



الهيئة الوطنية لخدمات الشبكة
National Agency For Network Services

الجمهورية العربية السورية

وزارة الاتصالات والتقانة

الهيئة الوطنية لخدمات الشبكة

اللائحة التنظيمية

رقم NANS/SP/01

النواظم والمعايير التقنية لمقدمي خدمات النفاذ إلى الشبكة

النسخة الأولى

ضبط الوثيقة

سجلات التغيير

النسخة	الحالة	إصدار	التاريخ
1.0	مسودة		12/04/2013
1.1	إقرار		10/12/2013
1.1	إصدار		

المراجعات

الصفة	الاسم	التاريخ
خبير	طلال شرابي	21/02/201
فنيون وإداريون	مزودات خدمة الانترنت	21/05/2013
فنيون	مزودات خدمة الانترنت	25/06/2013



جدول المحتويات

4	أولاً: مقدّمة
5	ثانياً: أحكام عامة
5	ثالثاً: مسؤولية مقدّمي خدمات النفاذ
5	1- متابعة بيانات الحركة
7	2- خباياة المحتوى
9	3- حجب المواقع حسب الطلب

أولاً: مقدمة:

تهدف هذه اللائحة إلى تحديد النواظم والمعايير التقنية التي تؤمن الحد الأدنى من المعلومات والبيانات الواجب توفرها لدى مقدمي خدمات النفاذ إلى الشبكة، وذلك بهدف تقديمها إلى السلطات القضائية المختصة عند الطلب.

التعريف:

إن جميع التعابير المستخدمة في هذه اللائحة متوافقة مع ما ورد بقانون تنظيم التواصل على الشبكة و مكافحة الجريمة المعلوماتية.

القانون: قانون " تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية " الصادر بالمرسوم التشريعي رقم 17/ لعام 2012.

التعليمات التوضيحية والتنفيذية: التعليمات التوضيحية لقانون التواصل على الشبكة، والصادرة بقرار وزير الاتصالات والتقانة رقم 290/ لعام 2012.

مقدم خدمات النفاذ إلى الشبكة: مقدم الخدمات الذي يتيح للمستخدمين لديه النفاذ إلى الشبكة والوصول إلى المعلومات والخدمات المتوفرة عليها.

برمجيات خبيثة: برمجيات حاسوبية مصممة لإلحاق الضرر بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو المواقع الإلكترونية أو الشبكة، أو تعطيل عملها أو تبطئتها، أو تخريب محتوياتها أو مواردها، أو جمع معلومات عن مالكيها أو مستخدميها أو عن بياناتهم دون إذنهم، أو إتاحة الدخول إليها أو استخدامها أو استخدام مواردها بصورة غير مشروعة.

البريد الواعل: أي شكل من أشكال الرسائل، مهما كان محتواه، التي تُرسل على الشبكة إلى الغير، دون رغبة الملقّي في وصولها إليه.

سلامة المحتوى Integrity: ضمان حالة المحتوى صحيحة ودقيقة دون تعرضها لأي تغيير (تعديل أو حذف) بشكل غير مرخص به، وذلك في أي مرحلة من مراحل المعالجة أو التخزين أو النقل.

السرية Confidentiality: الحفاظ على سرية المعلومات، وتدقيقها، والمعاملات والخدمات أو الإجراءات التي تجري عبر الشبكة، ومنع إفشائها إلى أطراف غير مرخص لها، كما تهدف إلى حماية تلك المعلومات من الاطلاع عليها أو استنساخها بصورة غير قانونية، أثناء تخزينها أو معالجتها أو نقلها.

ثانياً: أحكام عامة

1. تطبق هذه اللائحة على مقدمي خدمات النفاذ إلى الشبكة المرخص لهم في الجمهورية العربية السورية.
2. تشمل هذه اللائحة الضوابط والمعايير الفنية التي يجب أن يحققها مقدم وخدمات النفاذ إلى الشبكة وذلك لتطبيق أحكام المواد (2-3) من القانون، وتوضيحات المواد (2-3) من التعليمات التوضيحية والتنفيذية.
3. يخضع مقدم وخدمات النفاذ إلى الشبكة عند عدم توفر المعلومات والبيانات المطلوبة في هذه اللائحة إلى العقوبة المنصوص عليها في المادة (8) من القانون.

