ىلثملا ةرابعلا ديدحت ءاطخأ فاشكتسأ ليلد اهحالصإو AnyConnect نم

المحتويات

<u>المقدمة</u> كيف تعمل شركة OGS؟ ذاكرة التخزين المؤقت OGS تحديد الموقع <u>سيناريوهات الفشل</u> عند فقد الاتصال بالبوابة الاستئناف بعد الإيقاف المؤقت يحدد حجم نافذة TCP المؤجلة-ACK بوابة غير صحيحة مثال نموذجي للمستخدم أستكشاف أخطاء OGS وإصلاحها <u>الخطوة 1. مسح ذاكرة التخزين المؤقت OGS لإجبار إعادة التقييم</u> الخطوة 2. التقاط مستكشفات الخادم أثناء محاولة الاتصال الخطوة 3. التحقق من البوابة المحددة من قبل OGS الخطوة 4. التحقق من صحة حسابات OGS التي يتم تشغيلها بواسطة AnyConnect تحليل أسئلة وأجوبة

المقدمة

يصف هذا المستند كيفية أستكشاف أخطاء تحديد العبارة (OGS) الأمثل وإصلاحها. OGS هي ميزة يمكن إستخدامها لتحديد البوابة التي تحتوي على أقل وقت لرحلة ذهاب وإياب (RTT) والتوصيل بهذه البوابة. ويمكن إستخدام ميزة OGS لتقليل زمن الوصول لحركة مرور الإنترنت دون تدخل من المستخدم. باستخدام OGS، يحدد Cisco AnyConnect Secure Mobility Client (AnyConnect (AnyConnect Secure Mobility Client (AnyConnect هذه البوابة. تبدأ OGS عند التوصيل الأول أو عند إعادة التوصيل بعد أربع ساعات على الأقل من الانفصال السابق. يمكن العثور على مزيد من المعلومات ف<u>ي دليل المسؤول</u>.

تلميح: يعمل OGS بشكل أفضل مع أحدث عميل AnyConnect وبرنامج ASA الإصدار 3)9.1)<u>*</u> أو إصدار أحدث.

کیف تعمل شرکة OGS؟

لا يعمل طلب **إختبار الاتصال** لبروتوكول رسائل التحكم في الإنترنت (ICMP) البسيط لأنه تم تكوين العديد من جدران حماية جهاز الأمان القابل للتكيف (ASA) من Cisco لحظر حزم ICMP لمنع الاكتشاف. بدلا من ذلك، يرسل العميل ثلاثة طلبات HTTP/443 إلى كل وحدة توصيل تظهر في **دمج** لكل ملفات التعريف. وتتم الإشارة إلى مستكشفات HTTP هذه باسم إختبارات OGS في السجلات، ولكنها، كما هو موضح مسبقا، ليست إختبارات اتصال ICMP. لضمان ألا يستغرق الاتصال (re)وقتا طويلا جدا، يقوم OGS بتحديد البوابة السابقة بشكل افتراضي إذا لم تستلم أي نتائج إختبار اتصال OGS في غضون سبع ثوان. (ابحث عن **نتائج إختبار اتصال OGS** في السجل.)

ملاحظة: يجب أن يرسل AnyConnect طلب HTTP إلى رقم 443، لأن الاستجابة نفسها مهمة، وليست

إستجابة ناجحة. لسوء الحظ، يرسل إصلاح معالجة الوكيل جميع الطلبات ك HTTPS. راجع معرف تصحيح الأخطاء من Cisco <u>CSCtg38672</u> - يجب أن يتم إختبار اتصال OGS بطلبات HTTP.

ملاحظة: في حالة عدم وجود أي نهايات توصيل في ذاكرة التخزين المؤقت، يرسل AnyConnect أولا طلب HTTP لتحديد ما إذا كان هناك وكيل مصادقة، وما إذا كان يمكنه معالجة الطلب. فقط بعد هذا الطلب الأولي أن يبدأ OGS إختبار من أجل أستكشاف الخادم.

تحدد OGS موقع المستخدم استنادا إلى معلومات الشبكة، مثل اللاحقة الخاصة بنظام اسم المجال (DNS) • وعنوان IP لخادم DNS. يتم تخزين نتائج RTT، مع هذا الموقع، في ذاكرة التخزين المؤقت OGS.

يتم تخزين إدخالات موقع OGS مؤقتا لمدة 14 يوما. تم تصنيف معرف تصحيح الأخطاء من Cisco • <u>CSCtk66531</u> لجعل هذه الإعدادات قابلة للتكوين من قبل المستخدم.

