هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار أمن الخادم الوكيل

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة.
وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اختر التصنيف

الإصدار <1.0>

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <1.0>

قائمة المحتويات

الغرض

يهدف هذا المعيار إلى تحديد متطلبات الأمن السيبراني التفصيلية ذات العلاقة بحلول الخادم الوكيل لدى <اسم الجهة>.

تمت مواءمة متطلبات هذا المعيار مع متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني بما في ذلك على سبيل المثال لا الحصر، الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018)، بالإضافة إلى المتطلبات التشريعية والتنظيمية للأمن السيبراني ذات العلاقة.

نطاق العمل

يغطي هذا المعيار الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة> والأطراف الخارجية ذات العلاقة.

المعايير

1	المتطلبات العامة (General requirements)
الهدف	ضبط إعدادات الخادم الوكيل وإدارته واستخدامه بشكل آمن وملائم عند الحاجة لمنع الدخول إلى الشبكة الخاصة.
المخاطر المحتملة	قد يؤدي ضبط إعدادات الخادم الوكيل بشكل خاطئ إلى فتح ثغرات قد يترتب عليها سرقة المعلومات والكشف عنها والوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-1	جميع المتطلبات في هذا المعيار مرتبطة بكل أنواع الخوادم الوكيلة المدرجة في الجدول "أ" ويجب تطبيقها عليها.
2-1	أن يقتصر الوصول الفعلي إلى الخادم الوكيل على الموظفين المصرح لهم فقط (الحدّ الأدنى من الصلاحيات لمختلف مديري النظام).
3-1	فصل مُجمّعات معلومات الشبكة (NICs) غير المستخدمة عن أي شبكة.
4-1	أن يدعم الخادم الوكيل حزمة الإصدار الرابع من بروتوكول الإنترنت (IPv4) والإصدار السادس من بروتوكول الإنترنت (IPv6) لمعالجة حركة البيانات وتحديد قواعد الأمن وسياسة حركة البيانات على الشبكة.

5-1	تثبيت كافة التحديثات الأمنية للخادم الوكيل فور إصدارها من المورّد ووفقًا لسياسة إدارة التغييرات المعمول بها في <اسم الجهة>.
6-1	التأكد من إمكانية استخدام الخادم الوكيل من خلال منهجيات مختلفة - النشر المُضمّن، خادم وكيل غير مرئي، خادم وكيل مرئي، نطاق - كما هو موضح في الجدول "أ" وفقًا لبنية الشبكة الخاصة ب<اسم الجهة>.
7-1	يجب أن تستخدم جميع قنوات الاتصال الإدارية شبكة إدارة مُخصصة، أو مصادقة اتصالات الشبكة الإدارية وتشفيرها باستخدام وحدات التشفير، بما يتوافق مع المعايير الوطنية للتشفير.
8-1	يجب أن يكون حق الوصول الإداري إلى واجهة إدارة الخادم الوكيل مقتصرًا على مديري النظام المصرّح لهم فقط.
9-1	يجب مزامنة إعدادات الوقت الخاصة بالخادم الوكيل مع خوادم زمنية موثوقة.
2	إدارة حركة البيانات (Traffic shaping)
الهدف	ضبط إعدادات الخادم الوكيل بشكل سليم وإدارته بشكل آمن من أجل فرز اتصالات الشبكة بشكل صحيح.
المخاطر المحتملة	قد يؤدي الإعداد الخاطئ لقواعد إدارة حركة البيانات إلى عواقب وخيمة مثل حجب حركة البيانات الأساسية وحجب الخدمة.
الإجراءات المطلوبة	
1-2	أن يوفر الخادم الوكيل سياسة للتحكم بحركة البيانات تسمح بتحديد أقل عنوان من عناوين بروتوكول الإنترنت للمصدر والوجهة، والمنفذ المتوافق مع بروتوكول التحكم في الإرسال، وخيارات التسجيل.
2-2	أن يكون المستخدمون الإداريون قادرين على إعداد قوائم ثابتة بالموارد المتاحة دائمًا أو المرفوضة التي يجب التحقق منها عن طريق خادم وكيل أثناء معالجة حركة البيانات.
3-2	أن يتعرف الخادم الوكيل على عناوين الإنترنت (محددات الموارد الموحدة) والتطبيقات (بناءً على التوقيعات) وعناوين بروتوكول الإنترنت والمنافذ المتوافقة مع بروتوكول التحكم في الإرسال.
4-2	أن يكون الخادم الوكيل قادرًا على تخزين كائنات الويب الأكثر استخدامًا لتحسين النطاق الترددي لحركة البيانات والتأخير.
5-2	أن يكون الخادم الوكيل قادرًا على ضبط أو إضافة أو إعادة كتابة عناوين الحزم.