ثالثاً: مسؤوليات مقدمي خدمات النفاذ إلى الشبكة:

تتخصر مسؤوليات مقدمي خدمات النفاذ إلى الشبكة في ثلاثة مواضيع رئيسية:

- متابعة بيانات الحركة Accounting وفق المادة 2 / (أ) من القانون والتعليمات التوضيحية.
- خباية المحتوى Caching، وفق المادة 3 البند (أ) من القانون والتعليمات التوضيحية.
- حجب المحتوى حسب الطلب، وفق المادة 3 البند (ج) من القانون والتعليمات التوضيحية.

(1) متابعة بيانات الحركة:

(1-1). بيانات الحركة الواجب تخزينها:

المرجع: المادة 2 / (أ) / (ت3) من القانون والتعليمات التوضيحية.

- اسم المستخدم (Username).
- عنوان المصدر للمستخدم (Source IP address).
- توقيت البدء وتوقيت النهاية لجلسة الاتصال (Start time & Stop time).
- حجم البيانات التي تم تبادلها ضمن الجلسة.

(2-1). مدة التخزين:

المرجع: المادة 2 / (أ) / (ت1) من القانون والتعليمات التوضيحية.

- تخزين بيانات الحركة لمدة سنة واحدة على الأقل.

(3-1). المتطلبات التقنية:

المرجع: المادة 2 / (أ) / (ت2) من القانون والتعليمات التوضيحية.

يجب تأمين المتطلبات التقنية التالية كحد أدنى:

1. توفرُ التجهيزات والبرمجيات التالية لدى مقدمي خدمات النفاذ إلى الشبكة:

- جهازُ حاسوب بمواصفاتٍ مخدّم من حيثُ سرعة الأداء وسعة التخزين.

- نظامٌ متابعةٍ برمجيّ (AAA System) يقومُ بتحليل البيانات القادمة من التجهيزات الشبكيّة

وتخزينها، وإعادة عرضها بشكلٍ تقاريرٍ حسب الطلب ضمن المعلومات المطلوب تخزينها.

- قاعدة معطياتٍ مركزيّةٍ محميّةٍ بكلمة مرور، تُدارُ من قبل مديرٍ نظامٍ خاصّ (Database

Administrator) وتحققُ المتطلبات التالية:

○ الإدارة المركزيّة (Central Management).

○ التّحديثُ المركزي (Central Update).

○ الحماية المركزيّة، مع إمكانيّة تشفيرها لضمان السريّة.

○ سهولة توليدُ التقارير المطلوبة (Reports Generating).

○ سهولة عمليّة التخزين (Easy Storage).

○ سهولة استرجاع البيانات في أيّ وقتٍ.

2. استخدامُ بروتوكولٍ خاصٍ لمتابعة بيانات الحركة يحقّقُ الوظائف التالية:

- إمكانيّة تشفير اسم المستخدم وكلمة المرور الخاصّة به.

- إمكانيّة توليد تقارير ديناميكيّة حسب الحاجة.

- إمكانيّة تشفير بيانات الحركة.

3. وجودُ مخدّم احتياطيّ لإتمام عمليّة تخزين بيانات الحركة في حال تعطلّ المخدّم الرئيسيّ .

(2) خباية المحتوى:

تهدفُ عمليةُ خبايةِ المحتوى لدى مقدّمي الخدمات إلى الشبكةِ بشكلٍ رئيسيٍّ إلى تحسينِ جودةِ الخدمةِ المقدّمة، دونَ أن تتسبّب بأيِّ جملٍ إضافيٍّ على الشبكةِ.

(1-2) المتطلباتُ الفنيّةُ:

المرجعُ: المادةُ 3 / (أ) / (ت1) من القانونِ والتّعليماتِ التّوضيحيّةِ.

