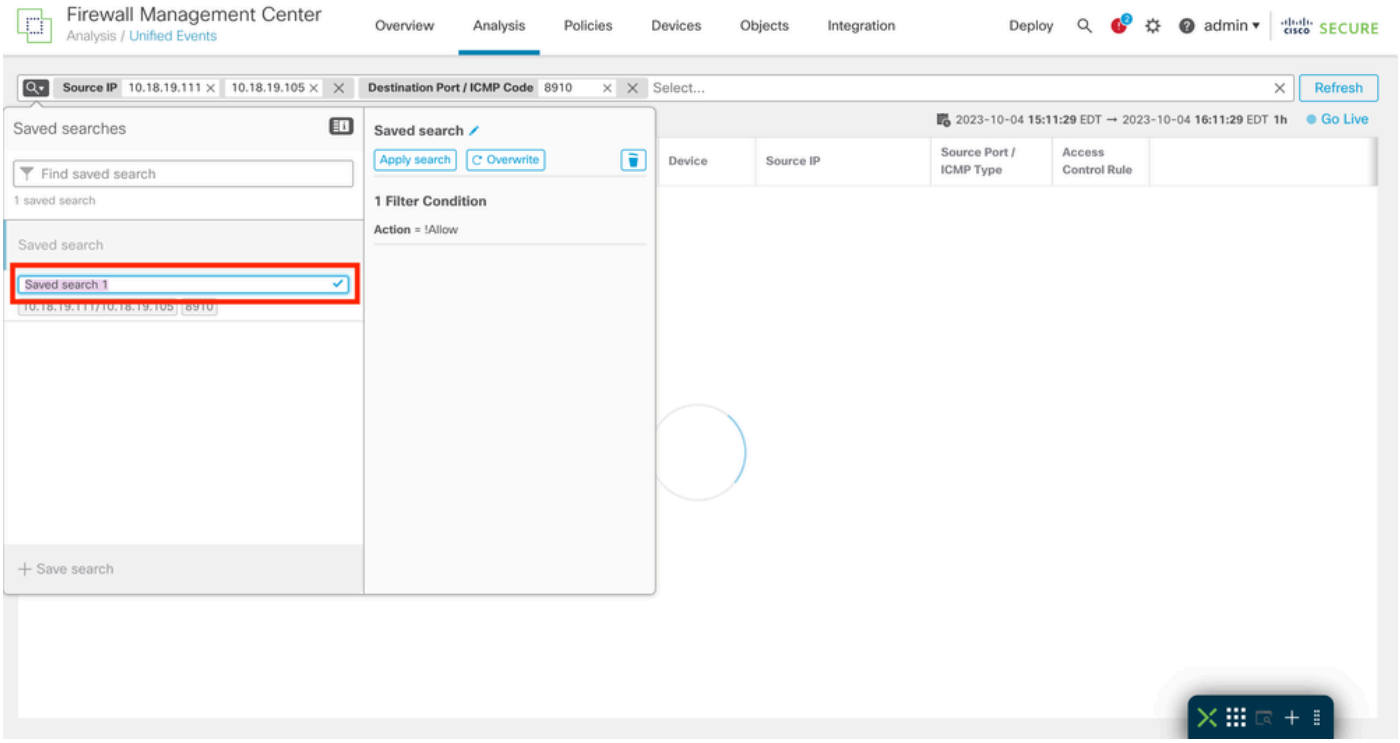
الخطوة 1. انقر على أيقونة العدسة المكبرة.



الخطوة 2. انقر فوق حفظ البحث.