• لا يتم تشغيل OGS مرة أخرى من هذا الموقع حتى 14 يوما بعد تخزين إدخال الموقع مؤقتا لأول مرة. خلال هذا الوقت، يتم إستخدام الإدخال المخزن مؤقتا ووحدات RTT المحددة لذلك الموقع. وهذا يعني أنه عندما يبدأ AnyConnect مرة أخرى، فإنه لا يقوم بتنفيذ OGS مرة أخرى، وبدلا من ذلك، فإنه يستخدم ترتيب العبارة الأمثل في ذاكرة التخزين المؤقت لذلك الموقع. في سجلات أداة تقارير AnyConnect (DART) التشخيصية، يتم عرض هذه الرسالة:

> > *****

• يتم تحديد RTT باستخدام تبادل TCP إلى منفذ طبقة مآخذ التوصيل الآمنة (SSL) من البوابة التي سيحاول المستخدم الاتصال بها كما هو محدد بواسطة إدخال المضيف في ملف تعريف AnyConnect.

ملاحظة: على عكس إختبار اتصال HTTP، الذي يقوم بنشر HTTP بسيط ثم يعرض RTT والنتيجة، فإن عمليات حساب OGS أكثر تعقيدا بقليل. يرسل AnyConnect ثلاثة مستكشفات لكل خادم، ويحسب التأخير بين HTTP syn الذي يرسله و FIN/ACK لكل من هذه المستكشفات. ومن ثم، فإنه يستخدم أدنى الخوادم من أجل مقارنة الخوادم وتحديد موقعها. لذلك، على الرغم من أن إختبارات إختبارات HTTP تعد مؤشرا جيدا إلى أي خادم سيختاره AnyConnect، إلا أنها قد لا تكون بالضرورة متطابقة. وهناك المزيد من المعلومات حول هذا الأمر في باقى المستند.

حاليا، يقوم OGS فقط بتشغيل التحققات إذا خرج المستخدم من الإيقاف المؤقت، وتم تجاوز الحد. لا تتصل • OGS ب ASA مختلف إذا كان المستخدم متصلا بتعطل أو أصبح غير متاح. يتصل OGS فقط بالخوادم الأساسية في التوصيف لتحديد الخادم الأمثل.

بمجرد تنزيل ملف تعريف عميل OGS، عندما يقوم المستخدم بإعادة تشغيل عميل AnyConnect، سيتم تصنيف خيار تحديد ملفات التعريف الأخرى كما هو موضح هنا:

S Cisco AnyCor	nect Secure Mobility Client	
	VPN: Please enter your username and password. Automatic Selection	Connect
\$ ()		altaba

حتى إذا كان لجهاز المستخدم ملفات تعريف أخرى متعددة، فلن يتمكن من تحديد أي منها حتى يتم تعطيل OGS.

ذاكرة التخزين المؤقت OGS

بمجرد انتهاء عملية الحساب، يتم تخزين النتائج في الملف preferences_global. هناك مشاكل في هذه البيانات التي لم يتم تخزينها في الملف السابق.

راجع معرف تصحيح الأخطاء من Cisco <u>CSCtj84626</u> للحصول على مزيد من التفاصيل.

تحديد الموقع

يعمل التخزين المؤقت ل OGS على مجموعة من مجال DNS وعناوين IP الخاصة بخادم DNS. وتعمل على النحو التالي:

- يحتوي الموقع A على مجال DNS ل **locationa.com**، وعنوان IP لخادم DNS **IP1** وDNS. تقوم كل مجموعة مجال/IP بإنشاء مفتاح تخزين مؤقت يشير إلى إدخال ذاكرة تخزين مؤقت OGS. على سبيل المثال: locationa.com|ip1 -> ogscache1locationa.com|ip2 -> ogscache1
 - إذا كان AnyConnect يتصل بعد ذلك بشبكة مختلفة ماديا، يتم إنشاء نفس عملية إنشاء مجموعات المجال/IP وفحصها مقابل القائمة المخزنة مؤقتا. في حالة وجود أي تطابقات على الإطلاق، يتم إستخدام قيمة ذاكرة التخزين المؤقت OGS، ولا يزال العميل يعتبر في **الموقع A**.

سيناريوهات الفشل

فيما يلي بعض سيناريوهات الفشل التي قد يواجهها المستخدمون:

عند فقد الاتصال بالبوابة

عند إستخدام OGS، في حالة فقد الاتصال بالبوابة التي يتصل بها المستخدمون، يتصل AnyConnect بالخوادم الموجودة في **قائمة ملقمات النسخ الاحتياطيوليس** إلى مضيف OGS التالي. وترتيب العمليات هو كما يلي:

ولا يتصل OGS إلا بالخوادم الأساسية لتحديد الخادم الأمثل.