- توقّرُ مخرّجاتِ Servers تُستخدمُ لخبايةِ المحتوى ذاتِ مواصفاتٍ فنيّةٍ جيّدةٍ.
- تأمِينُ حمايةِ المخرّجاتِ من الاختراقاتِ والهجماتِ الأمنيّةِ.

(2-2) مدّةُ الخبايةِ المسموحِ بها:

المرجعُ: المادةُ 3 / (أ) / (ت2) من القانونِ والتّعليماتِ التّوضيحيّةِ.

تتحدّدُ مدّةُ الخبايةِ المسموحِ بها للمحتوى المخبوءِ في مخرّجاتِ الخبايةِ بالفترةِ الزمانيّةِ التي تضمّنُ وجودَ تطابقٍ بينَ المحتوىِ المخبوءِ والمحتوى الحقيقيّ على المخرّمِ الرّئيسيِّ للموقعِ، على أن يتمّ تحديثُ المحتوىِ المخبوءِ في حالِ تغيّرِ المحتوىِ الحقيقيّ.

(3-2) البياناتُ الواجبُ تخزينُها:

المرجعُ: المادةُ 2 / (أ) / (ت3) من القانونِ والتّعليماتِ التّوضيحيّةِ.

- ملفُّ النّفاذِ Access log الخاصّ بالمخرّجاتِ.
- عناوينُ الإنترنتِ URL التي تمّ طلبُها.
- العناوينُ IP Address التي تمّ الطّلبُ منها.
- توقيتُ البدءِ وتوقيتُ النّهايةِ لجلسةِ الاتّصالِ (Start time & Stop time).
- يجبُ حفظُ هذهِ البياناتِ لمدّةِ سنةٍ واحدةٍ على الأقلّ.

(2-4) سلامة المحتوى المخبوء:

المرجع: المادة 3 / (أ) / (ت2) من القانون والتعليقات التوضيحية.

لضمان سلامة المحتوى المخبوء ضمن خدمات خباية المحتوى، يجب تحقيق المتطلبات التالية:

- أن يتوقف مشغل البروكسي الخاص بمخدم خباية المحتوى آلياً عن العمل وبشكل فوري في حالات عدم استجابة مخدم خباية المحتوى، من أجل السماح للمستخدم بالتخاطب المباشر مع المخدم الرئيسي للموقع المطلوب.
- استخدام أسلوب إعادة التوجيه إلى مخدم خباية المحتوى Redirection وعدم استخدام نمط خباية المحتوى في الوسط Caching inline، لضمان استمرار الاستجابة لطلب المستخدم في حال حدوث أي خطأ في مخدم خباية المحتوى. ويفضل أيضاً في هذه الحالة استخدام قواعد خاصة Rules ضمن الموجّه الذي يقوم بإعادة توجيه الطلبات إلى الموقع الرئيسي الذي يحتوي على المحتوى الحقيقي من أجل معالجة حالات الفشل في مخدم خباية المحتوى.
- ضمان عدم تقديم موقع يختلف عن الموقع الأصلي.

(2-5) الحفاظ على السرية والخصوصية:

المرجع: المادة 3 / (أ) / (ت2) من القانون والتعليقات التوضيحية.

لضمان سرية وخصوصية المحتوى المخبوء ضمن خدمات خباية المحتوى، يجب تحقيق المتطلبات التالية:

- عدم حفظ أي معلومات تدل على هوية المستخدمين الشخصية، أو المحتوى الذي تم طلبه من قبلهم أو أي معلومات أخرى تشير بشكل مباشر أو غير مباشر إليهم ضمن مخدم خباية المحتوى.
- أن يتضمن مشغل البروكسي الخاص بمخدم خباية المحتوى على إعدادات خاصة بحماية البيانات التي يتم تخزينها بحيث لا يتم انتهاك الخصوصية ، وبشكل رئيسي آليات التشفير والاستيقان Authentication ، وذلك لضمان عدم الوصول أو الاستنساخ أو التعديل أو الحذف للمحتوى بشكل غير مرخص به.

