Norton DNS هو أحد مكونات Norton Everywhere ، والذي سيمنحك في النهاية التحكم في المواقع التي قد يشاهدها العاملون أو أفراد عائلتك ، بالإضافة إلى القدرة على حظر الوصول إلى المواقع المعروفة بنقل المعلومات الضارة. لا تزال لوحة إدارة المستخدم غير متوفرة ، على الرغم من حقيقة أن الإصدار التجريبي من OpenDNS يقيد الوصول الضار إلى الموقع. ومع ذلك ، إذا كان شخص مجرم الإنترنت يحاول بدء هجوم ناجح للبرامج الضارة ، فسيتعين عليه إنشاء برنامج يعمل بنجاح ، وتشغيل عدد من جدران الحماية ، ثم إقناع المستخدم بفتح ملف لتشغيله أو التعمق في جهاز لبدء الفيروس. سرعان ما أدرك لصوص الإنترنت أنه كان من الأسهل العمل على الإنترنت: دع الأهداف تأتي إليهم.
قد لا تعرف ، ولكن وفقا لمايكروسوفت نفسها ، كانت الثغرات الأمنية المستندة إلى التطبيقات مسؤولة عن أكثر من 90٪ من جميع هجمات البرامج الضارة في عام 2008 ، في حين شكلت نقاط الضعف في برامج نظام التشغيل 6٪ فقط من جميع هجمات البرامج الضارة. يتمتع المجرمون بوصول أسهل إلى أجهزة الكمبيوتر المستهدفة بفضل تطبيقات مثل متصفحات الويب وبرامج المراسلة الفورية وأنظمة البريد الإلكتروني. يعد استخدام متصفح الويب لقيادة الضحية إلى موقع مصاب إحدى الطرق التي يمكن لمجرمي الإنترنت من خلالها تعريض أجهزة الكمبيوتر الخاصة بهم لهجوم. يمكن أن يكون موقع الويب هذا شرعيا ، أو قد يكون تصيد احتيالي ، وهو عندما يتم تصميم موقع ليبدو مطابقا تقريبا لموقع شركة شرعية وجديرة بالثقة.

فهم نظام أسماء النطاقات من Norton

نظام اسم المجال (DNS) هو دليل هاتف الإنترنت. يستخدم البشر أسماء النطاقات ، مثل nytimes.com أو espn.com ، للوصول إلى المحتوى عبر الإنترنت. تتواصل متصفحات الويب عبر عناوين بروتوكول الإنترنت (IP). يقوم DNS بتحويل أسماء النطاقات إلى عناوين IP حتى تتمكن المتصفحات من الوصول إلى موارد الإنترنت.
يحتوي كل جهاز متصل بالإنترنت على عنوان IP فريد قد تستخدمه الأجهزة الأخرى لتحديد موقع الجهاز. تقلل خوادم DNS من متطلبات البشر لتذكر عناوين IP مثل 192.168.1.1 (في IPv4) أو عناوين IP الأبجدية الرقمية الحديثة الأكثر تعقيدا مثل 2400: :: 1 :2048 :cb00 c629: d7a2 (في IPv6).

شرح عمل DNS

تحليل DNS هو طريقة أو عملية تحويل اسم مضيف (على سبيل المثال www.example.com) إلى عنوان IP متوافق مع الكمبيوتر (مثل 192.168.1.1). يتم تعيين عنوان IP لكل جهاز على الإنترنت ، وهذا العنوان مطلوب لتحديد موقع جهاز الإنترنت المناسب ، تماما كما يتم استخدام عنوان الشارع لتحديد موقع سكن معين. عندما يطلب المستخدم صفحة ويب، يجب أن تتم الترجمة بين ما يضعه المستخدم في متصفح الويب الخاص به (example.com) والعنوان المناسب للآلة المطلوب للوصول إلى صفحة الويب example.com.