6-2	أن يكون الخادم الوكيل قادرًا على التحقق من مستوى الامتثال لمعايير البروتوكول ويمنع حركة البيانات غير الممتثلة (أو تصحيح وإصلاح حركة البيانات غير الممتثلة). فعلى سبيل المثال، يمكن لخادم وكيل البث إيقاف هجوم تجاوز سعة التخزين المؤقت بشكل كامل باستخدام إنفاذ الامتثال للبروتوكول.
7-2	أن يوفر الخادم الوكيل القدرة على ترجمة البروتوكولات من أحد جانبي الاتصال إلى الآخر. فعلى سبيل المثال، إذا كان العميل قادرًا فقط على استخدام الإصدار الرابع من بروتوكول الإنترنت، فيمكن استخدام الخادم الوكيل كوسيط لربط العميل بالإصدار السادس من بروتوكول الإنترنت، مما يسمح للعميل بالوصول للشبكة بدون توفر دعم الإصدار السادس من بروتوكول الإنترنت لدى العميل. وبالمثل، يمكن لعميل أو بيئة تمتلك الإصدار السادس من بروتوكول الإنترنت فقط الوصول إلى خادم ويب مدعوم بالإصدار الرابع من بروتوكول الإنترنت من خلال خادم وكيل الويب.
3	فحص حركة البيانات (Traffic inspection)
الهدف	يجب أن تعالج الخوادم الوكيلة حركة البيانات بطريقة آمنة لرصد الإشارات التي تدل على سلوك غير طبيعي أو خبيث بعناية وتقييمها.
المخاطر المحتملة	قد تؤدي معالجة حركة البيانات بدون توفير طبقة أمنية إلى انتشار البرمجيات الضارة بسهولة وتعريض الشبكة لمخاطر التصيد الاحتيالي وتسرب المعلومات.
الإجراءات المطلوبة	
1-3	أن يتضمن الخادم الوكيل ميزة قاعدة تصنيف عناوين الإنترنت (محددات الموارد الموحدة) وتقسيمها إلى فئات مختلفة، مثل التصيد الاحتيالي، والأخبار، والأدوية، والخدمات الطبية، والخدمات المصرفية، وغيرها.
2-3	أن يحتوي الخادم الوكيل على وحدة برمجيات مكافحة الفيروسات لفرز جميع العناصر المنقولة إلى العملاء، وتقنية الكشف عن نقطة النهاية والاستجابة لها لتحديد السلوكيات المشبوهة. يجب أن تكون وحدة برمجيات مكافحة الفيروسات متوافقة مع متطلبات معيار الحماية من البرمجيات الضارة المطبق في <اسم الجهة>.
3-3	أن يحتوي الخادم الوكيل على قاعدة تطبيقات مقسمة إلى فئات متنوعة، مثل الشبكة الخاصة الافتراضية، وخادم وكيل تور، وغيرها.
4-3	تحديث قاعدة تصنيف عناوين الإنترنت والتطبيقات وتوقيعات الفيروسات يوميًا على الأقل.
5-3	أن يحلل الخادم الوكيل الاتصال بأكمله، بما في ذلك عناوين الحزم، ومعايير طلب بروتوكول نقل النص التشعبي، وعناصر الويب، والنصوص، وما إلى ذلك.