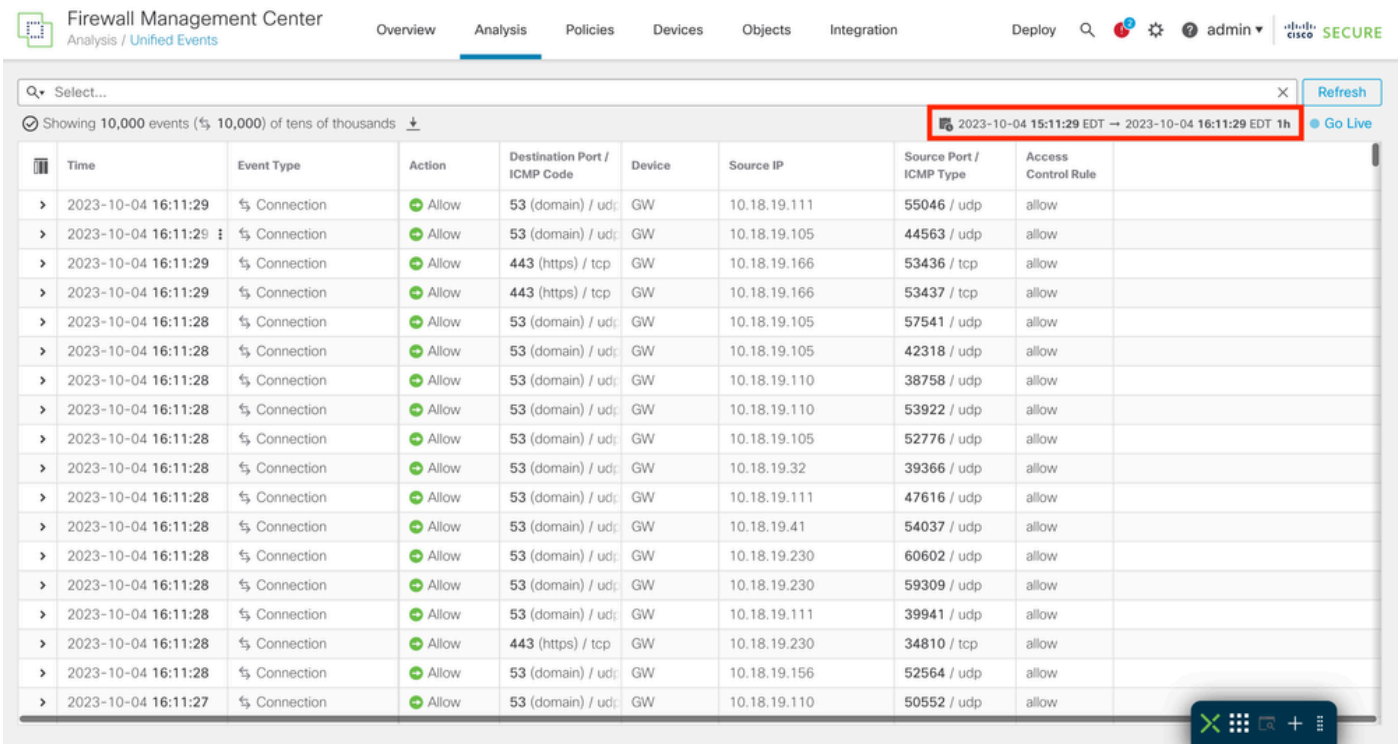
الخطوة 3. (إختياري) قم بتغيير اسم البحث.