- أن يكون لدى مُقدّمي خدماتِ النفاذِ إلى الشبكةِ سياسةَ حمايةٍ خاصةٍ تحدّدُ المخولّينَ بالنفاذِ إلى مخدّم خباية المحتوى من قبلِ موظّفي مقدّم الخدمة، وضمان عدم الوصولِ غير المرخّصِ به من أشخاصٍ غير مخولّين بذلك، مع ضرورة إجراءِ مراجعةٍ دوريةٍ لملفِ Log Files الذي يتم فيه تسجيل جميع النّشاطات التي تجري على مخدّم خباية المحتوى.
- التّحديثُ الدّوري لمشغّل البروكسي الخاص بمخدّم خباية المحتوى، وتنصيبُ آخر التّحديثاتِ Patches المعلن عنها، وذلك لسدّ الثغراتِ الأمنيّة والبرمجيّة المكتشفة فيه.
- إمكانية إضافة برمجياتٍ أخرى إلى مشغّل البروكسي الخاص بمخدّم خباية المحتوى، مثل برمجيات الحماية من البريد الواعِل والبرمجيات الخبيثة .

(2-6) إتلاف المحتوى المخبوء:

المرجع: المادة 3 / (أ) / (ت2) من القانون والتّعليمات التوضيحية.

يتم إتلاف المحتوى المخبوء من مخدّم خباية المحتوى آلياً فور تحديته من المخدّم الرئيسي للمحتوى.

(3) حجب المحتوى حسب الطلب:

يقصدُ به إمكانية حجب الوصول إلى مواقع إلكترونية معينة أو محتوى معين على الشبكة بناءً على طلبِ المشترك.

(3-1) المتطلبات التقنية:

المرجع: المادة 3 / (ج) / (ت1) (ت2) من القانون والتّعليمات التوضيحية.

يمكن لمقدّمي خدماتِ النفاذِ إلى الشبكة تحقيق ذلك عن طريق إحدى الوسائل التقنية التالية:

- مخدّم بروكسي Proxy Server بمواصفاتٍ فنيّة جيّدة.
- تجهيزاتٍ شبكيّة أو برمجياتٍ تلبّي هذه الوظيفة بأداءٍ جيّد دون أن تسبّب عبءاً على الشبكة.

يجب أن تحقّق هذه الخدمة المتطلبات التالية من حيث الآلية العمل:

1. تمرير كامل طلبات تصفّح المواقع الخاصة بالمشترك عبر قائمة الحجب الخاصة به ويتم مقارنة الموقع الذي تم طلبه مع هذه القائمة.

2. في حال كانَ الموقعُ المطلوبُ محجوباً بناءً على طلبه، يتم توجيهه إلى صفحةٍ خاصّةٍ تحتوي على رسالةٍ تُعلمه بأنّ الموقعَ محجوبٌ بناءً على طلبه.
3. إذا لم يحدث تطابقٌ مع قائمةِ الحجب يتم توجيهُ طلبِ المشتركِ إلى الموقعِ المطلوبِ.
4. تُقدّمُ خدمةُ حجبِ المواقعِ على مستوى موقعٍ معيّنٍ (مثال www.example.com) أو على مستوى رابطٍ محدّدٍ (مثال www.example.com/files/somfiles.zip).
5. تُقدّمُ هذه الخدمةُ على مستوى بروتوكول الويب HTTP بالحدِّ الأدنى.
6. يجبُ حجبُ جميعِ النطاقاتِ الرديفةِ للموقعِ المطلوبِ حجبه.
7. تُقدّمُ هذه الخدمةُ بناءً على طلبِ شخصيٍّ من قبلِ المشتركِ إلى مُقدّمِ خدمةِ التّفاذ، يحتوي هذا الطّلبُ على قائمةِ المواقعِ التي يرغبُ بحجبها، ولا يجوزُ تعديلها أو إلغاؤها إلا بناءً على طلبِ المشترك شخصياً.