Norton DNS - فهم التشريح

Norton DNS هي خدمة تتيح التصفح عبر الإنترنت بشكل أسرع وأكثر موثوقية مع توفير الحماية الأساسية. لا يستلزم استخدام العميل. يمكنك استخدام Norton DNS على أجهزة الكمبيوتر الفردية أو تمكين Norton DNS على جهاز التوجيه الخاص بك لتأمين جميع أجهزة منزلك.
كان Norton من بين أوائل مزودي DNS العامين المجانيين الذين قدموا مستوى معينا من الأمان. كان لديهم ثلاث سياسات:
A — الأمان (الفيروسات ومواقع التصيد الاحتيالي ومواقع الاحتيال): 199.85.126.10
ب - الأمن + المواد الإباحية: 199.85.126.20
ج - الأمن + المواد الإباحية + أخرى: 199.85.126.30
يمكن للمستخدمين استخدام هذا لإنشاء جدار حماية قائم على DNS ، مما يمنع الوصول إلى المواد غير المرغوب فيها. تبحث Symantec في سلوك هجوم البرامج الضارة وكيفية انتشاره. يقال أيضا أن Norton Secure DNS عضو في مجموعة عمل مكافحة التصيد الاحتيالي. منظمة صناعية مكرسة لتثقيف المستهلكين حول الاحتيال عبر الإنترنت والقضاء عليه.
تم إطلاق Norton Safe DNS منذ ذلك الحين كخدمة مجانية لجميع الاستخدامات غير التجارية. كل ما يحتاجه الشخص من موقع Norton DNS Server هو اتخاذ بعض الخطوات السهلة لتحويل جهاز الكمبيوتر الخاص به إلى نظام Norton Connectsafe DNS. حتى أن هناك موقع ويب للتحقق يمكنه إخبار المستخدم ما إذا كان قد قام بإعداده بشكل صحيح.

كيف يمكن أن تساعد؟

Norton DNS ، مثل أي خدمة DNS أخرى. سيقوم بتحويل عنوان الويب المستند إلى النص إلى عنوان IP رقمي وإعادة توجيه المستخدم إلى موقع الويب المطلوب. من ناحية أخرى ، لا يحقق Norton DNS ذلك فحسب ، بل يقوم أيضا بإجراء فحص سريع من خلال قاعدة بيانات الويب الآمن من Norton للتأكد من أن الموقع غير معروف بأي مشكلات ، مثل التصيد الاحتيالي أو هجمات البرامج الضارة. بالإضافة إلى ذلك ، قد يذهب الشخص إلى safeweb.norton.com لاكتشاف ما إذا كان هناك أي عنوان URL للويب في قاعدة البيانات دون زيارته فعليا. علاوة على ذلك ، إذا كانت هناك إشارة حمراء ، فسيعرض Norton DNS تفاصيل شاملة حول سبب شعور Symantec بأن الموقع ضار.
على الرغم من حقيقة أنه يؤدي خدمات أكثر من DNS القياسي ، يعتقد الكثير من الناس أن Norton DNS يعمل بشكل أسرع. كما أن لديها 17 مركز بيانات مستضاف في جميع أنحاء العالم لتقديم خدمة سريعة. نظرا لحقيقة أنه مجاني ، لا يقصد من Norton DNS أن يكون بديلا عن حل شامل لمكافحة الفيروسات ومكافحة البريد العشوائي وأنواع أخرى من البرامج الضارة القائمة على مكافحة التطفل. من ناحية أخرى ، يوفر Norton DNS طبقة إضافية من الأمان لمحاربة مواقع الويب الخطرة ، وهي الطريقة الحالية التي يستخدمها المتسللون للهجوم على أهدافهم.

كيفية إعداد نورتون DNS؟

للبدء في إعداد Norton ، قمبالخطوات الواردة أدناه.