2. وبمجرد تحديدها، تكون خوارزمية الاتصال كما يلي: حاول الاتصال بالخادم الأمثل.إذا فشل ذلك، فجرب قائمة خادم النسخ الاحتياطي الأمثل للخادم.إذا فشل ذلك، جرب كل خادم باق في قائمة تحديد OGS، حسب نتائج التحديد الخاصة به.

.1

ملاحظة: عندما يقوم المسؤول بتكوين قائمة خادم النسخ الاحتياطي، يسمح محرر ملف التعريف الحالي للمسؤول بإدخال اسم المجال المؤهل بالكامل (FQDN) لخادم النسخ الاحتياطي فقط، ولكن ليس لمجموعة المستخدمين كما هو ممكن للخادم الأساسي:

ctovpnoutbound6.cisco.com Group URL	/ ogs)	
Backup Server List		Load Balancing Server List "Always On" is disabled.	Load Balancing Fields have been disab
Host Address	Add	> Host Address	Add
	Move Up		Delete
	Move Down		
	Delete		
	(
Primary Protocol	SSL ÷	Automatic SCEP Host	
Auth Method During	KE Negotiation [KE-R \$]	Prompt For Challenge Pa	ssword
IKE Identity		CA Thumbprint	

تم تصنيف معرف تصحيح الأخطاء من Cisco <u>CSCud84778</u> لتصحيح هذا الأمر، ولكن يجب إدخال عنوان URL الكامل في حقل عنوان المضيف لخادم النسخ الاحتياطي، ويجب أن يعمل: **-https://<***ip*. address/userGroup.

الاستئناف بعد الإيقاف المؤقت

لكي يعمل OGS بعد السيرة الذاتية، يجب أن يكون لدى AnyConnect اتصال تم إنشاؤه عند وضع الجهاز في وضع السكون. يتم إجراء OGS بعد إستئناف التشغيل فقط بعد إجراء إختبار بيئة الشبكة، والذي يقصد به تأكيد توفر اتصال الشبكة. يتضمن هذا الاختبار الاختبار الفرعي لاتصال DNS.

ومع ذلك، إذا قام خادم DNS باسقاط النوع A من الطلبات التي تحمل عنوان IP في حقل الاستعلام، بدلا من الرد باستخدام "لم يتم العثور على الأسم" (الحالة الأكثر شيوعا، والتي تتم مواجهتها دائما أثناء الاختبارات)، فحينئذ معرف تصحيح الأخطاء من Cisco <u>CSCti20768</u> ينطبق "استعلام DNS من النوع A لعنوان IP، يجب أن يكون PTR لتجنب المهلة".

يحدد حجم نافذة TCP المؤجلة-ACK بوابة غير صحيحة

عند إستخدام إصدارات ASA الأقدم من الإصدار 9.1(3)، تظهر عمليات الالتقاط على العميل تأخيرا مستمرا في مصافحة SSL. ما يتم ملاحظته هو أن العميل يرسل ClientHello الخاص به، ثم يرسل ASA ServerHello الخاص به. وعادة ما تتبع ذلك رسالة شهادة (طلب شهادة إختياري) ورسالة ServerHelloDone. ويتلخص هذا الشذوذ في شقين:

لا يقوم ASA بإرسال رسالة الشهادة على الفور بعد ServerHello. حجم نافذة العميل هو 64،860 بايت، وهو أكثر من كاف للاحتفاظ باستجابة ASA بالكامل.

2. لا يقوم العميل بوضع ServerHello في الحال، لذلك يقوم ASA بإعادة إرسال ServerHello بعد حوالي 120

مللي ثانية، وفي هذه النقطة يقوم العميل بوضع البيانات في ذاكرة الوصول الفوري. ثم يتم إرسال رسالة الشهادة. ويكاد الأمر يبدو وكأن العميل ينتظر المزيد من البيانات.

يحدث هذا بسبب التفاعل بين <u>TCP بطيء البدء</u> و<u>TCP مؤجل-ACK</u>. قبل الإصدار 3)(3) من ASA، يستخدم ASA حجم نافذة بدء بطيء بقيمة 1، في حين يستخدم عميل Windows قيمة ACK متأخرة مقدارها 2. وهذا يعني أن ASA يرسل حزمة بيانات واحدة فقط إلى أن يحصل على ACK، ولكنه يعني أيضا أن العميل لا يرسل ACK حتى يستلم حزمتي بيانات. يعرض ASA الأمر بعد 120 مللي ثانية ويعيد إرسال ServerHello، وبعد ذلك يقوم العميل بسرد البيانات واستمرار الاتصال. تم تغيير هذا السلوك بواسطة معرف تصحيح الأخطاء من Cisco <u>CSCug98113</u> حتى يستخدم ASA

يمكن أن يؤثر ذلك على حساب OGS عندما:

• تعمل البوابات المختلفة على تشغيل إصدارات ASA المختلفة.