6-3	يجب أن يكون الخادم الوكيل قادرًا على اعتراض حركة البيانات المؤمنة ببروتوكول طبقة المقابس الآمنة وبروتوكول أمان طبقة النقل - فك تشفير الاتصالات المحددة وفحصها وتشفيرها.
7-3	خلال عملية فحص اتصالات الإنترنت المشفرة ببروتوكول طبقة المقابس الآمنة، يجب أن يستخدم الخادم الوكيل شهادة موقعة من قبل هيئة إصدار الشهادات الخاصة بـ<اسم الجهة>.
8-3	أن يتمتع المستخدمون الإداريون بإمكانية استبعاد بعض الاتصالات من عملية الفحص (على سبيل المثال، عملية تقاطع طبقة المقابس الآمنة).
9-3	أن يتمتع المستخدمون الإداريون بإمكانية دمج الخادم الوكيل مع الحلول الأمنية الأخرى، مثل البيئة التجريبية ووسيط أمان الوصول إلى السحابة ومنع فقدان البيانات، وغيرها باستخدام واجهات قياسية مثل بروتوكول تكييف محتوى الإنترنت.
10-3	أن يمنع الخادم الوكيل وصول المستخدمين غير المصرح لهم إلى موارد الويب من خلال فرض بوابة الوصول المُقيد أو عن طريق دمجها مع نظام المصادقة الخاص بـ<اسم الجهة>.
11-3	أن يُبلغ الخادم الوكيل المستخدمين بالإجراءات المتخذة (لا سيما الطلبات أو الملفات المحجوبة) عبر صفحات الويب للاستجابة القابلة للتهيئة والإعداد.
12-3	أن يستخدم الخادم الوكيل تدفقات البيانات الأمنية الواردة من الجهات الوطنية الموثوقة، مثل الفريق الوطني للاستجابة لحوادث أمن الكمبيوتر.
4	التسجيل والمراقبة (Logging and Monitoring)
الهدف	مراقبة وتخزين جميع الأحداث الحساسة المتعلقة بأمن الخادم الوكيل للكشف عن هجمات الأمن السيبراني بشكل استباقي.
المخاطر المحتملة	لا يمكن إجراء فحص للأداء وهجمات الشبكة وتدابير الأمن السيبراني الرقابية، مثل مؤشرات الأداء الرئيسية ومخالفات الحوكمة والامتثال، من دون ضبط الإعدادات والتهيئة الصحيحة للسجلات.
الإجراءات المطلوبة	
1-4	ضبط إعدادات الخادم الوكيل لتسجيل الأحداث وسجلات التدقيق في نظام السجلات المركزي.
2-4	أن يجمع الخادم الوكيل الأحداث في ملفات منفصلة، لا سيما لأغراض التدقيق والأحداث المرتبطة بحركة البيانات.

3-4	أن يقوم الخادم الوكيل بتسجيل جميع طلبات عناوين الإنترنت والجلسات المرفوضة والتهديدات.
4-4	أن يجمع الخادم الوكيل على الأقل الأحداث المرتبطة بمحاولات تسجيل الدخول الفاشلة أو الناجحة إلى واجهات الإدارة في ملف سجل التدقيق.
5-4	أن تكون سجلات الخادم الوكيل متوافقة مع متطلبات إدارة تسجيل الأحداث ومعيار المراقبة المطبق في <اسم الجهة>.
6-4	أن تشتمل سجلات الخادم الوكيل على المعلومات التالية، كحد أدنى: ● تاريخ ووقت الجلسة ● عنوان بروتوكول الإنترنت المصدر ● بيانات تسجيل دخول المستخدم ● بروتوكول الإنترنت الوجهة ● التدابير المتخذة ● المسار الكامل لعنوان الإنترنت ● تصنيف عنوان الإنترنت ● سياسة حركة البيانات المتبعة
7-4	ضبط إعدادات الخادم الوكيل لإرسال سجلات محددة فقط إلى نظام السجلات المركزي باستخدام بروتوكول سجل النظام (syslog) وبتنسيق الحدث العام (CEF) أو التنسيق الموسع لسجل الحدث (LEEF) أو تنسيق RFC 5425 المحدد للسجلات.