1. من قائمة ابدأ ، حدد لوحة التحكم.
2. عرض حالة الشبكة والمهام بالنقر فوق الزر عرض حالة الشبكة والمهام.
3. حدد اتصال الشبكة الذي ترغب في التبديل إليه إلى Norton DNS.
4. حدد بروتوكول الإنترنت الإصدار 4 من القائمة المنسدلة.
5. انقر فوق خصائص مرة أخرى ، ثم أدخل عناوين IP الخاصة ب Norton DNS الواردة أدناه.
6. في موجه الأوامر ، اكتب ipconfig / تجديد لتحديث إعداد IP الخاص بك.
7. تحقق من التغيير عن طريق تشغيل ipconfig /all في سطر الأوامر والتأكد من أن خوادم DNS تعرض القيم المحدثة.

خطوات البحث عن DNS

في معظم الحالات ، يهتم DNS بترجمة اسم المجال إلى عنوان IP الصحيح. لفهم كيفية عمل هذه العملية. تتبع مسار بحث DNS من مستعرض ويب إلى عملية بحث DNS والعودة مرة أخرى. دعنا ننتقل إلى الخطوات واحدة تلو الأخرى.

1. عندما يقوم المستخدم بإدخال "example.com" في مستعرض ويب ، يتم توجيه الاستعلام عبر الإنترنت ويتم استلامه بواسطة محلل DNS المتكرر.
2. بعد ذلك ، يطلب المحلل خادم أسماء جذر DNS (.).
3. ثم يستجيب خادم الجذر للمحلل من خلال توفير عنوان خادم DNS لنطاق المستوى الأعلى (TLD) (مثل as.com or.net) ، والذي يحتفظ بمعلومات لمجالاته. عندما نبحث عن example.com ، يتم إرسالنا إلى the.com TLD.
4. بعد ذلك ، يتم إرسال طلب من قبل المحلل إلى .com TLD.
5. بعد ذلك ، يجيب خادم TLD بعنوان IP لخادم أسماء المجال ، example.com.
6. أخيرا ، يقوم المحلل العودي بالاستعلام عن خادم أسماء المجال.
7. يقوم خادم الأسماء بعد ذلك بإرجاع عنوان IP ل example.com إلى المحلل.
8. ثم يقوم محلل DNS بإرجاع عنوان IP للمجال الذي تم طلبه في الأصل إلى متصفح الويب.

4 أنواع من خوادم DNS

مؤشر DNS

مؤشر DNS هو خادم يقبل الطلبات من الأجهزة العميلة عبر برامج مثل متصفحات الويب. غالبا ما يكون المؤشر مسؤولا عن إجراء استعلامات إضافية من أجل تلبية استعلام DNS الخاص بالعميل.

خادم اسم الجذر

خادم أسماء الجذر هو المرحلة الأولية في تحويل (حل) أسماء المضيفين التي يمكن قراءتها من قبل الإنسان إلى عناوين IP. يمكن مقارنته بفهرس في مكتبة يرتبط برفوف كتب مختلفة - بشكل عام. إنه بمثابة مرجع لمواقع أخرى أكثر تحديدا.

خادم اسم TLD

فكر في خادم نطاق المستوى الأعلى (TLD) كحامل محدد للكتب في المكتبة. خادم الأسماء هذا هو المرحلة التالية في البحث عن عنوان IP معين. يستضيف العنصر الأخير من اسم المضيف (خادم TLD في example.com هو "com").

خادم الأسماء الموثوق

فكر في خادم الأسماء النهائي هذا كقاموس على رف الكتب. حيث يمكن ترجمة اسم معين إلى تعريفه. المحطة الأخيرة في استعلام خادم الأسماء هي خادم الأسماء الموثوق. إذا كان خادم الأسماء الموثوق لديه حق الوصول إلى السجل المطلوب. سيعود إلى مؤشر DNS الذي قدم الطلب الأولي لعنوان IP لاسم المضيف المطلوب.