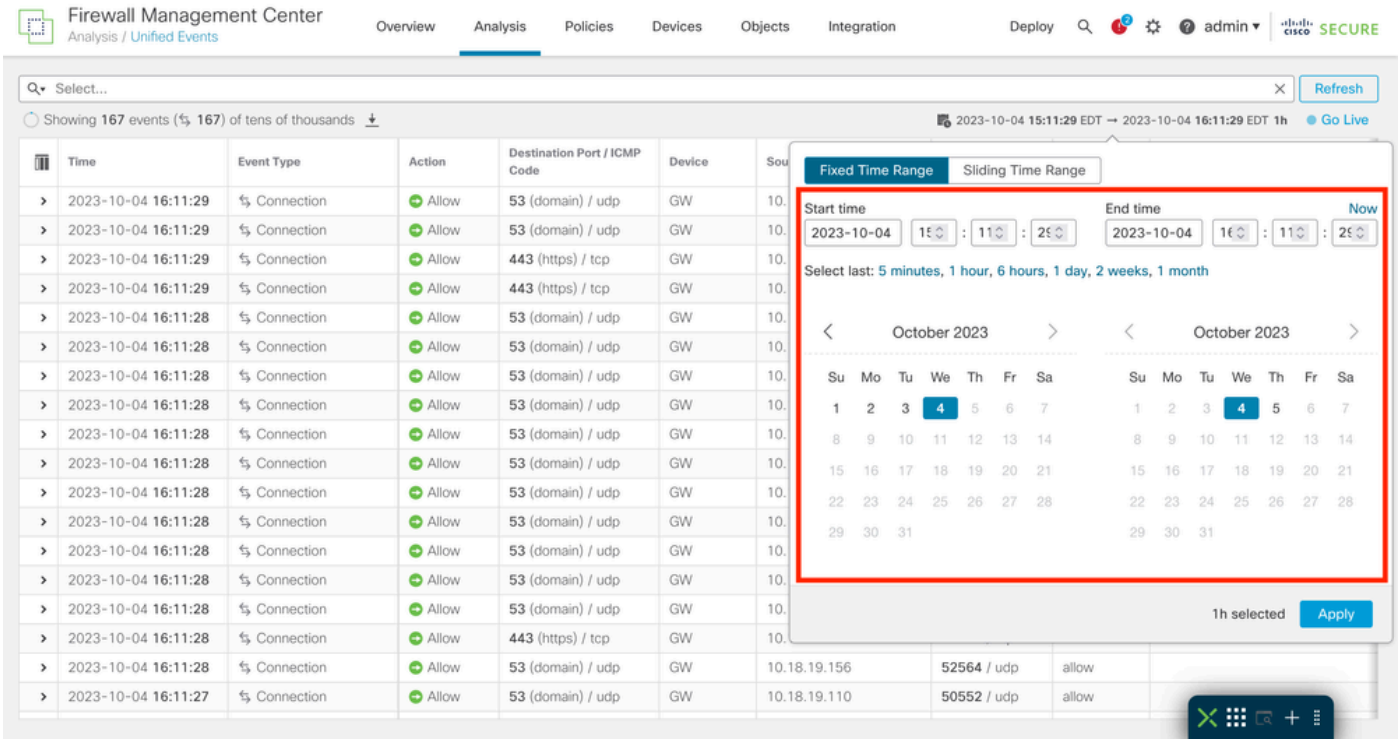
الإطار الزمني

من الأسهل تضييق الأحداث ذات الصلة، بناء على وقت معين، من خلال تعديل الإطار الزمني.

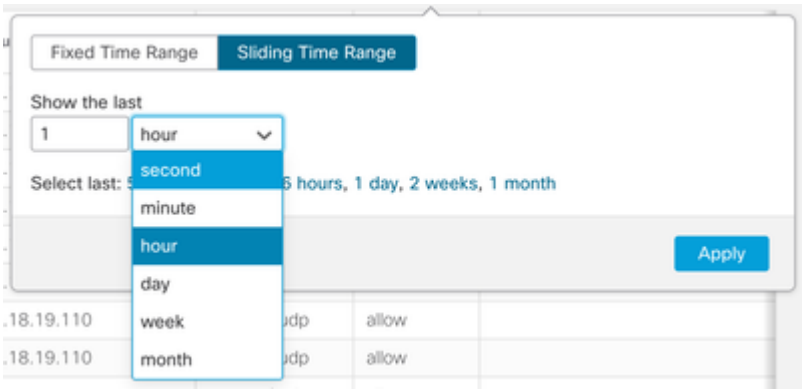
الخطوة 1. لتعديل إطار الإطار الإطار للأحداث، انقر فوق نطاق التاريخ.



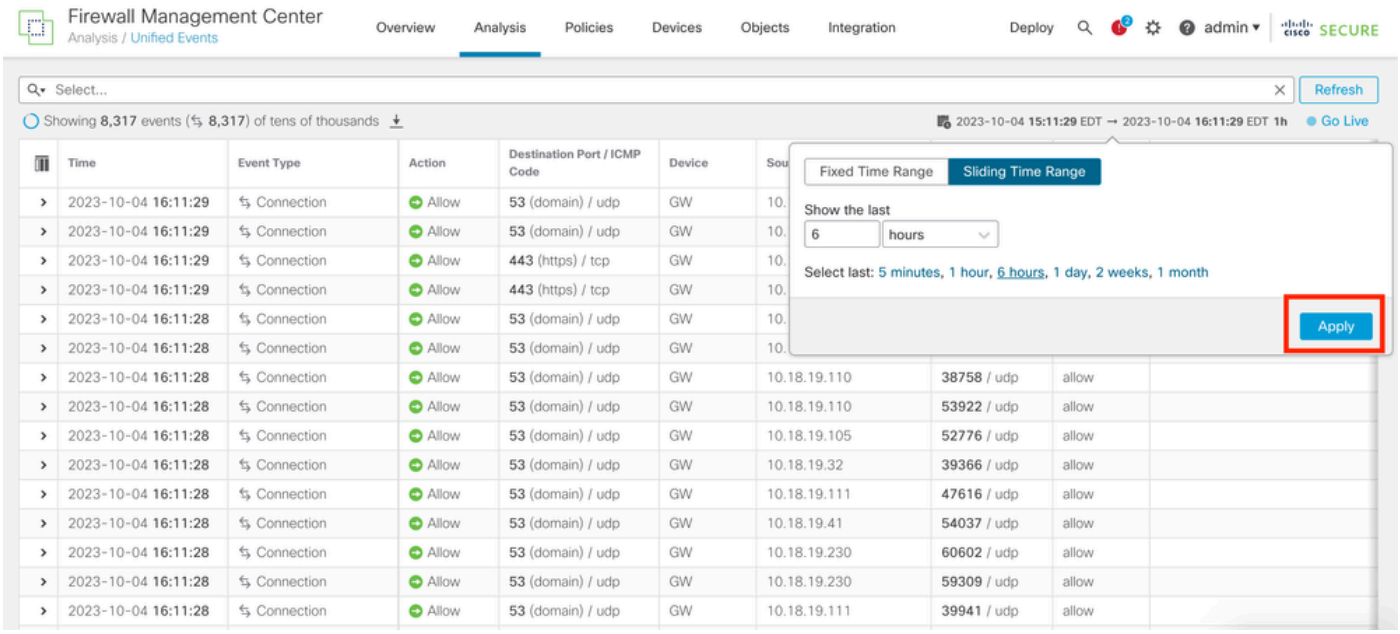
الخطوة 2. حدد نطاق الوقت في النافذة المنبثقة.