• لدى العملاء أحجام إطارات Delayed-Ack مختلفة.

وفي مثل هذه الحالات، قد يكون التأخير الذي يحدثه نظام الحجز الآلي المتأخر كافيا لجعل العميل يختار نظام الحجز المؤقت غير الصحيح. إذا كانت هذه القيمة تختلف بين العميل و ASA، فقد تكون هناك مشاكل. في مثل هذه الحالات، يكون الحل البديل هو ضبط حجم نافذة الإقرارات المؤجلة.

ويندوز

السجل.	محرر	تشغيل	بدء
--------	------	-------	-----

.2	ى بالقارن الذي تريد تعطيل ACK المؤجل عليه. للقيام بذلك، انتقل إلى: Microsoft > WindowsNT > CurrentVersion > حبرنامج > KKEY	حدد GUID الخاص CAL_MACHINE
هة (على الفريد	(رقم). ; تحت بطاقات NetworkCards. على الجانب الأيمن، يجب أن يسرد الوصف الواج (Intel(R) Wireless WiFi Link 5100) ويجب أن يسرد ServiceName المعرف المقابل.	NetworkCards راجع کل رقم مدرج مسبیل المثال، AGN العمومي (GUID) ا
•		

.1

.5

.6

حدد موقع مفتاح التسجيل الفرعي هذا ثم انقر فوقه: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interface s\<interface GUID>

في قائمة تحرير، أشر إلى جديد، ثم انقر **قيمة DWORD**. 4

قم بتسمية القيمة الجديدة TcpAckFrequency، وقم بتعيينها بقيمة 1.

إنهاء محرر السجل.

7. قم بإعادة تشغيل Windows حتى يصبح هذا التغيير نافذ المفعول.

ملاحظة: تم تصنيف معرف تصحيح الأخطاء من Cisco <u>CSCum19065</u> لجعل معلمات ضبط TCP قابلة للتكوين على ASA.

مثال نموذجي للمستخدم

أكثر حالات الاستخدام شيوعا هي عندما يقوم المستخدم في المنزل بتشغيل OGS في المرة الأولى، فإنه يسجل إعدادات DNS وينتج إختبار اتصال OGS في ذاكرة التخزين المؤقت (الإعداد الافتراضي هو مهلة 14 يوما). عندما يعود المستخدم إلى المنزل في المساء التالي، يكتشف OGS نفس إعدادات DNS، ويعثر عليها في ذاكرة التخزين المؤقت، ويتخطى إختبار إختبار إختبار OGS. وفي وقت لاحق، عندما يذهب المستخدم إلى فندق أو مطعم يقدم خدمة الإنترنت، يكتشف OGS إعدادات DNS مختلفة، ويقوم بتشغيل إختبارات إختبار OGS، ويحدد أفضل بوابة، ويسجل النتائج في ذاكرة التخزين المؤقت.

تكون المعالجة متطابقة عند إستئنافها من حالة الإيقاف المؤقت أو الإسبات، إذا كانت إعدادات إستئناف OGS و

أستكشاف أخطاء OGS وإصلاحها

الخطوة 1. مسح ذاكرة التخزين المؤقت OGS لإجبار إعادة التقييم

من أجل مسح ذاكرة التخزين المؤقت ل OGS وإعادة تقييم RTT للبوابات المتاحة، ما عليك سوى حذف ملف تفضيلات AnyConnect العام من الكمبيوتر الشخصي. يختلف موقع الملف باختلاف نظام التشغيل:

• Windows Vista و Windows 7

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\preferences_global.xml Note: in older client versions it used to be stored in C:\ProgramData\Cisco\Cisco AnyConnect VPN Client

• ويندوز إكس بي

C:\Documents and Settings\AllUsers\Application Data\Cisco\Cisco AnyConnect VPN Client\preferences_global.xml

• ماك أو إس إكس

opt/cisco/anyconnect/.anyconnect_global/ ..Note: with older versions of the client it used to be /opt/cisco/vpn

• لينكس

opt/cisco/anyconnect/.anyconnect_global/
..Note: with older versions of the client it used to be /opt/cisco/vpn

الخطوة 2. التقاط مستكشفات الخادم أثناء محاولة الاتصال

بدء محاولة اتصال على AnyConnect.