الجدول "أ" - منهجيات نشر الخادم الوكيل

المنهجية	الوصف
النشر المُضمّن	عادة ما يستخدم النشر المُضمّن في الجهات الصغيرة بسبب سهولة تنفيذه ومستوى الأمان العالي الذي يوفره. من خلال النشر المُضمّن، يتم وضع بوابة الويب مباشرة في مسار حركة البيانات على جميع الشبكات القادمة إلى والمغادرة من شبكة الإنترنت. إذا اخترت النشر المُضمّن، فتأكد من أن بوابة الويب الخاصة بك قادرة على تجاوز حركة البيانات على الشبكة التي لا تريد معالجتها بواسطة بوابة الويب. وفي كثير من الحالات، يمكنك اختيار إما "الخادم الوكيل" (إعادة التوجيه) أو "تجاوز" بروتوكول معين. فإذا قررت استخدام الخادم الوكيل للبروتوكول، فهذا يعني أن بوابة الويب ستنهي حركة البيانات القادمة من العميل إلى الخادم محليًا وتعيد إنشاء اتصال جديد لاستخدامه كعميل للخادم للحصول على المعلومات المطلوبة.
النشر المرئي	عادة ما تُستخدم آلية النشر المرئي عند استخدام بوابة ويب على شبكة أكبر، وكان تصميم الشبكة يتطلب عدم وجود نقطة فشل واحدة. تتيح آلية النشر المرئي وضع بوابة الويب في أي موضع على الشبكة يمكن لجميع المستخدمين الوصول إليه ويتيح للجهاز نفسه الاتصال بالإنترنت. تستخدم آلية النشر المرئي تعريفًا صريحًا على متصفح الويب. ولتسهيل هذا النوع من النشر، يمكن للمدير توزيع ملفات بروتوكول الاكتشاف التلقائي لوكيل الويب أو ملفات الإعداد التلقائي للوكيل من أجل إعداد الوكيل المرئي في متصفحات المستخدم النهائي.
النشر غير المرئي	يسمح النشر غير المرئي باستخدام بوابة الويب في أي موقع على الشبكة يتضمن اتصال بالإنترنت على غرار آلية النشر المرئي، مما يقلل من الحاجة إلى تغيير إعدادات الشبكة. بالإضافة إلى ذلك، لا يترتب على ضبط إعدادات أنظمة المستخدمين النهائيين أي نفقات إدارية عامة لأن عملية توجيه حركة البيانات ببروتوكول نقل النص التشعبي وبروتوكول نقل النص التشعبي الآمن عادة ما تتم بواسطة الموجّه أو أي جهاز آخر متصل بالشبكة. غالبًا ما يُستخدم الخادم الوكيل غير المرئي عندما يكون حجم الجهة كبيرًا جدًا لدرجة لا يمكن معها استخدام النشر المُضمّن، ولا تريد الجهة تحمل العبء الإضافي والنفقات العامة التي تستلزمها آلية التنفيذ الصريح. تعتمد معظم آليات النشر غير المرئي على بروتوكول اتصالات ذاكرة التخزين المؤقت للويب وهو بروتوكول تدعمه العديد من الأجهزة المتصلة بالشبكة. بدلًا من ذلك، يمكن الاستعانة بآلية النشر غير المرئي باستخدام التوجيه القائم على السياسة أو استخدام أجهزة التحكم في تنفيذ التطبيقات لإدارة وتحسين اتصالات العميل بخوادم الويب والتطبيقات.

محلّل المنفذ المحوّل	تُعرف آلية نشر محلّل المنفذ المحوّل (SPAN) أحيانًا بآلية النشر القائمة على إعادة ضبط بروتوكول التحكم بالإرسال نظرًا لاعتمادها على عمليات إعادة ضبط بروتوكول التحكم بالإرسال لتنفيذ سياسة بوابة الويب. يتم نشر بوابة الويب من خلال ربطها بمحلّل المنفذ المحوّل على المُبدّل. وعلى عكس آليات النشر الثلاثة الأخرى التي تعالج حركة البيانات على الشبكة وتنفذ السياسات بناءً على مدى استجابة الشبكة لمشاكل بوابة الويب، تقوم بوابة الويب المفعلة عبر منفذ محلل المنافذ المحول بإنفاذ السياسات من خلال إصدار أمر إعادة ضبط بروتوكول التحكم بالإرسال لنظام العميل لمنع استكمال عملية تحميل أي محتوى مخالف.
الخادم الوكيل العكسي	الخادم الوكيل العكسي هو خادم يتميز بقربه من خادم أو أكثر من خوادم الويب، ويقوم باعتراض الطلبات التي تصل من العميل. ويختلف عن الخادم الوكيل الأمامي الذي عادة ما يتخذ موقعًا بالقرب من العملاء أنفسهم. يقوم الخادم الوكيل العكسي بتوجيه طلبات العميل (مثل متصفح الإنترنت) إلى خوادم الويب، وتُستخدم الخوادم الوكيلة العكسية عادةً لزيادة مستوى الأمن والأداء والموثوقية (على سبيل المثال لتجنب القيود المفروضة على تصفح الإنترنت من قبل الدولة أو المؤسسات، أو منع الوصول إلى نوع معين من المحتوى، أو لحماية الهويات على الإنترنت)

الأدوار والمسؤوليات

1- **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

2- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

3- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات> و <الإدارة المعنية بالأمن السيبراني>.

4- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو عند حدوث تغييرات تقنية جوهرية في البنية التحتية أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دوريًا.

اختر التصنيف

الإصدار <1.0>

2- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.

3- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.