الخطوة 3. (إختياري) أستخدم نطاق زمني منزلق لعرض الأحداث من وقت معين إلى وقتك الحالي.



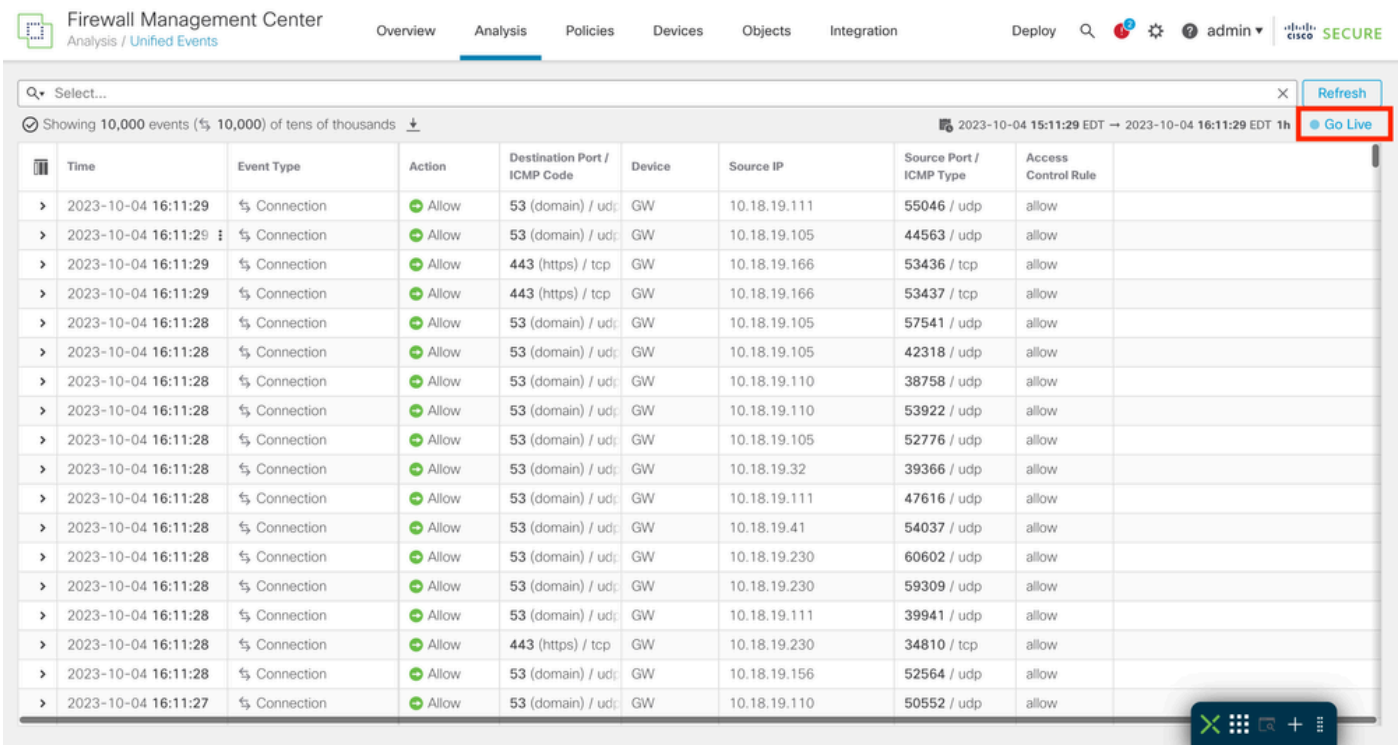
الخطوة 4. انقر فوق تطبيق لتصفية الأحداث الموجودة على النطاق الزمني الذي تم تكوينه.



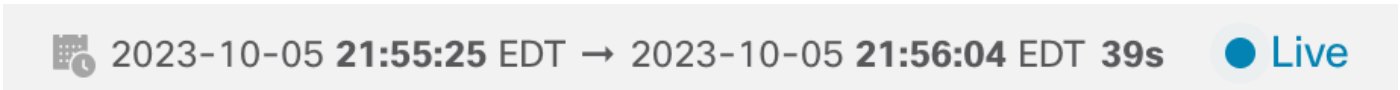
جو لايف

يمكنك تمكين ميزة Go Live لعرض الأحداث في الوقت الفعلي. تظهر الأحداث كما يتم توليدها.

للتمكين، انقر فوق Go Live.



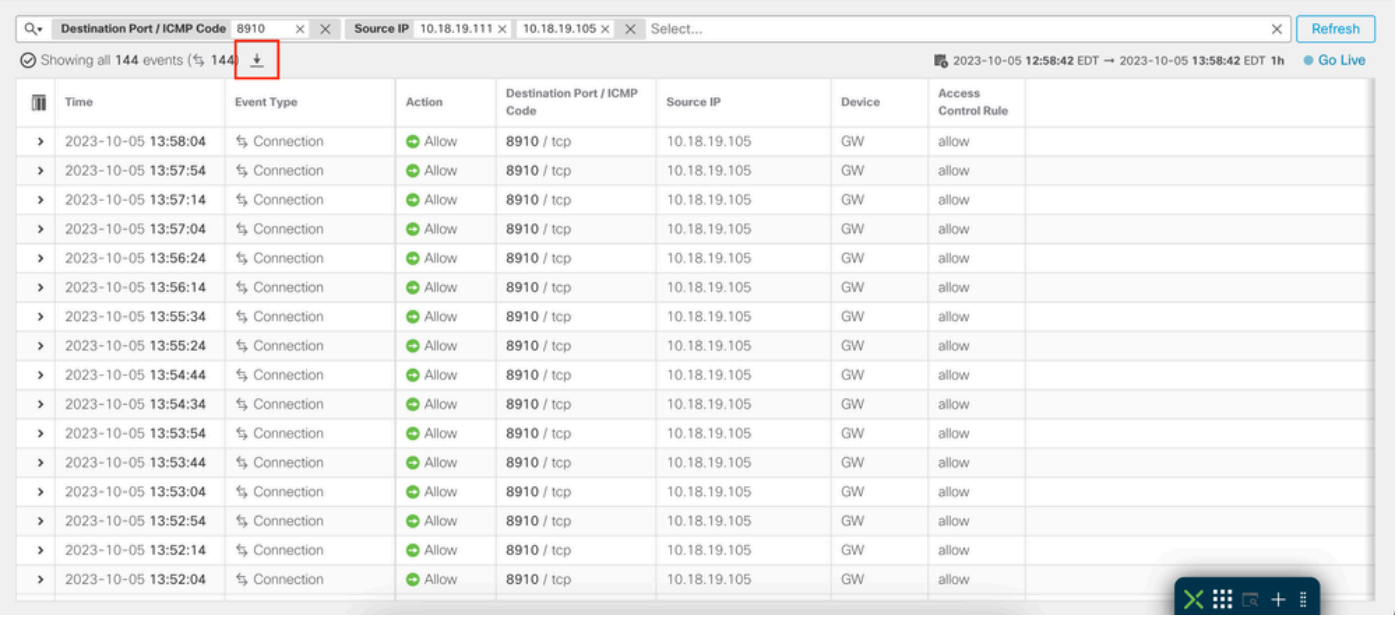
وبمجرد تمكينها، فإنها تعرض كلمة Live.



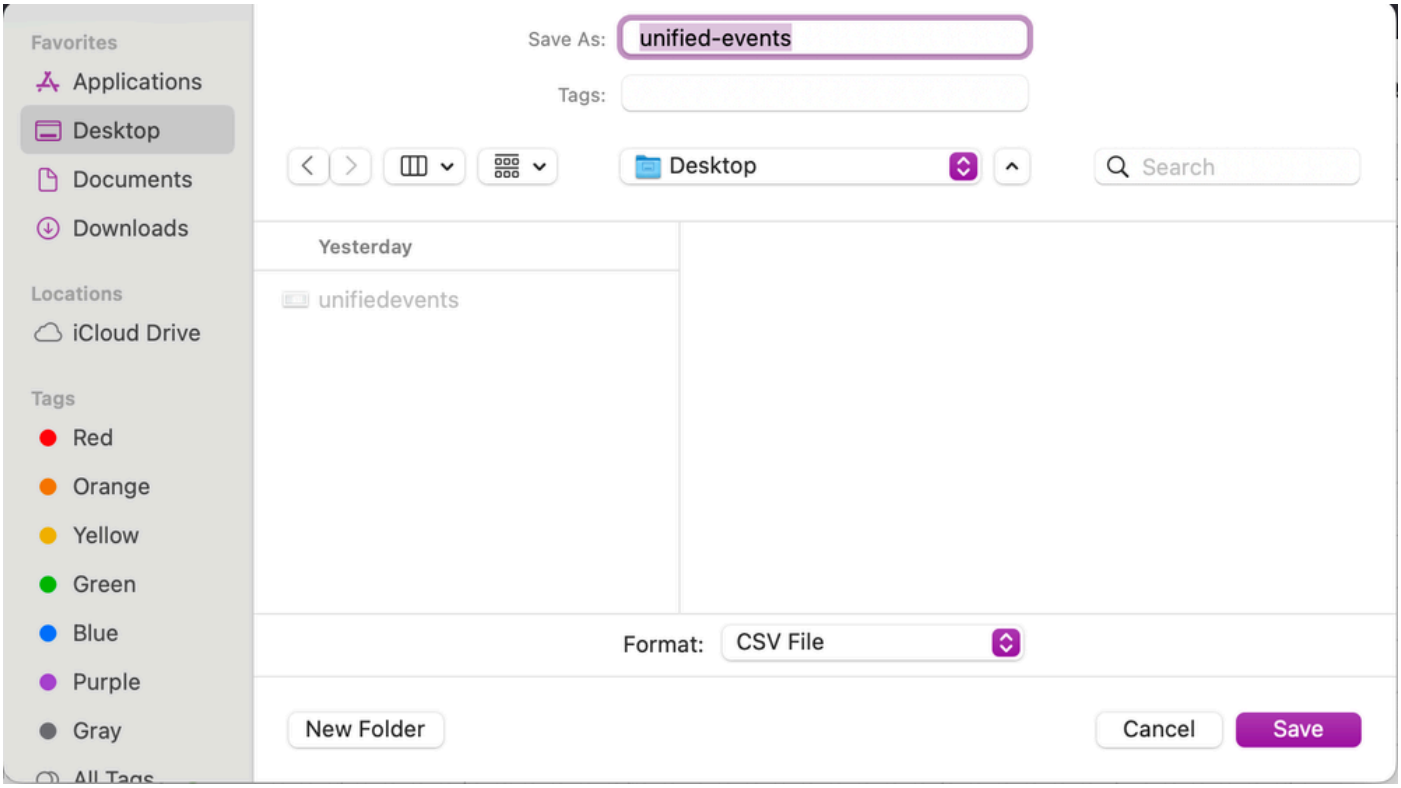
⚠ تحذير: عند تمكين Live، لا يمكن تعديل الإطار الزمني. لتعديل الإطار الزمني، قم أولا بتعطيل خيار Live بالنقر عليه مرة أخرى.

تنزيل الأحداث باسم قيم مفصولة بفاصلة (CSV)

الخطوة 1. انقر فوق رمز التنزيل لإنشاء ملف يحتوي على الأحداث المعروضة حاليا على الصفحة.



الخطوة 2. حدد مجلد التنزيل والاسم وانقر على حفظ.



الخطوة 3. تحقق من ملف CSV.

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	37412 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	54766 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.166	54279 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	55185 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	46312 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	36785 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	57394 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	57395 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	38278 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44865 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	58387 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	49873 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	51060 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	34103 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.31	60020 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	43410 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47406 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	43359 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	43336 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	42658 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52923 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	46485 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.201	52178 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55864 / udp	allow

معلومات ذات صلة

- العمل مع عارض الأحداث الموحد
- Cisco Secure Firewall - عارض الأحداث الموحدة: النصائح والحيل
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).