3. أوقف التقاط Wireshark بمجرد اكتمال الاتصال. **تلميح**: نظرا لأن الالتقاط يتم إستخدامه فقط لاختبار OGS، فمن الأفضل إيقاف الالتقاط بمجرد أن يحدد AnyConnect بوابة. من الأفضل عدم المرور عبر محاولة اتصال كاملة، لأن ذلك يمكن أن يؤدي إلى إعتام التقاط الحزمة.

الخطوة 3. التحقق من البوابة المحددة من قبل OGS

للتحقق من سبب تحديد OGS لبوابة معينة، أكمل الخطوات التالية:

بدء توصيل جديد.

2. تشغيل DART ل AnyConnect:

قم بتشغيل AnyConnect، وانقر فوق **خيارات متقدمة**.انقر فوق **التشخيص**.انقر فوق **التالي)**.انقر فوق Next (التالي). اختبر نتائج DART الموجودة في ملف DartBundle_XXXX_XXzip الذي تم إنشاؤه حديثا على سطح 3. المكتب. انتقل إلى Cisco AnyConnect Secure Mobility Client > AnyConnect.txt.

.1

.2

.1

لاحظ الوقت الذي بدأت فيه إختبارات OGS لخادم معين من سجل DART هذا:

Date : 10/04/2013 Time : 14:21:27 Type : Information Source : acvpnui Description : Function: CHeadendSelection::CSelectionThread::Run File: .\AHS\HeadendSelection.cpp Line: 928 OGS starting thread named gw2.cisco.com

عادة يجب أن تكون حول نفس الوقت، ولكن في حالة أن تكون عمليات الالتقاط كبيرة، فإن الطابع الزمني يساعد على تضييق الحزم التي هي مستكشفات HTTP وتلك التي هي محاولات الاتصال الفعلية.

بمجرد أن يرسل AnyConnect ثلاثة مستكشفات إلى الخادم، يتم إنشاء هذه الرسالة باستخدام النتائج لكل تجربة:

Date : 10/04/2013 Time : 14:31:37 Type : Information Source : acvpnui

Description : Function: CHeadendSelection::CSelectionThread::logThreadPingResults File: .\AHS\HeadendSelection.cpp Line: 1137 (OGS ping results for gw2.cisco.com: (219 218 132

من المهم أن تنتبه إلى هذه القيم الثلاث، لأنها يجب أن تطابق نتائج الالتقاط.

ابحث عن الرسالة التي تحتوي على "*** نتائج تحديد OGS**" لعرض RTT الذي تم تقييمه، وإذا كانت أحدث محاولة اتصال هي نتيجة RTT الذي تم تخزينه مؤقتا أو نتيجة حساب جديد.

qw2.cisco.com

فيما يلي مثال: Date : 10/04/2013 : 12:29:38 Time Type : Information Source : vpnui Description : Function: CHeadendSelection::logPingResults File: .\AHS\HeadendSelection.cpp Line: 589 *** OGS Selection Results *** 'OGS performed for connection attempt. Last server: 'gw2.cisco.com .Results obtained from OGS cache. No ping tests were performed (Server Address RTT (ms qwl.cisco.com 302

132 <======= As seen, 132 was the lowest delay

of the three probes from the previous DART log gw3.cisco.com 506 gw4.cisco.com 877 .Selected 'gw2.cisco.com' as the optimal server

الخطوة 4. التحقق من صحة حسابات OGS التي يتم تشغيلها بواسطة AnyConnect

فحص الالتقاط لاستكشافات TCP/SSL المستخدمة لحساب RTT. راجع المدة التي يستغرقها طلب HTTPS على اتصال TCP واحد. يجب أن يستخدم كل طلب تحقيق اتصال TCP مختلف. للقيام بذلك، افتح الالتقاط في Wireshark، وكرر الخطوات التالية لكل خادم:

أستخدم عامل تصفية ip.addr لعزل الحزم المرسلة إلى كل خادم في الالتقاط الخاص بها. للقيام بذلك، انتقل1. إلى **تحرير**، وحدد **وضع علامة على جميع الحزم المعروضة**. ثم انتقل إلى **ملف > حفظ باسم**، وحدد خيار **الحزم المميزة فقط**، وانقر فوق **حفظ**:



في هذا الالتقاط الجديد، انتقل إلى **عرض > تنسيق عرض الوقت > التاريخ والوقت من اليوم**:

.2

● ○ ○ \\ \\ \C27454747.pcaprg. (Wireshark 1.6.2 GVN Rev 38931 from /trunk=1.6()					
Eile Edit	View Go Capture Analyze Stat	istics Telephon	w Iools Internals Help		
EX 84 8	 Main Toolbar 		🛶 🔻 🛓 🔲 🗐 ାର୍ ର୍ ର୍ 🕐 📓 📓 🐒	100	
	 ✓ Eilter Toolbar 				
riter: ip.	< <u>S</u> tatusbar		pression Clear Apply		
No.	< Packet List		Protocol Length Info		
677	Packet Details		CP 62 4542 > https: [SYN] Segr0 Vbrv65525 Lerv0 MSS+1 (2) https://www.syn.ex.doi.org/10.1001/10.1001/00.0000000000000000000	1460 SHOL_PERM	
660	 Packet Bytes 		CP 54 4542 > https://www.index.add/.add/.add/.add/.add/.add/.add/.add)	
650	Time Display Format		Data and Time of Dev: 1970-01-01 01-02-08 128456	Orlanda	
709	Name Besolution		Time of Day: 01:02:03 123456	Otrl+At+2	
710	< Colorize Packet List	-	 Seconds Since Epoch (1970-01-01): 1234567890.123456 	Ctrl+At+3	
711	< Auto Scroll in Live Capture		Seconds Since Beginning of Capture: 123.123456	Ctrl+AE+4	
729			Seconds Since Previous Captured Packet: 1.123456	Ctrl+At+5	
730	is ∠oom in	Ctrl++	Seconds Since Previous Displayed Packet: 1.123456	Ctrl+Alt+6	
732	C. Nacroal Size	Orl+-	Automatic (Ella Careat Pracisian).		
•	Resize All Columns	Shift + Christelle	Seconds: 0		· · · · · · · · · · · · · · · · · · ·
Frame 67	Displayed Columns	arm + curr+k	Deciseronds: 0.1		
P Ethermet	D Obrahea Caronina		Centiseconds: 0.12		
P Transmis	Expand Subtrees	Shift+Right	Milliseconds: 0.123	I	
	Expand All	Ctrl+Right	Microseconds: 0.123456		
	Collapse All	Ctrl+Left	Nanoseconds: 0.123456789		
	Colorize Conversation	•	Display Seconds with hours and minutes	Orleand	
	Reset Coloring 1-10	Ctrl+Space	orspray beconds with mours and minutes	CONTRACTO	
	Scoloring Rules				
	Show Packet in New Window				
	S Beload	Ctrl+R			
0000 00 24	14 9b 30 e5 10 de f1 12 c5 e9 00 fd 1d 40 00 80 05 00 00 0a 0a 0a	004500 .\$. 9ec15e .0.	.0E.		
0020 84 br	11 be 01 bb 80 41 20 96 00 00 00 66 00 00 00 02 04 05 b4 01 01 03	00 70 02			
Eile: */L	sers/atbasu/Desktop/X-Files/6274	194747 Par	kets: 1538 Displayed: 61 Marked: 61 Load time: 0:10 992		Profile: Default

حدد حزمة HTTP syn الأولى في هذا الالتقاط الذي تم إرساله عندما تم إرسال تحقيق OGS استنادا إلى 3. سجلات DART كما هو محدد في الخطوة 3.3.2. من المهم تذكر أن أول طلب HTTP، بالنسبة للخادم الأول، ليس تحقيق خادم. من السهل أن نخطئ في أول طلب لاستقصاء خادم، وبالتالي فإننا نتوصل إلى قيم مختلفة تماما عما يقدمه OGS من تقارير. ويتم إبراز هذه المشكلة هنا:

677 2013-10-07 11:51:03.040834 10.10.0.154		193:019:0k02v288a	TCP	62 4542 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
689 2013-10-07 11:51:03.164885 10.10.0.154	Test HTTP Connection	101-01-01-02-02-02-02-02-02-02-02-02-02-02-02-02-	TCP	54 4542 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
690 2013-10-07 11:51:03.165061 10.10.0.154		191710-112-108	SSL	167 Continuation Data
710 2013-10-07 11:51:03.286837 10.10.0.154		1930130/252/3884	TCP	54 4542 > https [ACK] Seg=114 Ack=2 Win=65535 Len=0
711 2013-10-07 11:51:03.288937 10.10.0.154		23931-12301-232-128883a	TCP	54 4542 > https [FIN, ACK] Seg=114 Ack=2 Win=65535 Len=0
713 2013-10-07 11:51:03.297522 10.10.0.154		1911101132198	TCP	62 4543 > https [SYN] Seg=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
732 2013-10-07 11:51:03,424015 10,10,0,154		19302300282v288a	TCP	54 4543 > https [ACK] Seg=1 Ack=1 Win=65535 Len=0
734 2013-10-07 11:51:03.424384 10.10.0.154		193-1190-137-1881a	TLSv1	131 Client Hello
762 2013-10-07 11:51:03.552735 10.10.0.154	OGS Text 1	193710.137198	TCP	54 4543 > https [ACK] Seg=78 Ack=1486 Win=65535 Len=0
763 2013-10-07 11:51:03.553816 10.10.0.154		19301380/18201884	TLSv1	368 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess
779 2013-10-07 11:51:03.747197 10.10.0.154		2931/2360/232/23860	TLSV1	192 Application Data
792 2013-10-07 11:51:03.874861 10.10.0.154		199719971379188	TCP	54 4543 > https [ACK] Seg=530 Ack=1850 win=65172 Len=0
793 2013-10-07 11:51:03.876186 10.10.0.154		103:110:133:588:0	TCP	54 4543 > https [FIN, ACK] Seg=530 Ack=1850 Win=65172 Len=0
794 2013-10-07 11:51:03.877037 10.10.0.154		193-110-0682-188-1-	TCP	62 lanner-lm > https [51N] Seg=0 Win=65535 Len=0 MSS=1460 SACK_PERM
809 2013-10-07 11:51:04.001356 10.10.0.154		109/110/199/1988	TCP	54 lanner-lm > https [ACK] Seg=1 Ack=1 Win=65535 Len=0
810 2013-10-07 11:51:04.001693 10.10.0.154		193003945245245888	TLSV1	163 Client Hello
827 2013-10-07 11:51:04.127077 10.10.0.154	OGS Test 2	statues and a second seco	TLSv1	101 Change Cipher Spec, Encrypted Handshake Message
828 2013-10-07 11:51:04.129515 10.10.0.154		191110:112:108	TLSv1	192 Application Data
844 2013-10-07 11:51:04.254843 10.10.0.154		191013901304080	TCP	54 lanner-lm > https [ACK] Seg=295 Ack=444 Win=65093 Len=0
845 2013-10-07 11:51:04.254860 10.10.0.154		191-036-032-0884	TCP	54 lanner-lm > https (FIN, ACK) Seq=295 Ack=444 Win=65093 Len=0
846 2013-10-07 11:51:04.255775 10.10.0.154		100/10/0/10/100	TCP	62 ods-adppiw-db > https [SYN] Seg=0 Win=65535 Len=0 MSS=1460 SACK_F
856 2013-10-07 11:51:04.382426 10.10.0.154		1984130:132:088=	TCP	54 ods-adpoiw-db > https [ACK] Seg=1 Ack=1 Win=65535 Len=0
857 2013-10-07 11:51:04.382941 10.10.0.154		191-194-191-198-1	TLSv1	163 Client Hello
866 2013-10-07 11:51:04.510362 10.10.0.154	OSS Test 8	199.110.152.188	TLSv1	101 Change Cipher Spec, Encrypted Handshake Message
867 2013-10-07 11:51:04.512581 10.10.0.154		1930139018201884	TLSV1	192 Application Data
895 2013-10-07 11:51:04.639659 10.10.0.154		2931/2260/232/228844	TCP	54 ods-adopiw-db > https [ACK] Seg=295 Ack=444 Win=65093 Len=0
896 2013-10-07 11:51:04.640162 10.10.0.154		193 110 137 188	TCP	54 gds-adppiw-db > https [FIN, ACK] Seq=295 Ack=444 win=65093 Len=0

من أجل التعرف على كل من المستكشفات بسهولة أكبر، انقر بزر الماوس الأيمن فوق HTTP SYN للتحقيق4. الأول، ثم حدد **تلوين المحادثة** كما هو موضح هنا:



كرر هذه العملية ل SYNs على كل المستكشفات. كما هو موضح في الصورة السابقة، يصور المسابيران الاولان بألوان مختلفة. تتمثل ميزة تلوين محادثات TCP في تحديد نقاط إعادة الإرسال أو غيرها من هذه الروائح بسهولة لكل مسبار.

.5

لتغيير عرض الوقت، انتقل إلى **عرض > تنسيق عرض الوقت > ثوان منذ الحقبة**:

0 0 0					
Elle Edit 😢 en Go Capture Analyze Statistics Telephony Tools Internals Help					
EX 64 8	≺ <u>M</u> ain Toolbar				
_	< <u>F</u> ilter Toolbar				
Filter: ip.	< Statusbar	pression Clear Apply			
No.	< Packet List	Protocol Length Info			
677	- Packet Details	CP 62 4542 > https [SYN] Seq=0 VLr=65535 Ler=0 MSS=1460 SAOX_PERM=1			
669	< Packet Bytes	CP 62 https > 4542 LSYN, ACKI Seq=0 ACK=1 VLN=8192 Len=0 MSS=1360 CP 54 d542 > https [4CK] Seq=1 Ack=1 Kin=65535 Len=0	•		
690		61 bél continuation Cata			
708	Time Display Format	Date and Time of Day: 1970-01-01 01:02:03.123456 Ctrl+AR+1			
710	Colorine Dark et List	Time of Day: 01:02:05.123456 CD/1-AE+2			
711	< Auto Sepalities Line Conture	Seconds Since Epoch (1970-01-01): 1234567690(123456) C01+48+43 Seconds Since Evolution of Conture: 123.133455 Cold Ab 44			
729	· Auto scroll ill cige capcure	Seconds Since Beginning of Capture: 125.125456 Ctrit+Ak+4			
730	@ <u>Z</u> oom in Ctri++	Seconds Since Previous Capitaled Packet: 1.129456 Orl+Ak+6			
791	Q Zoom Qut Ctrl+-	Seconds and e memods of sprayed racket. 1:123450 Contracto	L L		
	Q Normal Size Ctr1+=	Automatic (File Format Precision)			
b Frame 67	E Resize All Columns Shift+Ctrl+R	Seconds: 0			
Ethernet	Displayed Columns	Deciseconds: 0.1			
Enternet Transmis	Expand Subtrees Shift+Right	Cerriteronatic 0.122			
	Expand All Ctrl+Right	Miniseconds: W123			
	Collapse All Ctrl+Left	Nanoseconds: 0.122456799			
	Colorize Conversation				
	Reset Colorino 1–10 Ctrl+Space	Display Seconds with hours and minutes Ctrl+At+D			
	S Coloring Rules				
	Show Packet in New Window				
	Eligan Colt-M				
0000 22 24	14 90 30 e6 10 de 11 12 c6 e9 08 00 45 00	.0E.			
0010 00 30 0020 94 bc	2010 00 30 74 14 40 00 80 06 00 00 04 00 00 94 01 66 0.0.9				
0030 ff ff	66 00 00 00 02 04 05 b4 01 01 04 02				
Ethernet	Detth) 14 hytes	kets: 1538 Displayed: 61 Marked: 0 Load time: 0:10 997	Profile: Default		

حدد **مللي ثانية**، لأن هذا هو مستوى الدقة الذي يستخدمه OGS.

6. حساب فرق الوقت بين نظام HTTP و FIN/ACK، كما هو موضح في الرسم التخطيطي للخطوة 4. كرر هذه العملية لكل من المسابير الثلاثة، وقارن القيم بتلك الموضحة في سجلات DART في الخطوة 3.3.3.

تحليل

إذا تم إحتساب قيم RTT المحددة بعد تحليل عمليات الالتقاط ومقارنتها بالقيم التي تم مشاهدتها في سجلات DART وتم العثور على كل شيء متطابق، ولكن لا يزال يبدو أنه يتم تحديد العبارة الخطأ، فهذا يرجع إلى واحدة من مشكلتين:

هناك مشكلة في وحدة الاستقبال والبث. إذا كان هذا هو الحال، فقد يكون هناك الكثير جدا من إعادة الإرسال • من رأس واحد معين، أو أي أشياء أخرى مماثلة ترى في التحقيقات. ويلزم إجراء تحليل أدق للتبادل.

∙ توجد مشكلة في موفر خدمة الإنترنت (ISP). إذا كان هذا هو الحال، فقد تظهر تجزئة أو تأخيرات كبيرة لمحطة الاستقبال والبث المحددة.

أسئلة وأجوبة

س: هل تعمل OGS مع موازنة الأحمال؟

أ: نعم. لا يعلم OGS إلا بالاسم الرئيسي لنظام المجموعة، ويستخدم ذلك للحكم على أقرب وحدة الاستقبال والبث.

س: هل يعمل OGS مع إعدادات الوكيل المحددة في المستعرض؟

A: لا يدعم OGS ملفات التكوين التلقائي للوكيل أو الوكيل التلقائي (PAC)، ولكنه يدعم خادم الوكيل الذي تم ترميزه بشكل ثابت. وعلى هذا النحو، لا تحدث عملية OGS. رسالة السجل ذات الصلة هي: **لن يتم تنفيذ OGS بسبب تكوين الكشف التلقائي للوكيل**.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما