أكاديمية التعلم
Academy Of Learning

أمن الشبكات الحاسب المتقدم

دبلوم الأمن السيبراني

تحت إشراف

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

- يشرح وظيفة التواقيع الرقمية.
- يشرح الغرض من الشبكات الافتراضية VPNs.
- يشرح كيفية تشغيلIPsec VPNs .
- يعد VPN من موقع إلى موقع باستخدام سطر الأوامر.
- يشرح كيفية عمل ASA كجدار حماية.
- يهيئ جدار الحماية ASA.
- يعد الوصول عن بعد للشبكات الافتراضية VPN على ASA.
- يشرح مختلف الأساليب والأدوات المستخدمة لاختبار الشبكات.
- يشرح كيفية وضع سياسة أمنية شاملة.

❖ فهرس الكتاب

❖ الفصل الأول: أنظمة التشفير

❖ الفصل الثاني: تنفيذ VPN

❖ الفصل الثالث: تنفيذ ASA

الفصل الأول
أنظمة التشفير

في هذا الفصل سنتعرف على المواضيع التالي:

- مقدمة
- خدمات التشفير
- أنواع التشفير
- التوقيع الرقمي (السلامة والموثوقية)
  - تطبيقات التواقيع الرقمية
  - وظيفة التواقيع الرقمية
  - كيف تعمل التواقيع الرقمية
- الركائز الثلاثة لأمن المعلومات (السرية)
- ملخص
- أسئلة المراجعة

❖ مقدمة

أنظمة التشفير هي الأساس لحماية المعلومات الرقمية وضمان سريتها وسلامتها. يعرض هذا الفصل مفاهيم التشفير الأساسية وأنواع أنظمة التشفير وتطبيقاتها والتوقيع الرقمي.

تحذر العديد من المؤسسات من نقل البيانات الحساسة عبر الشبكات فمثلا المستشفيات تنقل معلومات المريض الحساسة لشركات التأمين. وذلك بسبب خوفها من إمكانية عرض البيانات، أو تغييرها أثناء النقل، أو استخدامها من قبل الأشخاص الخبثاء لإيذاء المرضى، أو التسبب في دعاوى قضائية، أو بغرض الاحتيال. لذلك تريد المؤسسات أن يظل هذا النوع من اتصالات البيانات خاصًا فقد تم تصميم تشفير البيانات لحماية البيانات الحساسة.

تحتوي عملية التشفير على جانبين هما:

١. التشفير

التشفير (Cryptography) هو عملية تحويل البيانات والمعلومات أو خلطها إلى إصدار مشفر غير قابل للقراءة لا يمكن قراءته إلا من خلال الوصول المصرح به. وهو أداة أمان تستخدم على نطاق واسع يمكنها منع اعتراض البيانات الحساسة، إما أثناء تخزينها في ملفات أو أثناء النقل عبر الشبكات. كما يمكن تعريف التشفير أو التعمية على أنه تحويل نص واضح مقروء إلى نص غير مفهوم باستخدام إحدى طرق التشفير والتي قد تكون غير سرية، لكنها تستخدم مفتاحاً سرياً يمكن من يمتلكه من أن يعيد النص المشفر إلى النص الواضح.

٢. تحليل الشفرات

تحليل الشفرات (Cryptanalysis) هو علم وفن فك التشفير دون معرفة مفتاح التشفير، بهدف الوصول إلى البيانات الأصلية أو اكتشاف الثغرات في نظم التشفير. وهو أيضا العملية العكسية للتشفير، أي محاولة معرفة المفتاح السري من النص المشفر، ومن ثم الحصول على النص الواضح.

بعض المفاهيم الأساسية في علم التشفير:

- علم التشفير (Cryptography): هو تحويل البيانات إلى رمز مشفر يتم فك تشفيره وإرساله عبر شبكة خاصة أو عامة.
- النص الواضح (Plain text): البيانات التي يمكن قراءتها وفهمها دون بذل أي جهد خاص.
- النص المشفر (Cipher text): رسالة مشفرة غير قابلة للقراءة.
- التشفير (Encryption): عملية تحويل البيانات إلى نموذج يصعب قراءته دون المعرفة المناسبة.
- فك التشفير (Decryption): عملية تحويل البيانات المشفرة إلى الشكل الأصلي.
- التشفير غير المتماثل (المفتاح العام) Asymmetric encryption (public key):

يستخدم مفاتيح تشفير مختلفة للتشفير وفك التشفير، تُعرف هذه المفاتيح باسم المفاتيح العامة والخاصة.

دمج أمان التشفير في الشبكة:

يتيح تطبيق Cisco لتشفير طبقة الشبكة لمسؤولي الأمان العمل بسلاسة دمج أمان التشفير في الشبكة، ويتوفر التكامل للمستخدمين النهائيين وتطبيقاتهم ، يجب أن يحدث التشفير فقط على حافة الشبكة على LAN حيث تنشأ البيانات الحساسة ، وفك التشفير ليس ضروريًا حتى تصل البيانات إلى جهاز التوجيه في أقصى الحدود LAN حيث يوجد المضيف الوجهة ، يحتفظ مديرو الشبكات بخيار التشفير في أي مكان في مسار البيانات ، عن طريق التشفير بعد بروتوكول (UDP) أو headers TCP ، بحيث يتم تشفير حمل pay-load IP فقط ، يسمح تشفير Cisco IOS network layer لجميع أجهزة التوجيه والمحولات الوسيطة لإعادة توجيه حركة المرور كما تفعل مع أي حزم IP أخرى.
هذا يسمح تشفير الحمولة فقط بتبديل التدفق وجميع ميزات قائمة الوصول للعمل مع البيانات المشفرة، تمامًا كما هو الحال مع حركة مرور النص العادي، وبالتالي الحفاظ على جودة الخدمة المطلوبة (QoS) لجميع البيانات، يمكن للمستخدمين إرسال البيانات المشفرة عبر الإنترنت بشفافية.

❖ خدمات التشفير

التعريف الأبسط هو أن التشفير عبارة عن طريقة تخزين ونقل البيانات في نموذج يمكن للمستلم المقصود فقط قراءته أو معالجته، علم التشفير هو علم الأمان والاتصالات السرية، يسمح الأمان للمرسل بتحويل المعلومات إلى رسالة مشفرة باستخدام مفتاح سري، وهي معلومة معروفة فقط للمرسل والمتلقي المعتمد.
يمكن للمستقبل المعتمد فك التشفير لاستعادة المعلومات المخفية، إذا كان غير مصرح به يتلقى الأفراد الرسالة المشفرة بطريقة أو بأخرى، يجب ألا يتمكنوا من فك تشفيرها بدونها معرفة المفتاح، المفتاح الذي عادة ما يكون سلسلة متغيرة الطول من bits، يعمل مع خوارزمية التشفير لتشفير أو فك تشفير الرسائل.

الخوارزمية: هي مجموعة القواعد الرياضية، توضح كيف يتم التشفير وكيفية فك التشفير ونجد أن العديد من الخوارزميات معروفة للجميع وليست هي الجزء السري من عملية التشفير، السر وراء استخدام خوارزمية تشفير معروفة هو المفتاح.

يمكن أن يكون المفتاح أي قيمة مكونة من سلسلة كبيرة من البتات العشوائية ، تحتوي الخوارزمية على keyspace ، وهو نطاق من القيم التي يمكن استخدامها لبناء مفتاح ، يتكون المفتاح من قيم عشوائية داخل ملف نطاق keyspace كلما زادت مساحة المفاتيح ، زادت القيم المتاحة التي يمكن استخدامها لتمثيل مفاتيح مختلفة ، وكلما كانت المفاتيح أكثر عشوائية ، يصعب على المتسللين اكتشافها ، مفتاح كبير يسمح لمزيد من المفاتيح الممكنة ، يجب أن تستخدم خوارزمية التشفير كاملkeyspace واختر القيم لتكوين المفاتيح بشكل عشوائي قدر الإمكان ، لو تم استخدام keyspace أصغر ، سيكون هناك عدد أقل من القيم للاختيار من بينها عند تكوين مفتاح ، هذا من شأنه زيادة فرصة المهاجم في معرفة القيمة الرئيسية وفك تشفير البيانات المحمية .

بعد تحويل الرسالة إلى نص مشفر، لا ينبغي أن يكون الإنسان ولا الآلة قادرين على معالجتها بشكل صحيح حتى يتم فك تشفيره ، هذا يتيح نقل المعلومات السرية عبر قنوات غير آمنة دون إفشاء غير مصرح به ، عندما يتم تخزين البيانات على جهاز الكمبيوتر ، فهي كذلك عادة ما تكون محمية بواسطة ضوابط الوصول المنطقية والمادية ، عندما تكون هذه المعلومات الحساسة نفسها المرسلة عبر شبكة ، لم يعد بإمكانك أخذ عناصر التحكم هذه كأمر مسلم به ، والمعلومات موجودة في ملف دولة أكثر عرضة للخطر ، إذا التقط متنصت رسالة أثناء مرورها بين رسالتين سيتمكن المتصنت من عرض الرسالة ، لكنها تظهر في شكلها المشفر ولذلك سيكون غير قابل للاستخدام ، حتى لو كان المتنصت يعرف الخوارزمية التي يستخدمها الشخصان لتشفير المعلومات وفك تشفيرها ، بدون المفتاح ، تظل المعلومات عديمة الفائدة لـلمتنصت.

وفيما يلي أمثلة لأهم الخوارزميات التي تستخدم للتشفير:

- AES (Advanced Encryption Standard): تستخدم هذه الخوارزمية على نطاق واسع للتشفير السريع والقوي. تستند إلى تشفير متكامل باستخدام مفاتيح متغيرة بطول ١٢٨أو ٢٥٦ بت.
- RSA (Rivest-Shamir-Adleman): تستخدم هذه الخوارزمية في التشفير الغير متماثل، حيث يستخدم المفتاح العام للتشفير، ويستخدم المفتاح الخاص لفك التشفير.

يمكن تحقيق التشفير الحديث من خلال استخدام البرامج أو الأجهزة، المعدات عادةً ما يكون التشفير هو الطريقة المفضلة، ويرجع ذلك جزئيًا إلى التخصص المخصص للتطبيق الدوائر المتكاملة (ASICs) ومعالجات الإشارات المتقدمة التي لا تعتمد على الجهاز المركزي وحدة المعالجة (CPU) للجهاز، والتي عادة ما تكون مشغولة بأداء العديد من الوظائف الأخرى، إلى تقديم خدمات تشفير مكثفة.

❖ أنواع التشفير

هناك نوعان من خوارزميات التشفير: متماثل (يسمى أيضًا خوارزمية المفتاح المشترك) وغير متماثل (يُعرف أيضًا باسم خوارزمية المفتاح العام).

١. التشفير المتماثل (Symmetric encryption)

يستخدم التشفير المتماثل نفس المفتاح للتشفير وفك التشفير، نظرًا لأنه يستخدم نفس المفتاح، يمكن أن يكون التشفير المتماثل أكثر فعالية من حيث التكلفة للأمان الذي يوفره، ومع ذلك، من المهم زيادة الاستثمار في التخزين الآمن للبيانات عند استخدام التشفير المتماثل. ومن تطبيقات التشفير المتماثل حماية البيانات أثناء النقل بين الأنظمة وتشفير الملفات والمجلدات على الأجهزة.

٢. التشفير غير المتماثل (Asymmetric encryption)

يستخدم التشفير غير المتماثل مفتاحين منفصلين: مفتاح عام ومفتاح خاص، غالبًا ما يتم استخدام مفتاح عام لتشفير البيانات بينما يكون المفتاح الخاص مطلوبًا لفك تشفير البيانات، يتم منح المفتاح الخاص فقط للمستخدمين الذين لديهم حق الوصول المصرح به، نتيجة لذلك، يمكن أن يكون التشفير غير المتماثل أكثر فعالية، ولكنه أيضًا أكثر تكلفة. ومن تطبيقات التشفير غير المتماثل تبادل المفاتيح بشكل آمن والتوقيع الرقمي والمصادقة.

❖ التوقيع الرقمي (السلامة والموثوقية)

يضمن تطبيق التشفير القوي سلامة البيانات الطبية وسريتها أثناء الإرسال، يسمح التشفير باستخدام الإنترنت لنقل البيانات الطبية السرية مما يجعل الإنترنت المتخصص المكلف مثل DGN غير ضروري، من خلال التوقيع والطابع الزمني للسجلات الطبية إلكترونيًا، يتم تحسين قوتها الإثباتية بشكل كبير في حالة رفع دعوى قضائية.

يعرف التوقيع الرقمي بأنه تقنية تعتمد على التشفير غير المتماثل وتستخدم للتحقق من صحة وسلامة البيانات والرسائل. يشبه التوقيع الرقمي التوقيع اليدوي التقليدي، ولكنه يوفر مستوى أعلى من الأمان والموثوقية عند التعامل مع المستندات والمعاملات الرقمية.

• تطبيقات التواقيع الرقمية

يوفر التوقيع الرقمي مستوى عالٍ من الأمان من خلال استخدام التشفير والمفاتيح العامة والخاصة، يمكن ضمان صحة وسلامة البيانات ومنع التلاعب أو الإنكار غير المشروع في عدة تطبيقات مثل:

١. التجارة الإلكترونية: التحقق من هوية الأطراف وتأمين المعاملات عبر الإنترنت.
٢. الوثائق القانونية: توقيع المستندات والعقود القانونية إلكترونيًا
٣. الاتصالات الآمنة: تأمين رسائل البريد الإلكتروني والمراسلات الأخرى.

• وظيفة التواقيع الرقمية

وظائف التوقيع الرقمي متعددة وتشمل مجموعة واسعة من الجوانب الأمنية والتجارية والتقنية. فيما يلي بعض الوظائف الرئيسية للتوقيع الرقمي:

١. التوثيق (Authentication): تضمن أن الرسالة أو المستند تم إرساله من قبل المصدر المحدد.
٢. السلامة (integrity): تضمن عدم تعديل البيانات منذ توقيعها.
٣. عدم الإنكار (Non-repudiation): تمنع المرسل من إنكار توقيعه على الوثيقة بعد إرسالها.

- **كيف تعمل التواقيع الرقمية**

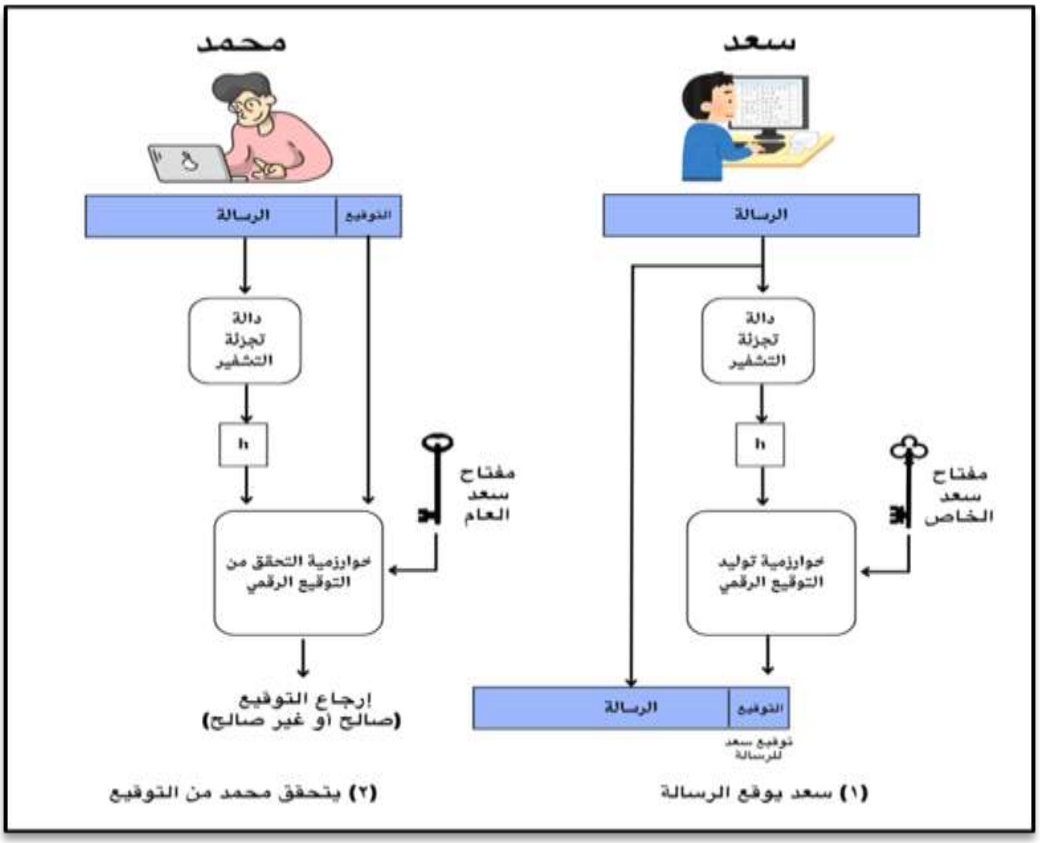
توفر التواقيع الرقمية ضمانات تتعلق بصحة المستند الرقمي وأصالته. تتضمن عملية التوقيع الرقمي الخطوات التالية:

١. يتم إنشاء تجزئة (Hash) للبيانات باستخدام دالة تجزئة.
٢. يتم تشفير التجزئة باستخدام المفتاح الخاص للموقع، مكونًا التوقيع الرقمي.
٣. يرسل المُوقع البيانات مع التوقيع الرقمي.
٤. يستطيع المستقبل التحقق من التوقيع باستخدام المفتاح العام للمُوقع؛ إذا تطابقت التجزئة الناتجة مع التجزئة الأصلية، يضمن المستقبل سلامة وتوثيق البيانات.

الصورة (١) توضح نموذج عام لكيفية عمل واستخدام التوقيعات الرقمية. لنفترض أن سعد يريد إرسال رسالة إلى محمد. يريد محمد أن يتأكد بان الرسالة من سعد بالفعل. ولهذا الغرض، يستخدم سعد دالة تجزئة آمنة، مثل SHA-512، لإنشاء قيمة تجزئة للرسالة. تعمل قيمة التجزئة هذه، جنبًا إلى جنب مع المفتاح الخاص لسعد، كمدخل لخوارزمية إنشاء التوقيع الرقمي. الذي ينتج كتلة قصيرة تعمل كتوقيع رقمي. يرسل بوب الرسالة مع التوقيع المرفق.

عندما يستلم محمد الرسالة ومضاف لها التوقيع، فإنه يقوم بحساب قيمة التجزئة (Hash) للرسالة ثم يوفر قيمة التجزئة (Hash) والمفتاح العام لسعد كمدخلات لخوارزمية التحقق من التوقيع الرقمي. إذا قامت الخوارزمية بإرجاع النتيجة التي تؤكد بأن التوقيع صالح، فيتأكد محمد من أن الرسالة فعلا تم توقيعها وإرسالها بواسطة سعد.

بما أنه لا أحد لديه المفتاح الخاص لسعد، فلا يمكن لأي شخص إنشاء توقيع يمكن التحقق منه لهذه الرسالة باستخدام المفتاح العام له. بالإضافة إلى ذلك، لا يمكن تغيير الرسالة دون الوصول إلى المفتاح الخاص لسعد، لذلك تتم المصادقة على الرسالة من حيث المصدر ومن حيث سلامة البيانات.



صورة (١): كيفية عمل التوقيع الرقمي

❖ الركائز الثلاثة لأمن المعلومات (السرية)

بالإضافة الى التشفير والتوقيع الرقمي، يعد أمن المعلومات مجالا مهما يهدف إلى حماية المعلومات من المخاطر على سلامتها وسريتها وتوافرها. يتم تمثيل جوهر أمن المعلومات من خلال الركائز الرئيسية CIA التالية:

١. السرية (Confidentiality): الغرض منه هو حماية المعلومات من الكشف غير المصرح به. هذا يعني أنك بحاجة إلى إتاحة المعلومات فقط لأولئك الذين لديهم إذن للوصول إليها.
٢. السلامة (Integrity): الغرض منه هو حماية المعلومات من التغييرات غير المصرح بها. هذا يعني أن المعلومات يجب أن تكون دقيقة وكاملة، ويجب الحفاظ على الحالة الأصلية دون تغييرات غير مصرح بها.
٣. التوافر (Availability): نهدف إلى ضمان توفر المعلومات والأنظمة المرتبطة بها وموثوقيتها عند الحاجة. هذا يعني أن المستخدمين المصرح لهم بحاجة إلى أن يكونوا قادرين على الوصول إلى المعلومات والأنظمة عندما يحتاجون إليها.

❖ ملخص

تلعب أنظمة التشفير دورا مهما في حماية المعلومات في العصر الرقمي. إن فهم أنواع التشفير المختلفة وآلياتها وتطبيقاتها سيمكنك من تحسين أمان البيانات وضمان سلامتها وسريتها في مواجهة التهديدات المتزايدة. يوفر التوقيع الرقمي مستويات عالية من الأمان والموثوقية عند التعامل مع المستندات والمعاملات الرقمية الحساسة.

❖ أسئلة المراجعة

١. ما هو الهدف الأساسي من أنظمة التشفير؟

أ- تسريع نقل البيانات

ب- حماية المعلومات الرقمية وضمان سريتها وسلامتها

ت- تقليل حجم البيانات

ث- تحسين جودة البيانات

٢. يعرف التشفير بأنه ...؟

أ- تحويل البيانات إلى نص واضح

ب- عملية نقل البيانات بسرعة

ت- تحويل البيانات إلى نص غير قابل للقراءة يمكن قراءته فقط من خلال الوصول المصرح به

ث- تخزين البيانات بأمان

٣. لماذا يعتبر المفتاح العشوائي ذو الحجم الكبير أكثر أمانًا؟

أ- لأنه يقلل من سرعة التشفير

ب- لأنه يحتوي على المزيد من القيم الممكنة للمفاتيح، مما يجعل اكتشافه أصعب على المتسللين

ت- لأنه يسهل عملية فك التشفير

ث- لأنه يخزن البيانات بشكل آمن

٤. أي من الخوارزميات التالية تستخدم للتشفير غير المتماثل؟

أ- AES

ب- RSA

ت- DES

ث- DES٣

٥. لماذا يمكن أن يكون التشفير غير المتماثل أكثر تكلفة؟

أ- لأنه يستخدم مفتاحًا واحدًا فقط

ب- لأنه يتطلب تخزينًا آمنًا للبيانات

ت- لأنه يستخدم مفتاحين منفصلين ويتطلب إدارة أكثر تعقيدًا

ث- لأنه يحتاج إلى استثمار أقل في الأمان

٦. كيف يضمن التوقيع الرقمي عدم تعديل البيانات؟

أ- عن طريق ضغط البيانات

ب- عن طريق إثبات صحة البيانات وسلامتها

ت- عن طريق حذف البيانات الحساسة

ث- عن طريق تغيير الخوارزمية المستخدمة

٧. كيف يضمن التوقيع الرقمي أن البيانات لم يتم تعديلها منذ توقيعها؟

أ- عن طريق التوثيق (Authentication)

ب- عن طريق عدم الإنكار (Non-repudiation)

ت- عن طريق السلامة (integrity)

ث- عن طريق حذف البيانات الحساسة

٨. التشفير لا يمكن استخدامه لمنع اعتراض البيانات الحساسة أثناء تخزينها في ملفات.

أ- صح

ب- خطأ

٩. التوقيع الرقمي يمكن استخدامه لتوقيع المستندات والعقود القانونية إلكترونيًا.

أ- صح

ب- خطأ

١٠. أحد تطبيقات التشفير المتماثل هو التوقيع الرقمي.

أ- صح

ب- خطأ

الفصل الثاني

تنفيذ VPN

في هذا الفصل سنتعرف على المواضيع التالي:

- مقدمة
- الشبكات الخاصة الافتراضية
- IPsec (Internet Protocol Security)
  - بروتوكولات IPsec
  - IPsec Modes
- تنفيذ IPsec VPN من موقع الى موقع (الجزء العملي)
  - الجزء الأول: تكوين IPsec على R1
  - الجزء الثاني: تكوين IPsec على R3
  - الجزء الثالث: التحقق من IPsec VPN
- ملخص
- أسئلة المراجعة

❖ مقدمة

الشبكة الافتراضية الخاصة (VPN) هي شبكة خاصة يتم إنشاؤها داخل نطاق البنية التحتية للشبكة العامة مثل الإنترنت العالمية، على سبيل المثال باستخدام (VPN)، يمكن للكمبيوتر الوصول عن بعد إلى شبكة مقر الشركة عبر الإنترنت من خلال بناء نفق آمن بين الكمبيوتر الشخصي وجهاز توجيه VPN في المقر المتواجد به.

إذاً (VPN) هي خدمة تقدم اتصال آمن وموثوق عبر بنية تحتية للشبكة العامة المشتركة مثل الإنترنت، و تحتفظ الشبكات الافتراضية الخاصة (VPN) بسياسات الأمان والإدارة مثل شبكة العمل الخاصة ، وإنها الطريقة الأكثر فعالية من حيث التكلفة لإنشاء اتصال من نقطة إلى نقطة بين المستخدمين البعيدين والمستخدمين الإلكترونيين كما تدعم منتجات Cisco أحدث تقنيات VPN.

❖ الشبكات الخاصة الافتراضية

توجد ثلاثة أنواع رئيسية من شبكات VPN:

١. الوصول عن بعد إلى VPN (المعروف أيضًا باسم VPN من عميل إلى موقع)
٢. VPN من موقع إلى موقع
٣. تطبيقات VPN للهواتف المحمولة
٤.

١. الوصول عن بعد إلى VPN (المعروف أيضًا باسم VPN من العميل إلى الموقع)

أحد أكثر أنواع VPN المستخدمة على نطاق واسع للكمبيوتر، وهو VPN للوصول عن بعد، يمنح المستخدمين خارج الموقع القدرة على الاتصال بشبكة المؤسسة، أو خادم بعيد، من أجهزتهم الشخصية. ويمكن تحقيق ذلك عن طريق إدخال بيانات اعتماد المصادقة الخاصة بك عبر صفحة تسجيل الدخول، والتي تسمح لك بعد ذلك بإجراء الاتصال من خلال متصفح الويب الخاص بك. ويمكن استخدام شبكة VPN للوصول عن بعد للاستخدام المهني والشخصي، ولهذا السبب فهي أحد أكثر أشكال VPN شيوعًا. فهو يمنح العاملين عن بعد القدرة على الوصول إلى ملفات الشركة ومواردها دون الحاجة إلى التواجد في المكتب، كما أنه يحمي البيانات الخاصة للشركات التي تعمل عن بعد أولاً بحيث أن تظل خاصة. أما بالنسبة للمستخدمين الأفراد الذين يرغبون ببساطة في تصفح الإنترنت العام بمزيد من الاستقلالية وعدم الكشف عن هويتهم، فإن شبكة VPN للوصول عن بعد تعد جزءًا لا يتجزأ من تجنب حظر المحتوى وجدران الحماية وتتبع مزود خدمة الإنترنت.

٢. VPN من موقع إلى موقع

قد تختار المؤسسات الكبيرة التي تحتاج إلى امان أكثر قوة شبكات VPN من موقع إلى موقع. شبكة VPN من موقع إلى موقع هي شبكة داخلية خاصة تتألف من شبكات متعددة داخل المؤسسة، والتي ترتبط ببعضها البعض بشبكات المنطقة المحلية (LANs) من خلال الإنترنت العام. ويتيح هذا الإعداد للمستخدمين عبر شبكتين منفصلتين، سواء داخل المؤسسة أو بالقرب منها، مشاركة الموارد مع بعضهم البعض مع الاستمرار في تقييد الوصول الكامل إلى جميع مواردهم، مما يضمن بقاء الاتصال داخل الشركة خاصًا وآمنًا قدر الإمكان. نظرًا لحجم وتعقيد شبكات VPN من موقع إلى موقع، فإن هذا النوع من الاتصال هو الأنسب للشركات على مستوى المؤسسة التي لديها أقسام عبر مواقع متعددة.

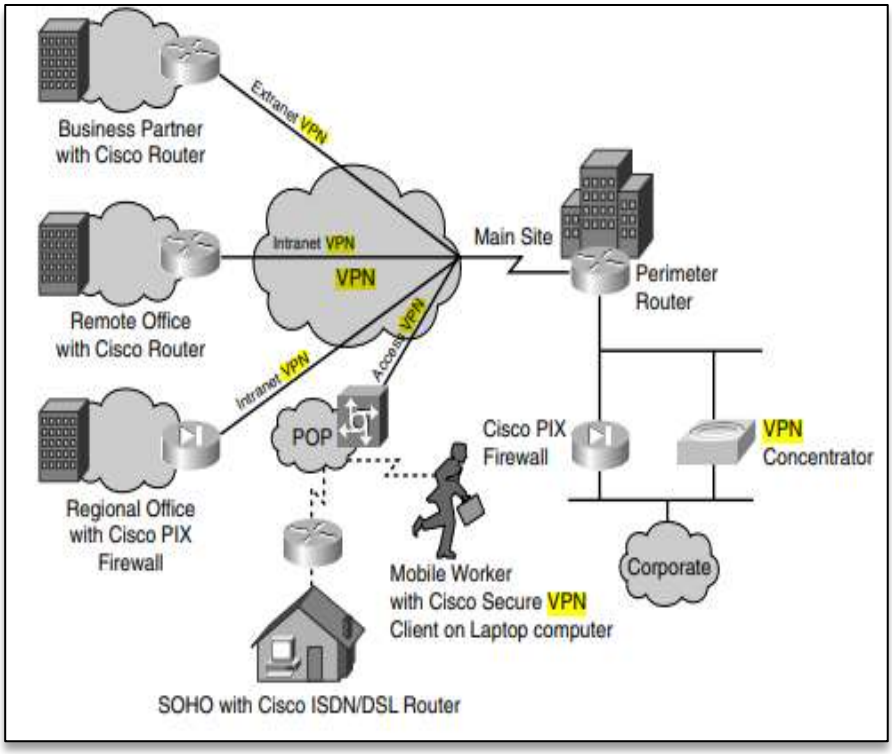
ضمن شبكات VPN من موقع إلى موقع، هناك نوعان من الشبكات:

- الشبكة الداخلية (Intranet VPN)

تقوم شبكة VPN من موقع إلى موقع على الإنترانت بربط عدة مواقع من نفس المؤسسة معًا عن طريق شبكة LAN. يكون هذا مفيدًا عندما تحتاج أقسام متعددة عبر مواقع متعددة إلى التعاون مع بعضها البعض داخل شبكة خاصة مغلقة. ومن خلال الاتصال من موقع إلى موقع، يمكن لهذه الأقسام تبادل الموارد مع بعضها البعض بشكل آمن وفعال.

- الشبكة الخارجية (Extranet VPN)

تربط شبكة VPN من موقع إلى موقع إكسترانت عدة مواقع من مؤسسات مختلفة معًا عن طريق شبكة LAN. قد تحتاج المؤسسة التي تتعاون بشكل متكرر مع الموردين أو الشركاء أو بائعي الأعمال الخارجيين إلى القدرة على تشكيل هذه الشبكة. يمكن للمؤسسات أيضًا تخصيص نطاق الوصول بين كل شبكة، بحيث تتم مشاركة بعض الموارد فقط، بينما تظل الموارد الأخرى خاصة. توضح الصورة (٢) الفرق بينهم.



صورة (٢): الفرق بين شبكات VPN من موقع إلى موقع

٣. تطبيقات VPN للهواتف المحمولة

في حين أن موفري VPN منذ فترة طويلة يلبون احتياجات مستخدمي سطح المكتب، فقد حفزت الهواتف الذكية زيادة كبيرة في النمو بين شبكات VPN للجوال - ولسبب وجيه. بالنسبة لمستخدمي الهواتف الذكية الذين يبحثون عن قدر أكبر من الأمان والحماية أثناء التنقل، تعد شبكة VPN المحمولة أمرًا ضروريًا.

لا توفر شبكات VPN المحمولة فوائد شبكة VPN التقليدية فحسب، بل تستمر أيضًا في حماية البيانات عندما يكون الاتصال بالإنترنت متقطعًا أو غير مستقر، أو عند التبديل بين بيانات الهاتف المحمول وشبكة Wi-Fi. وطالما أن التطبيق قيد التشغيل، يظل اتصال VPN آمنًا، ويظل جهازك محميًا. نظرًا للمرونة، وتعد شبكة VPN المحمولة مثالية للمستخدمين الذين يسافرون، أو لأولئك الذين لا يستطيعون الوصول إلى اتصال إنترنت موثوق.

- **تتمتع شبكات VPN بالمزايا التالية:**

١. يساعد استخدام (VPN) على حماية بيانات الشبكة ومواردها.
٢. يوفر (VPN) سهولة الوصول وسهولة استخدام موظفي الشركات للشبكة الخاصة عن بعد لأنهم سيتمكنون من الوصول بسهولة إلى موارد المكتب الرئيسية دون الحاجة إلى أن يكونوا بداخل الشركة، ومع ذلك، يتم الحفاظ على أمن الشبكة الخاصة ومواردها.
٣. يوفر الاتصال باستخدام (VPN) مستوى أعلى من الأمان مقارنة بأساليب الاتصال الأخرى عن بعد.
٤. المواقع الجغرافية للمستخدمين محمية ولا تتعرض للشبكات العامة أو المشتركة مثل الإنترنت.
٥. تسمح (VPN) بإضافة مستخدمين جدد أو مجموعة مستخدمين جدد دون الحاجة إلى مكونات إضافية أو تكوين معقد.

❖ IPsec (Internet Protocol Security)

IPsec اختصار لـ IP Security، وهو عبارة عن مجموعة من البروتوكولات والمعايير والخوارزميات لتأمين حركة مرور البيانات عبر شبكة غير موثوقة، مثل الإنترنت. ولذلك، فإن الغرض الرئيسي من IPsec هو تحقيق الركائز الثلاثة لأمن المعلومات والتي تعرف باسم "CIA TRIAD":

١. السرية – تمنع سرقة البيانات باستخدام خوارزميات التشفير (AES، 3DES، DES، وBlowfish).
٢. النزاهة – تضمن عدم التلاعب بالبيانات أو تغييرها أثناء الإرسال، باستخدام خوارزمية التجزئة (HMAC-MD، HMAC-SHA1٥).
٣. المصادقة – التأكد من هوية الذي يرسل البيانات باستخدام (المفاتيح المشتركة مسبقًا، التوقيعات الرقمية RSA).

وعادةً، يتم إرسال البيانات بنص واضح ولتشفيرها بواسطة أي من خوارزميات التشفير المذكورة سابقاً، نحتاج إلى مفاتيح، وهنا يظهر دور (D-H Diffie-Hellman) وهو المسؤول عن توليد المفاتيح التي تستخدم للتشفير وفك تشفير البيانات. هناك عدة مجموعات D-H تتحكم في قوة وطول المفتاح: -

المجموعة ١ - ٧٦٨ بت.

المجموعة ٢ – ١٠٢٤ بت.

المجموعة ٥ - ٢٠٤٨ بت.

- **بروتوكولات IPsec**

يستخدم IPsec أحد رأسي البروتوكولات "Protocol Headers" لتأمين البيانات:

١. رأس المصادقة (AH) يوفر ويدعم خدمات المصادقة والتكامل ولا يقوم بتشفير أي بيانات على الإطلاق.
٢. حمولة أمان التغليف (ESP) يوفر ويدعم كافة الخدمات السرية والمصادقة والنزاهة

تشرح الصورة ٣ تفاصيل رأسي بروتوكول IPsec.

- **IPsec Modes**

يمكن أن يعمل كل بروتوكول IPSEC (AH أو ESP) في أحد الوضعين:

١. وضع النقل (Transport mode) – يتم ترك عناوين IP الأصلية سليمة يستخدم عند تأمين الاتصال من جهاز إلى آخر.
٢. وضع النفق (Tunnel mode) – يتم تجزئة الحزمة الأصلية بالكامل و/أو تشفيرها، ويتم تطبيق عنوان IP مؤقت على الحزمة أثناء النقل.

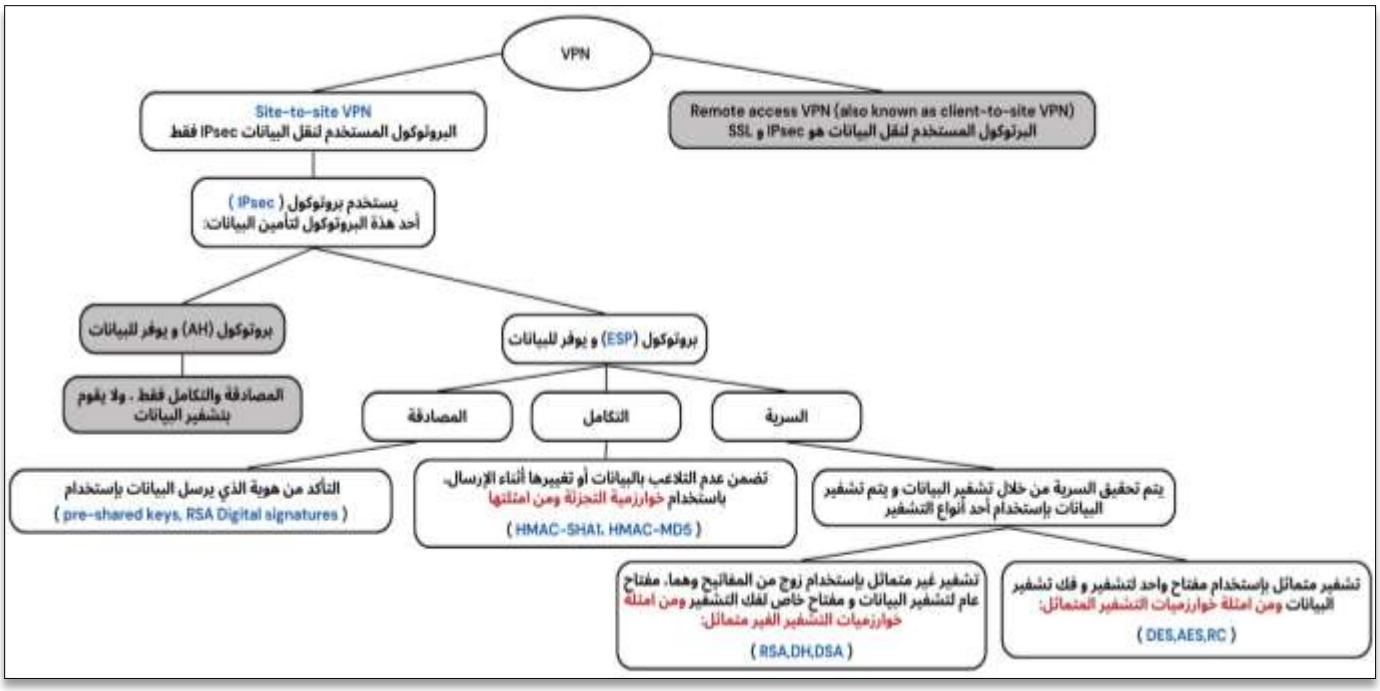
يقوم IPSEC VPN بإنشاء "اقتران" أو "اتصال" أو "سياسة" بين نقطتي بداية ونهاية نفق الـ VPN. نفق الـ VPN هو نفق افتراضي أحادي الاتجاه بين أقران VPN؛ وبالتالي، لكي يحدث اتصال كامل بينهم، يجب إنشاء واحد لكل اتجاه. ونحتاج هنا إلى وجود سياسة IKE مُحددة في كل نظير ليتم التفاوض عليها بواسطة بروتوكول IKE مع النظير البعيد والتأكد من مطابقتها.

تحدد سياسة IKE عدة معلمات، بما في ذلك:

- خوارزمية التشفير (مثل DES أو ٣DES أو AES).
- خوارزمية التجزئة (مثل ٥MD أو ١-SHA).
- طريقة المصادقة مثل المفاتيح المشتركة أو توقيعات RSA (Digital signature - RSA) او pre-shared keys).
- مجموعة DH (Diffie-Hellman) لإنشاء المفاتيح ومشاركتها.

وتسمى هذه الخطوة المرحلة الأولى وتتكون من سياسات/مفاوضات متفق عليها لنفق تبادل مفاتيح الإنترنت (IKE) حول كيفية مصادقة القناة وتأمينها ويتبادل المشاركون المقترحات الخاصة بخدمات أمنية مقبولة للطرفين.

بعد أن ينشئ المشاركون قناة آمنة وموثقة، ينتقلون إلى المرحلة الثانية، حيث يتفاوضون على الارتباطات الأمنية لتأمين البيانات التي سيتم نقلها عبر نفق IPsec.



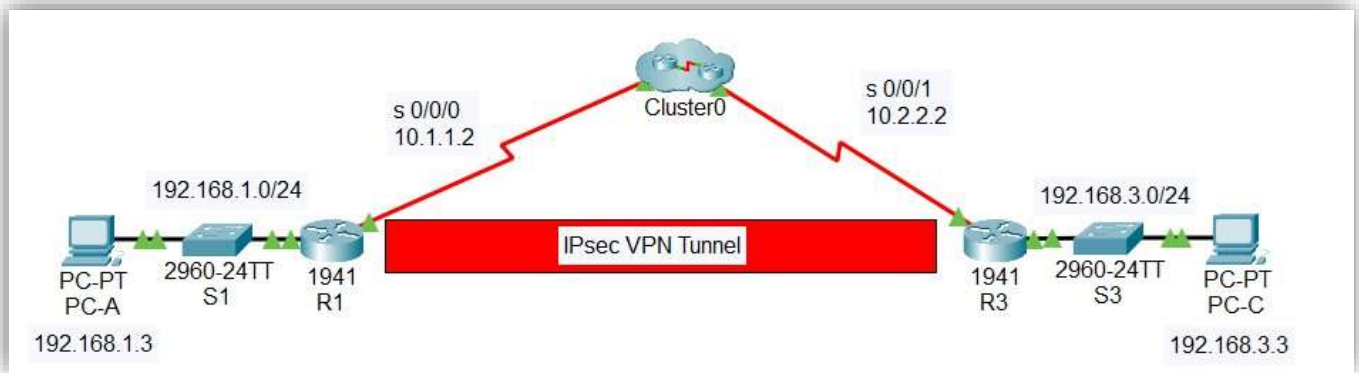
صورة (٣): تفاصيل رأسي بروتوكول IPsec

❖ تنفيذ IPsec VPN موقع لموقع (الجزء العملي)

الاهداف:

- التحقق من الاتصال عبر الشبكة.
- قم بتكوين كل من R3,R1 لدعم شبكة IPsec VPN من موقع إلى موقع

هيكل الشبكة Topology:



رابط الوصول الى ملف الشبكة

ملف الجزء العملي لمقرر امن شبكات الحاسب المتقدم

جدول العناوين:

- تم تعيين العناوين مسبقا كما هو موضح بالجدول التالي:

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

جدول Policy Parameters

- المرحلة الأولى من ISAKMP (ISAKMP Phase 1 Policy Parameters)

Parameters		R1	R3
Key Distribution Method	Manual or **ISAKMP**	**ISAKMP**	**ISAKMP**
Encryption Algorithm	**DES**, 3DES, or AES	AES 256	AES 256
Hash Algorithm	MD5 or **SHA-1**	**SHA-1**	**SHA-1**
Authentication Method	Pre-shared keys or **RSA**	pre-share	pre-share
Key Exchange	DH Group 1, 2, or 5	DH 5	DH 5
IKE SA Lifetime	86400 seconds or less	**86400**	**86400**
ISAKMP Key		vpnpa55	vpnpa55

- المرحلة الثانية من IPsec (IPsec Phase 2 Policy Parameters)

Parameters	R1	R3
Transform Set Name	VPN-SET	VPN-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	10.2.2.2	10.1.1.2
Traffic to be Encrypted	access-list 110 (source 192.168.1.0 dest 192.168.3.0)	access-list 110 (source 192.168.3.0 dest 192.168.1.0)
Crypto Map Name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

الخلفية / السيناريو:

تُظهر طوبولوجيا الشبكة ثلاثة أجهزة توجيه. مهمتك هي تكوين R1 وR3 لدعم شبكة IPsec VPN من موقع إلى موقع عندما تتدفق حركة المرور بين شبكات LAN الخاصة بكل منهما. يمتد نفق IPsec VPN من R1 إلى R3 عبر R2. يعمل R2 بمثابة ممر وليس لديه معرفة بشبكة VPN. يوفر IPsec نقلاً آمنًا للمعلومات الحساسة عبر شبكات غير محمية، مثل الإنترنت.

تم تكوين أجهزة التوجيه مسبقًا بما يلي:

كلمة المرور لخط وحدة التحكم (للدخول إلى المستوى الأول)	تمكين كلمة المرور للدخول إلى المستوى الثاني بعد كتابة أمر Enable
123	1234

الجزء الأول: تكوين IPsec على R1

الخطوة ١: تمكين حزمة تقنية الأمان.

- قم بإصدار الأمر version show لعرض معلومات ترخيص حزمة Technology Security على R1 .

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      disable       None          None
data          disable       None          None

Configuration register is 0x2102
```

- إذا لم يتم تمكين حزمة تقنية الأمان، استخدم الأمر التالي لتمكين الحزمة:

```
R1(config)# license boot module c1900 technology-package securityk9
```

- قبول اتفاقية ترخيص المستخدم النهائي

```
ACCEPT? [yes/no]: yes
```

- احفظ التكوين قيد التشغيل run-config باستخدام الامر التالي:

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

- أعد تحميل جهاز التوجيه لتمكين ترخيص الأمان باستخدام امر reload.

```
R1#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

____________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
################################################################################ [OK]
```

- تحقق من تمكين حزمة Technology Security باستخدام الأمر **version .show**

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

الخطوة ٢: قم بتكوين سياسة ISAKMP للمرحلة الأولى من IKE على R1.

- قم بتكوين خصائص ISAKMP policy 10 للتشفير على R1 مع مفتاح التشفير المشترك vpnpa55. ارجع إلى جدول المرحلة الأولى لـ ISAKMP للتعرف على القيم المحددة المطلوب تكوينها.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2
```

ملاحظة: أعلى مجموعة DH مدعومة بواسطة Packet Tracer هي group 5

الخطوة ٣: قم بتكوين سياسة IPsec للمرحلة الثانية من IKE على R1.

- قم بإنشاء transrorm-set وتسميتها بـ VPN-SET مع استخدام القيم والمعطيات الموضحة في جدول parameters policy الخاص بالمرحلة الثانية.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

الخطوة ٤: قم بإنشاء MAP على R1.

- أولاً يجب تكوين ACL 110 مع تحديد حركة المرور من الشبكة المحلية (LAN) على R1 إلى الشبكة المحلية (LAN) على R3

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

- قم بإنشاء خريطة التشفير VPN-MAP التي تربط جميع الـ parameters للمرحلة الثانية معًا. استخدم رقم التسلسل 10 وقم بتعريفه كخريطة من نوع ipsec-isakmp.

```
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

الخطوة ٥: قم بتكوين خريطة التشفير على الواجهة الصادرة.

- قم بربط خريطة تشفير VPN-MAP بالواجهة التسلسلية Serial 0/0/0

```
R1(config)# interface s0/0/0
R1(config-if)# crypto map VPN-MAP
```

الجزء الثاني: تكوين IPsec على R3

الخطوة ١: تمكين حزمة تقنية الأمان.

- في R3، قم بإصدار الأمر show version للتحقق من تمكين معلومات ترخيص حزمة Technology Security

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None

Configuration register is 0x2102
```

ملاحظة: بناء على معلومات ترخيص الحزمة Security فقد تم تكوين حزمة تقنية الأمان مسبقا في هذا الراوتر.

الخطوة ٢: قم بتكوين سياسة ISAKMP للمرحلة الأولى من IKE على R3

- قم بتكوين خصائص ISAKMP policy 10 للتشفير على R3 مع مفتاح التشفير المشترك vpnpa55. ارجع إلى جدول المرحلة الأولى لـ ISAKMP للتعرف على القيم المحددة المطلوب تكوينها.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2
```

الخطوة ٣: قم بتكوين سياسة IPsec للمرحلة الثانية من IKE على R3.

- قم بإنشاء transrorm-set وتسميتها بـ VPN-SET مع استخدام القيم والمعطيات الموضحة في جدول parameters policy الخاص بالمرحلة الثانية

```
R3(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

الخطوة ٤: قم بإنشاء خريطة MAP على R3.

- أولاً يجب تكوين ACL 110 مع تحديد حركة المرور من الشبكة المحلية (LAN) على R3 إلى الشبكة المحلية (LAN) علىR1

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

- قم بإنشاء خريطة التشفير VPN-MAP التي تربط جميع الـ parameters للمرحلة الثانية معًا. استخدم رقم التسلسل 10 وقم بتعريفه كخريطة من نوع ipsec-isakmp.

```
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

الخطوة ٥: قم بتكوين خريطة التشفير على الواجهة الصادرة.

- قم بربط خريطة تشفير VPN-MAP بالواجهة التسلسلية Serial 0/0/1

```
R3(config)# interface s0/0/1
R3(config-if)# crypto map VPN-MAP
```

الجزء الثالث: التحقق من IPsec VPN

الخطوة ١: التحقق من النفق قبل حركة المرور المثيرة للإهتمام.

- قم بإصدار الأمر **show crypto ipsec sa** على R1 لاحظ أن عدد الحزم

(encapsulated , encrypted , decapsulated , decrypted) كلها مضبوطة على ٠

```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 1.2.2.2 port 500
    PERMIT, flags={origin is acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:1.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
```

الخطوة ٢: إنشاء حركة مرور مثيرة للاهتمام .

- اختبار اتصال PC-C من PC-A

```
C:\> ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=15ms TTL=126
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126
Reply from 192.168.1.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 15ms, Average = 6ms
```

الخطوة ٣: التحقق من النفق بعد حركة المرور المثيرة للاهتمام.

- على R1، أعد إصدار الأمر **show crypto ipsec sa**

لاحظ أن عدد الحزم أكثر من ٠، مما يدل على أن نفق IPsec VPN يعمل.

```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:1.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
```

الخطوة ٤: إنشاء حركة مرور غير مثيرة للاهتمام.

- اختبار اتصال PC-B منPC-A

ملاحظة: إصدار اختبار ping من جهاز التوجيه R1 إلى PC-C أو R3 إلى PC-A لا يمثل حركة مرور مثيرة للاهتمام.

```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=16ms TTL=126
Reply from 192.168.2.3: bytes=32 time=12ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 7ms
```

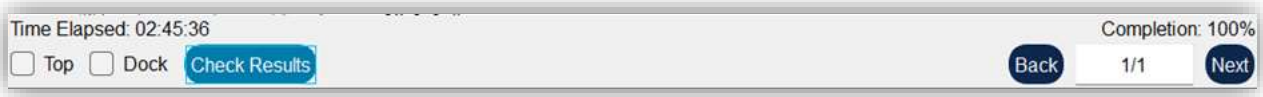
الخطوة ٥: التحقق من النفق.

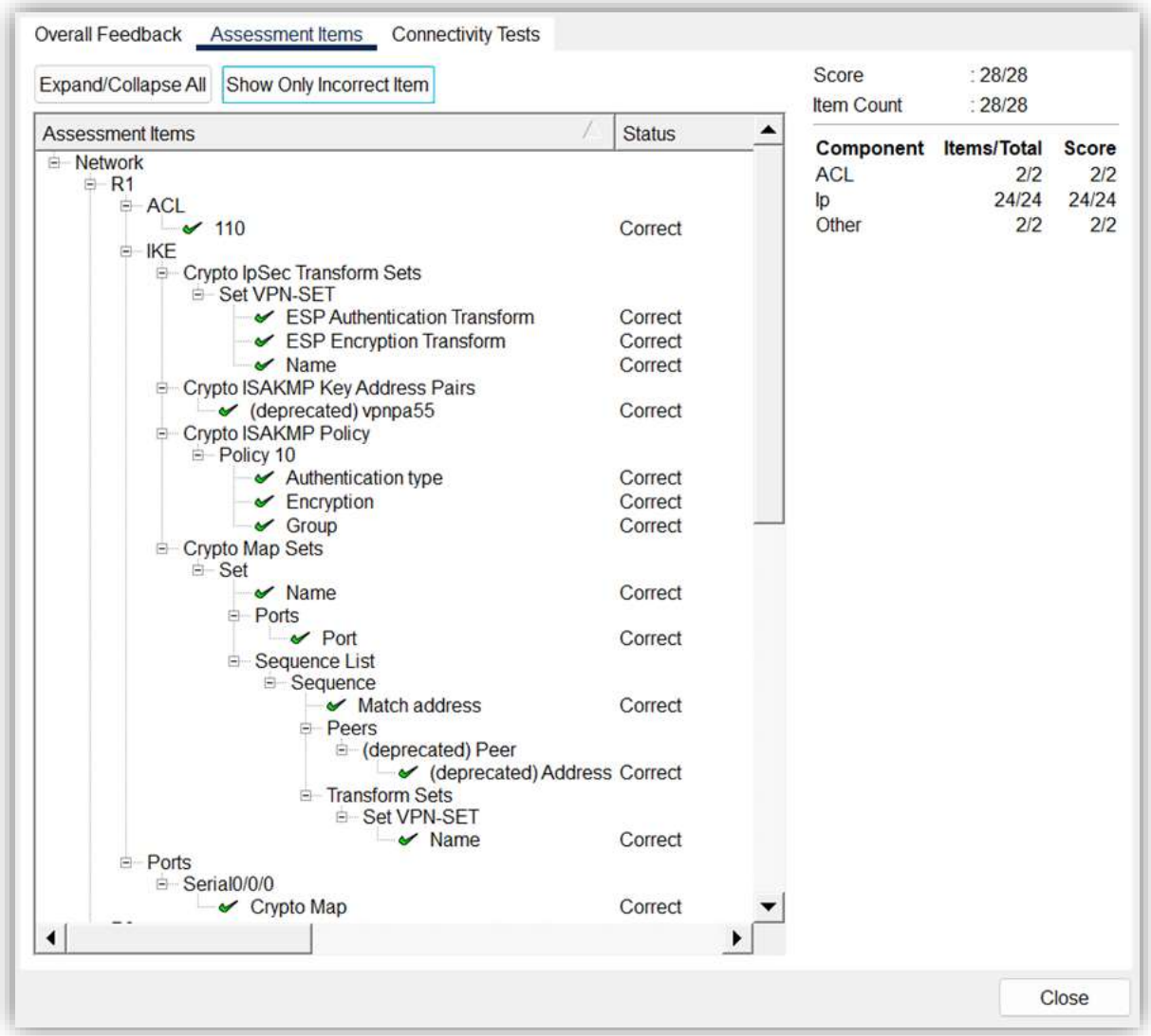
- على R1، أعد إصدار الأمر **show crypto ipsec sa**.

لاحظ أن عدد الحزم لم يتغير الذي يتحقق من عدم تشفير حركة المرور غير المثيرة لاهتمام.

```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:1.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
```

الخطوة ٦: التحقق من النتائج.




Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Only Incorrect Item
Assessment Items
Status
Network
R1
ACL
110
Correct
IKE
Crypto IpSec Transform Sets
Set VPN-SET
ESP Authentication Transform
Correct
ESP Encryption Transform
Correct
Name
Correct
Crypto ISAKMP Key Address Pairs
(deprecated) vpnpa55
Correct
Crypto ISAKMP Policy
Policy 10
Authentication type
Correct
Encryption
Correct
Group
Correct
Crypto Map Sets
Set
Name
Correct
Ports
Port
Correct
Sequence List
Sequence
Match address
Correct
Peers
(deprecated) Peer
(deprecated) Address
Correct
Transform Sets
Set VPN-SET
Name
Correct
Ports
Serial0/0/0
Crypto Map
Correct
Score : 28/28
Item Count : 28/28
Component Items/Total Score
ACL 2/2 2/2
Ip 24/24 24/24
Other 2/2 2/2
Close

ملخص الأوامر:

Router 1
R1(config)#license boot module c1900 technology-package securityk9 R1#copy running-config startup-config R1#reload R1(config)#crypto isakmp policy 10 R1(config-isakmp)#encryption aes 256 R1(config-isakmp)#authentication pre-share R1(config-isakmp)#group 5 R1(config-isakmp)#exit R1(config)#crypto isakmp key vpnpa55 address 10.2.2.2 R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac R1(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 R1(config)#crypto map VPN-MAP 10 ipsec-isakmp R1(config-crypto-map)#description VPN connection to R3 R1(config-crypto-map)#set peer 10.2.2.2 R1(config-crypto-map)#set transform-set VPN-SET R1(config-crypto-map)#match address 110 R1(config-crypto-map)#exit R1(config)#interface s0/0/0 R1(config-if)#crypto map VPN-MAP

Router 3
R3(config)#crypto isakmp policy 10 R3(config-isakmp)#encryption aes 256 R3(config-isakmp)#authentication pre-share R3(config-isakmp)#group 5 R3(config-isakmp)#exit R3(config)#crypto isakmp key vpnpa55 address 10.1.1.2 R3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 R3(config)#crypto map VPN-MAP 10 ipsec-isakmp R3(config-crypto-map)#description VPN connection to R1 R3(config-crypto-map)#set peer 10.1.1.2 R3(config-crypto-map)#set transform-set VPN-SET R3(config-crypto-map)#match address 110 R3(config-crypto-map)#exit R3(config)#interface s0/0/1 R3(config-if)#crypto map VPN-MAP

رابط شرح لتنفيذ المعمل:

(تنفيذ **IPsec VPN**) من موقع لموقع

❖ ملخص

IPSec هو وظيفة برمجية لتشفِّر البيانات لحماية محتواها من الأطراف غير المصرَّح لها ، تُشفر البيانات بواسطة مفتاح تشفير، ويلزم وجود مفتاح فك تشفير لفك تشفير المعلومات ، يدعم IPSec أنواعًا مختلفة من التشفير، بما في ذلك AES و Blowfish و Triple DESو ChaChaو DES-CBC.

يستخدم IPSec التشفير غير المتماثل والمتماثل لتوفير السرعة والأمان في أثناء نقل البيانات، في التشفير غير المتماثل، يصبح مفتاح التشفير عامًا بينما يظل مفتاح فك التشفير خاصاً، يستخدم التشفير المتماثل المفتاح العام نفسه لتشفير البيانات وفك تشفيرها، ينشئ IPSec اتصالاً آمنًا مع التشفير غير المتماثل ويتحول إلى التشفير المتماثل لتسريع نقل البيانات.

❖ أسئلة المراجعة

١. شبكة الوصول عن بعد الى VPN تعرف أيضاً باسم VPN من موقع الى موقع.

أ- خطأ

ب- صح

٢. ..... هي شبكة خاصة يتم إنشاؤها داخل نطاق البنية التحتية للشبكة العامة مثل الإنترنت العالمية:

أ- الشبكة الافتراضية الخاصة (VPN)

ب- الشبكة العنكبوتية

ت- الشبكة الكهربائية

ث- الشبكة الاجتماعية

٣. يوفر الاتصال باستخدام (VPN) مستوى أعلى من الأمان مقارنة بأساليب الاتصال الأخرى عن بعد.

أ- خطأ

ب- صح

٤. ..... تضمن عدم التلاعب بالبيانات أو تغييرها أثناء الإرسال.

أ- السرية

ب- النزاهة

ت- المصادقة

ث- لا شيء مما ذكر

٥. يستخدم IPsec أحد رأسي البروتوكولات "Protocol Headers" لتأمين البيانات ، حيثُ أن ..... يوفر ويدعم خدمات المصادقة والتكامل ولا يقوم بتشفير أي بيانات على الإطلاق.

أ- رأس المصادقة (AH)

ب- حمولة أمان التغليف (ESP)

ت- خوارزمية (RSA)

ث- خوارزمية (DES)

٦. يقوم IPsec VPN بإنشاء "اقتران" أو "اتصال" أو "سياسة" بين نقطتي بداية ونهاية نفق الـ VPN.

أ- خطأ

ب- صح

٧. نفق الـ VPN هو نفق حقيقي بين أقران VPN.

أ- خطأ

ب- صح

٨. تسمح شبكات (VPN) بإضافة مستخدمين جدد أو مجموعة مستخدمين جدد دون الحاجة إلى مكونات إضافية أو تكوين معقد.

أ- خطأ

ب- صح

٩. الغرض الرئيسي من IPsec هو تحقيق الركائز الثلاثة لأمن المعلومات والتي تعرف باسم "CIA TRIAD"

أ- خطأ

ب- صح

١٠. يساعد الامر الأمر show version في:

أ- معرفة إصدار الجهاز

ب- إنشاء نفق VPN

ت- تكوين سياسة ISAKMP

ث- تكوين سياسة IPsec

الفصل الثالث

تنفيذ ASA

في هذا الفصل سنتعرف على المواضيع التالية:

- ❖ مقدمة
  - ○ شبكة جدران الحماية
  - ○ أنواع جدران الحماية Firewall
- ❖ مقدمة في AAA
  - ○ Cisco ASA 5505 Model
- ❖ مصادقة محلية عن طريق AAA
  - ○ بروتوكولات AAA والخدمات التي تدعمها Cisco ASA
- ❖ إعدادات جدار الحماية AAA
  - ○ الوصول إلى أجهزة Cisco ASA
- ❖ تكوين إعدادات جهاز AAA الأساسية باستخدام CLI (الجزء العملي)
  - ○ الجزء الاول: التحقق من الاتصال واستكشاف جهاز ASA
  - ○ الجزء الثاني: تكوين إعدادات ASA وأمان الواجهة باستخدام واجهة سطر الأوامر (CLI)
  - ○ الجزء الثالث: تكوين الواجهات الداخلية والخارجية.
  - ○ الجزء الرابع: استخدم أوامر التحقق للتحقق من الاعدادات التي تم إنشاؤها.
- ❖ ملخص
- ❖ أسئلة المراجعة

❖ مقدمة

يعد الفهم التفصيلي لكيفية عمل جدران الحماية والتقنيات ذات الصلة أمراً بالغ الأهمية لجميع محترفي أمان الشبكات، تساعدك هذه المعرفة على تكوين وإدارة أمان شبكاتك بدقة وفعالية، الكلمة جدار الحماية يصف عادةً الأنظمة أو الأجهزة التي يتم وضعها بين شبكة موثوق بها وأخرى غير موثوق بها.
توفر العديد من حلول جدار حماية الشبكة فرضًا لسياسة المستخدم والتطبيق التي توفر الحماية لأنواع مختلفة من التهديدات الأمنية، غالبًا ما يقدمون تسجيل القدرات التي تمكن مسؤولي الأمن من تحديد هذه التهديدات والتحقيق فيها والتحقق منها ومعالجتها.

بالإضافة إلى ذلك، يمكن تشغيل العديد من تطبيقات البرامج على نظام لحماية هذا المضيف فقط تُعرف هذه الأنواع من التطبيقات بجدران الحماية الشخصية personal firewalls .

• شبكة جدران الحماية:

توفر جدران الحماية المستندة إلى الشبكة الميزات الرئيسية المستخدمة لأمن المحيط الابتدائي تتمثل مهمة جدار حماية الشبكة في رفض أو السماح بحركة المرور التي تحاول الدخول إلى الشبكة بناءً على سياسات وقواعد محددة مسبقًا، العمليات المستخدمة للسماح أو الحظر قد تشمل حركة المرور ما يلي:

- تقنيات ترشيح الحزمة البسيطة
- وكلاء تطبيق متعدد الأوجه
- أنظمة التفتيش الحكومية
- ترجمة عنوان الشبكة

• أنواع جدران الحماية Firewall

هناك ٥ أنواع أساسية لجدار الحماية، وجميع تلك الأنواع تعمل على منع الهجمات الضارة، ولكن يختلف أسلوب تشغيل كل نوع في تكوينه وكذلك في طريقتك بصد الهجمات الضارة، وبالتالي فإن الأنواع يمكن تقسيمها إلى ما يلي:

١. Packet Filtering Firewalls

يأتي هذا النوع من أقدم أنواع Firewall، ومن أفضل الأنواع التي يمكن أن تعتمد عليها لسرعتها وجودتها في فحص الاتصالات، حيث تشكل نقطة تفتيش خارجية، تقوم بجمع جميع المعلومات الصادرة من الخادم من رقم IP، ونوع الاتصال، ورقم بوابة الوصول وغير ذلك.

بعد ذلك يقوم بمقارنتهم بالمعايير الأمنية الخاصة به، وإذا اجتازوا هذا التحليل يقوم بالسماح بالاتصال المباشر، ولكن إذا لم يجتازوا هذه العملية من التحليل يتم منع جهات الاتصال من إتمام الاتصال بالشبكة.

٢. Proxy Firewalls

يأتي Proxy Firewalls من أنواع جدران الحماية القديمة أيضًا ويعرف باسم جدار الحماية الوسيط، وهو وسيط بين الشبكات الداخلية والخارجية والإنترنت كما يوحي الاسم.

على سبيل المثال إذا قمت بالبحث في جوجل عن معنى جدار الحماية، فسيقوم جهازك بطلب معلومات من خادم جوجل بشكل مباشر، ولكن عند استخدام Proxy Firewalls فسيقوم بالحصول على هذا الطلب وإعادة توجيه على أساس أنه صادر منه وليس من الجهاز مباشرًا، وبالتالي لا يستطيع خادم جوجل معرفة هوية جهازك الحقيقة أو موقعك الجغرافي أو جمع أي معلومات عنك لأن المعلومات التي سيحصل عليها ستكون من الوسيط الوهمي.

٣. Next-generation Firewalls

يعرف باسم جدار حماية من الجيل الثاني ويرمز له في أغلب المراجع باختصار (NGFW)، وهو من أفضل جدران الحماية التي تعتمد عليه الكثير من الشركات الكبرى.

يقوم هذا البروتوكول بفحص الاتصالات الصادرة والواردة من الإنترنت بشكل أعمق حيث يقوم بفحص جميع الاتصالات الواردة من الخادم، ويحتوي على بعض التقنيات الحديثة مثل تقنية IPS التي تقوم بحمايتك من الفيروسات والهجمات الضارة وتصفية البريد العشوائي بشكل تلقائي.

٤. Circuit-Level Gateway

هو جدار حماية تقليدي وسريع جداً ولا يستهلك جزء كبير من موارد الجهاز الأساسية عند العمل، حيث ويعتمد على تشكيل بوابات تقوم بفحص بروتوكول TCP، وهو بروتوكول يستخدم في نقل البيانات عبر الشبكات والتأكد من مطابقتها للمعايير الأمنية الخاصة به.

٥. Stateful Inspection Firewalls

يعرف باسم جدار الحماية التفتيشي، وهو نوع من أنواع Firewall التقليدي أيضًا، حيث يقوم بمراقبة حركة المرور الصادرة والواردة ويقوم بتصفيتها بشكل تلقائي بناءًا على القواعد الأمنية المُعدة بشكل مسبق من المستخدم، ولكن يتميز بمراقبة الاتصال من اللحظة الأولى من الاتصال حتى إغلاق الموقع بالكامل.

يعتمد هذا الأسلوب على التصفيات الناتجة من الاتصالات القديمة لنفس الخادم في منع الاتصالات الحديثة، لذلك يجب تحديثه بشكل مستمر، ويقوم بفحص بروتوكول TCP أيضًا، لذلك فهو يشكل حماية قوية جداً، إلا أنه يستهلك جزء كبير من موارد الجهاز الأساسية عند الفحص مما يسبب بطء في نقل البيانات عبر الشبكات.

❖ مقدمة في ASA

Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance

تدمج أجهزة الأمان التكيفية Cisco ASA 5500 Series جدار الحماية و IPS و إمكانيات VPN، فهي توفر حلاً متعدد الإمكانات لشبكتك ، دمج كل شيء في Cisco ASA تؤمن الشبكة دون الحاجة إلى تراكب إضافي من المعدات أو تعديلات الشبكة ، هذا شيء طلبه العديد من عملاء Cisco ومحترفي العمل على الإنترنت في منتج أمان.

هناك العديد من طرازات Cisco ASA 5500 Series وتشمل هذه:

■ Cisco ASA 5505 ■ Cisco ASA 5510 ■ Cisco ASA 5520 ■ Cisco ASA 5540■
Cisco ASA 5550 ■ Cisco ASA 5580-20 ■ Cisco ASA 5580-40

- ### Cisco ASA 5505 Model

تم تصميم Cisco ASA 5505 Adaptive Security Appliance للأعمال الصغيرة، فروع المكتب، وبيئات العمل عن بعد، على الرغم من صغر حجمه، فإنه يوفر جدار الحماية SSLو IPsec VPN والعديد من خدمات الشبكات المتوقعة على جهاز أكبر.

توضح الصورة (٤) المنظر الأمامي لـ Cisco ASA 5505

صورة (٤): المنظر الأمامي لـ Cisco ASA 5505

تحتوي اللوحة الأمامية على المكونات التالية:

١. منفذ USB - محجوز للاستخدام في المستقبل.

٢. مؤشرات LED لنشاط السرعة والارتباط — يحتوي Cisco ASA 5505 على مؤشر سرعة LED ومؤشر نشاط ارتباط منفصل LED لكل من منافذها الثمانية. عندما لا يضيء مؤشر LED للسرعة، فإنه يشير إلى أن حركة مرور الشبكة تعمل تتدفق بسرعة ١٠ ميغابت في الثانية عندما يكون مؤشر LED للسرعة باللون الأخضر يشير إلى أن حركة مرور الشبكة تتدفق بسرعة ١٠٠ ميجابت في الثانية، عندما الارتباط مؤشر LED للنشاط أخضر ثابت يشير إلى أن ارتباط الشبكة الفعلي يعمل؛ عندما تومض يشير إلى وجود نشاط للشبكة.

٣. مؤشر LED للطاقة - أخضر ثابت يشير إلى أن الجهاز قيد التشغيل.

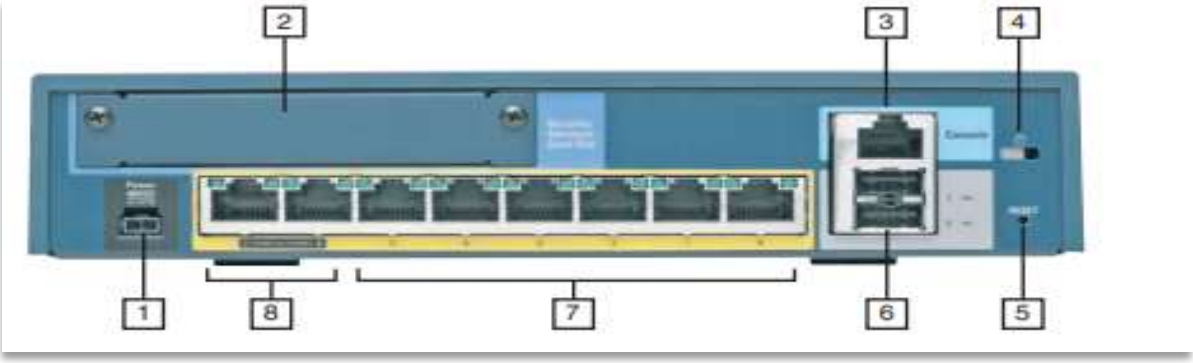
٤. مؤشر LED للحالة - يشير اللون الأخضر الوامض إلى أن النظام قيد التشغيل وأن اختبارات تشغيل الطاقة قيد التشغيل، يشير اللون الأخضر الثابت إلى أن اختبارات النظام قد اجتازت والنظام يعمل، يشير الكهرمان الصلب إلى فشل اختبارات النظام.

٥. نشط - يشير اللون الأخضر إلى أن Cisco ASA هذا نشط عند تكوينه من أجل تجاوز الفشل.

٦. VPN يشير اللون الأخضر الثابت إلى أن واحدًا أو أكثر من أنفاق VPN نشطة.

٧. مؤشر LED لبطاقة خدمات الأمان (SSC) - أخضر ثابت يشير إلى أن بطاقة SSC موجود في فتحة SSC. محجوزة للاستخدام في المستقبل.

توضح الصورة (٥) المنظر الخلفي لـ Cisco ASA 5505



صورة (٥): المنظر الخلفي لـ Cisco ASA 5505

تحتوي اللوحة الخلفية على المكونات التالية:

١. موصل الطاقة.

٢. فتحة SSC - محجوزة للاستخدام في المستقبل.

٣. منفذ وحدة التحكم التسلسلي - يمكّنك منفذ وحدة التحكم RJ-45 من الاتصال فعليًا بالجهاز للوصول إلى واجهة سطر الأوامر (CLI) الخاصة به للمبتدئين لوضع الإعدادات.

٤. قفل الجهاز — يُستخدم لقفل Cisco ASA فعليًا.

٥. زر إعادة الضبط — محجوز للاستخدام في المستقبل.

٦. منفذي USB الإصدار ٢,٠ - محجوزان للاستخدام في المستقبل.

٧. منافذ تبديل إيثرنت من ٠ إلى ٥-١٠ / ١٠٠ منافذ تبديل إيثرنت سريعة.

٨. منافذ تبديل إيثرنت ٦ و ٧-١٠ / ١٠٠ منافذ تبديل إيثرنت سريعة مع الطاقة عبر إيثرنت (PoE).

❖ مصادقة محلية عن طريق AAA

توفر **AAA (Authentication, Authorization, and Accounting)** مستوى إضافيًا من الحماية والتحكم في وصول المستخدم، بدلاً من الاعتماد فقط على قوائم الوصول. إذا كنت ترغب في تقييد الوصول إلى الخادم لبعض المستخدمين فقط، وقد لا تكون على علم دائمًا بعناوين IP الخاصة بهم، يمكنك تمكين AAA للسماح فقط للمستخدمين المفوض لهم بالوصول عبر جهاز الأمان. يدعم جهاز الأمان ASA مجموعة متنوعة من أنواع خوادم AAA بالإضافة إلى قاعدة البيانات المحلية المخزنة على الجهاز.

تُمكن AAA جهاز الأمان من التحقق من هوية المستخدم (المصادقة)، وتحديد ما يمكن للمستخدم القيام به (الترخيص)، وتسجيل ما قام به المستخدم (المحاسبة).

Authentication, Authorization, and Accounting

١. المصادقة (**Authentication**) - عملية التحقق من صحة المستخدمين استنادًا إلى هويتهم وبيانات الاعتماد المُعدلة مسبقًا، مثل كلمات المرور والآليات الأخرى مثل الشهادات الرقمية.

٢. التفويض (**Authorization**) - الطريقة التي يقوم بها جهاز الشبكة بتجميع مجموعة من السمات التي تنظم المهام المصرح للمستخدم بأدائها، هذه الصفات تقاس مقابل قاعدة بيانات المستخدم ، يتم إرجاع النتائج إلى جهاز الشبكة إلى تحديد مؤهلات المستخدم وقيوده ، يمكن تحديد موقع قاعدة البيانات هذه محليًا على Cisco ASA أو يمكن استضافته على RADIUS أو TACACS+ (Terminal Access controller System Plus).

٣. المحاسبة (**Accounting**) - عملية جمع معلومات المستخدم وإرسالها إلى AAA يستخدم الخادم لتتبع أوقات تسجيل الدخول (عندما يقوم المستخدم بتسجيل الدخول وتسجيل الخروج) والخدمات التي يصل إليها المستخدمون، يمكن استخدام هذه المعلومات لأغراض الفوترة والتدقيق وإعادة النقل.

بروتوكولات AAA والخدمات التي تدعمها Cisco ASA

يمكن تكوين Cisco ASA للاحتفاظ بقاعدة بيانات مستخدم محلي أو لاستخدام خدمة خارجية للمصادقة، فيما يلي البروتوكولات الأساسية لمصادقة AAA والخوادم المدعومة كمستودعات قاعدة بيانات خارجية:

- RADIUS
- TACACS +
- RSA SecurID (SDI)
- Windows NT
- Kerberos
- بروتوكول الوصول الخفيف إلى الدليل (LDAP)

يوصى باستخدام خادم مصادقة خارجي في عمليات النشر المتوسطة والكبيرة لتحسين قابلية التوسع وإدارة أسهل.

مثال خادم RADIUS (Example) **:**

يتلقى خادم RADIUS طلبات مصادقة المستخدم ويعيد بعد ذلك معلومات التهيئة المطلوبة للعميل (في هذه الحالة ، Cisco ASA) لدعم خدمة محددة للمستخدم ، يقوم خادم RADIUS بذلك عن طريق إرسال الإنترنت سمات فريق المهام الهندسية (IETF) أو السمات الخاصة بالبائع (مصادقة RADIUS السمات المحددة في RFC ٢٨٦٥).

في الصورة (٦) ، يعمل Cisco ASA بمثابة NAS وخادم RADIUS هو Cisco Secure Access Control Server (ACS).

- الخطوة الأولى

يحاول المستخدم الاتصال بـ Cisco ASA (أي الإدارة أو VPN أو Cut-through proxy).

- الخطوة الثانية

يطالب Cisco ASA المستخدم، ويطلب اسم مستخدم وكلمة المرور، يرسل المستخدم بيانات اعتماده إلى Cisco ASA.

- الخطوة الثالثة

يرسل Cisco ASA طلب المصادقة (طلب الوصول) إلى RADIUS Server.

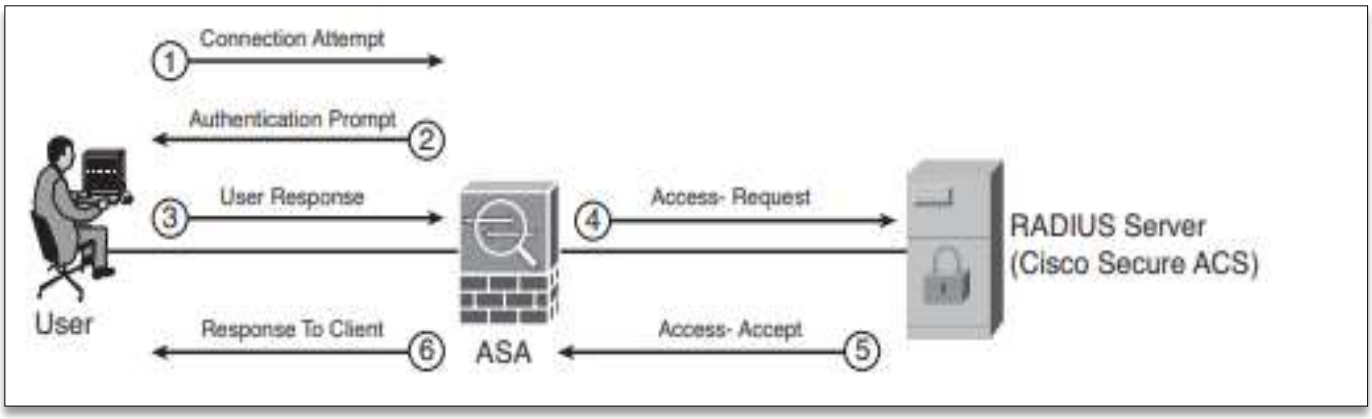
- الخطوة الرابعة

يرسل خادم RADIUS رسالة قبول وصول (إذا نجح المستخدم في مصادقة كاملة) أو رفض وصول (إذا لم ينجح المستخدم).

- الخطوة الخامسة

يستجيب Cisco ASA للمستخدم ويسمح بالوصول إلى خدمة معينة.

ملاحظة يتم إرسال كلمات المرور كرسائل مشفرة من Cisco ASA إلى RADIUS الخادم، هذا مفيد لحماية هذه المعلومات الهامة من الدخلاء Cisco ASA يقوم بتجزئة كلمة المرور، باستخدام السر المشترك المحدد في Cisco ASA و RADIUS Server .



صورة (٦): عمل Cisco ASA بمثابة NAS وخادم RADIUS

❖ إعدادات جدار الحماية ASA

• الوصول إلى أجهزة Cisco ASA

يوفر Cisco ASA نوعين من واجهات المستخدم:

١. واجهة سطر الأوامر (CLI) - توفر واجهة سطر الأوامر (CLI) وصولاً غير رسومي إلى Cisco يمكن الوصول إلى CLI من وحدة تحكم أو Telnet أو جلسة Secure Shell (SSH) .
٢. واجهة مستخدم رسومية (GUI) عبر ASDM — جهاز أمان تكيفي من Cisco

مدير (ASDM) يوفر واجهة رسومية سهلة التنقل وبسيطة لضبطها وإدارة الميزات المختلفة التي توفرها (Cisco Adaptive Security Appliance (ASA.

يتم تجميعها مع مجموعة متنوعة من أدوات الإدارة والمراقبة للتحقق من صحة الجهاز وحركة المرور عبره، يتطلب الوصول إلى ASDM اتصال IP بين عميل ASDM وجهاز الأمان ، اذا أنت لديك جهاز أمان جديد ، يمكنك تعيين عنوان IP الأولي عبر CLI و ثم قم بتأسيس اتصال GUI ASDM.

❖ تكوين إعدادات جهاز ASA الأساسية باستخدام CLI (الجزء العملي)

الأهداف:

- التحقق من الاتصال واستكشاف ASA
- تكوين إعدادات ASA الأساسية ومستويات أمان الواجهة باستخدام واجهة سطر الأوامر (CLI)
- ضبط اعدادات التاريخ والوقت في جهاز ASA.

ما هو جهاز ASA؟

Cisco Adaptive Security Appliance (ASA)

Cisco ASA 5505 هو عبارة عن جدار حماية كامل الميزات لبيئات العمل عن بعد للشركات الصغيرة والفرعية والمؤسسات. إنه يوفر جدار حماية عالي الأداء و SSL و IPsec VPN، وخدمات شبكات غنية في جهاز معياري يعمل فوراً.

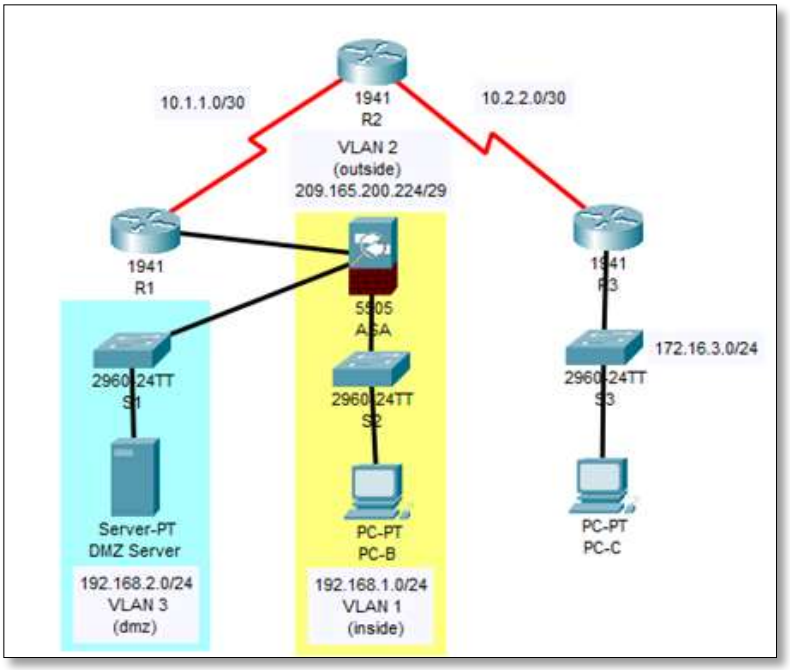
رابط الوصول الى ملف الشبكة

ملف الجزء العملي لمقرر امن شبكات الحاسب المتقدم

السيناريو:

تمتلك شركتك موقعًا واحدًا متصلاً بمزود خدمة الإنترنت. يمثل R1 جهاز CPE يديره مزود خدمة الإنترنت. يمثل R2 جهاز توجيه إنترنت متوسطًا. يمثل R3 مزود خدمة الإنترنت (ISP) الذي يقوم بتوصيل مسؤول من شركة إدارة الشبكة، والذي تم تعيينه لإدارة شبكتك عن بعد. ASA عبارة عن جهاز أمان CPE متطور يربط شبكة الشركة الداخلية مع الشبكات الخارجية. سيتم تكوين ASA للإدارة بواسطة مسؤول على الشبكة الداخلية.

هيكل الشبكة (Topology):



جدول العناوين:

- تم تعيين العناوين مسبقا كما هو موضح بالجدول التالي

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.225	255.255.255.248	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	NA
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	NA
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	NA
DMZ Server	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

الجزء الاول: التحقق من الاتصال واستكشاف جهاز ASA

- **الخطوة ١: اختبار الاتصال باستخدام Add Simple PDU اختبري اتصال الجهاز PC-C مع R1 و R3**

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC-C	R3	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC-C	R1	ICMP		0.000	N	1	(edit)	(delete)

الخطوة ٢: استعرضي مميزات وإصدار جهاز ASA.

- كتابة الأمر show version لعرض معلومات جهاز الـ ASA

```
ccnas-asa#show version

Cisco Adaptive Security Appliance Software Version 8.4(2)
Device Manager Version 6.4(5)
```

الجزء الثاني: تكوين إعدادات ASA وأمان الواجهة باستخدام واجهة سطر الأوامر (CLI)

الخطوة ١: تكوين اسم المضيف واسم المجال و وضع كلمة مرور على وضع التكوين.

- قم بتكوين اسم مضيف ASA كـ CCNAS-ASA
- قم بتكوين اسم المجال كـ ccnasecurity.com
- قم بتكوين كلمة مرور على وضع الـ Enable حيث ان كلمة المرور هي ciscoenpa55.

الخطوة ٢: ضبطي التاريخ والوقت.

- اضبطي الوقت على الساعة ٨ و٢٠ دقيقه و٠ ثانيه، والتاريخ على شهر أكتوبر يوم ٦ من سنة ٢٠٢٤.
- استعرضي الوقت والتاريخ.

```
ciscoasa#conf t
ciscoasa(config)#hostname CCNA-ASA
CCNA-ASA(config)#domain-name ccnasecurity.com
CCNA-ASA(config)#enable password ciscoenpa55
CCNA-ASA(config)#clock set 8:20:00 Oct 6 2024
CCNA-ASA(config)#exit
CCNA-ASA#show clock
8:20:30.843 UTC Sun Oct 6 2024
```

الجزء الثالث: تكوين الواجهات الداخلية والخارجية.

الخطوة ١: تكوين واجهات VLAN 1 (الداخلية) و٢ VLAN (الخارجية) في هذا الوقت.

- قم بتكوين واجهة VLAN 1 منطقية للشبكة الداخلية علماً بأن عنوان الشبكة هو (١٩٢,١٦٨,١,١) و قناعها (٢٢٥,٢٥٥,٢٥٥,٠) و تعيين مستوى الأمان على أعلى إعداد وهو ١٠٠ ثم قم بتمكين واجهة VLAN 1 .

- أنشئ واجهة VLAN 2 منطقية للشبكة الخارجية علماً بأن عنوان الشبكة هو (٢٠٩,١٦٥,٢٠٠,٢٢٤) وقناعها (٢٥٥,٢٥٥,٢٥٥,٢٤٨) واضبط مستوى الأمان على أدنى إعداد وهو ٠ ثم قم بتمكين واجهة VLAN 2 .

```
CCNA-ASA(config)#int vlan 1
CCNA-ASA(config-if)#nameif inside
CCNA-ASA(config-if)#ip address 192.168.1.1 255.255.255.0
CCNA-ASA(config-if)#security-level 100
CCNA-ASA(config-if)#exit
CCNA-ASA(config)#int e0/1
CCNA-ASA(config-if)#switchport access vlan 1
CCNA-ASA(config-if)#no shutdown
CCNA-ASA(config-if)#exit
CCNA-ASA(config)#int vlan 2
CCNA-ASA(config-if)#nameif outside
CCNA-ASA(config-if)#ip address 209.165.200.224 255.255.255.0
CCNA-ASA(config-if)#security-level 0
CCNA-ASA(config-if)#exit
CCNA-ASA(config)#int e0/0
CCNA-ASA(config-if)#switchport access vlan 2
CCNA-ASA(config-if)#no shutdown
CCNA-ASA(config-if)#exit
```

الجزء الرابع: استخدم أوامر التحقق للتحقق من الاعدادات التي تم إنشاؤها.

ملاحظة: في هذا المعمل تم تنفيذ تكوين إعدادات جهاز ASA الأساسية فقط لذلك ستلاحظ ان النسبة لم تصل الى ١٠٠٪

الخطوة ١: استعراض عناوينIP

- استعراض عناوين IP التي تم تكوينها على الواجهات من خلال امرshow interface IP brief

```
CCNA-ASA#show int ip brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  down                  down
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet0/4            unassigned      YES unset  down                  down
Ethernet0/5            unassigned      YES unset  down                  down
Ethernet0/6            unassigned      YES unset  down                  down
Ethernet0/7            unassigned      YES unset  down                  down
Vlan1                  192.168.1.1     YES manual up                    up
Vlan2                  209.165.200.224 YES manual up                    up
```

الخطوة ٢: عرض جميع واجهات ASA

- استخدم الأمر show Switch vlan لعرض شبكات VLAN الداخلية والخارجية التي تم تكوينها على ASA.

```
CCNA-ASA(config)#show switch vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    inside                           up        Et0/1, Et0/2, Et0/3, Et0/4
                                                Et0/5, Et0/6, Et0/7
2    outside                          up        Et0/0
```

ملخص لجميع الأوامر:

في جهاز ASA
ciscoasa#conf t ciscoasa(config)#hostname CCNA-ASA CCNA-ASA(config)#domain-name ccnasecurity.com CCNA-ASA(config)#enable password ciscoenpa55 CCNA-ASA(config)#clock set 8:20:00 Oct 6 2024 CCNA-ASA(config)#exit CCNA-ASA#show clock 8:20:30.843 UTC Sun Oct 6 2024 CCNA-ASA#conf t CCNA-ASA(config)#int vlan 1 CCNA-ASA(config-if)#nameif inside CCNA-ASA(config-if)#ip address 192.168.1.1 255.255.255.0 CCNA-ASA(config-if)#security-level 100 CCNA-ASA(config-if)#exit CCNA-ASA(config)#int e0/1 CCNA-ASA(config-if)#switchport access vlan 1 CCNA-ASA(config-if)#no shutdown CCNA-ASA(config-if)#exit CCNA-ASA(config)#int vlan 2 CCNA-ASA(config-if)#nameif outside CCNA-ASA(config-if)#ip address 209.165.200.224 255.255.255.0 CCNA-ASA(config-if)#security-level 0 CCNA-ASA(config-if)#exit CCNA-ASA(config)#int e0/0 CCNA-ASA(config-if)#switchport access vlan 2 CCNA-ASA(config-if)#no shutdown CCNA-ASA(config-if)#exit CCNA-ASA(config)#show switch vlan

رابط شرح لتنفيذ المعمل:

تكوين إعدادات جهاز **ASA** الأساسية وجدار الحماية باستخدام **CLI**

❖ ملخص

يمكن إعداد Cisco Adaptive Security Appliance (ASA) بعدة طرق للتكيف مع أي طوبولوجيا الشبكة، ومع ذلك، فإن التخطيط السليم ضروري للتنفيذ الناجح لميزات الأمان التي توفرها Cisco ASA.

يوفر Cisco ASA نوعين من واجهات المستخدم:

١. واجهة سطر الأوامر (CLI) - توفر واجهة سطر الأوامر (CLI) وصولاً غير رسومي إلى Cisco.

٢. واجهة مستخدم رسومية (GUI) عبر ASDM —جهاز أمان تكيفي من Cisco.

عندما يتم تمهيد جهاز الأمان بدون تكوين، فإنه يقدم قائمة الإعداد التي يمكّنك من تكوين المعلمات الأولية مثل اسم الجهاز وعنوان IP يمكنك اختيار الانتقال من خلال قائمة الإعداد الأولية للتهيئة السريعة.

❖ أسئلة المراجعة

١. جدار الحماية يُستخدم لمنع حركة المرور بين شبكة موثوق بها وأخرى غير موثوق بها.

أ- صح

ب- خطأ

٢. جدار الحماية الوسيط (Next-generation Firewalls) يعمل كوسيط بين الشبكات الداخلية والخارجية لتوجيه حركة المرور.

أ- صح

ب- خطأ

٣. يُوصى بأن تُستخدم خدمة مصادقة خارجية في النشرات الكبيرة لأنها تحسن من قابلية التوسع والإدارة.

أ- صح

ب- خطأ

٤. لا يمكن استخدام Kerberos كبروتوكول مصادقة في ASA Cisco .

أ- صح

ب- خطأ

٥. ما الذي يمكن أن تقدمه جدران الحماية الشخصية(Personal Firewalls) ؟

أ- حماية للأجهزة الشخصية فقط

ب- حماية للشبكات الصغيرة فقط

ت- حماية للشبكات الكبيرة والأجهزة الشخصية

ث- حماية للشبكات الكبيرة فقط

٦. جدران الحماية التفتيشية ذات الحالة معروفة بـ:

أ- تصفية حركة المرور استنادًا إلى عناوين MAC .

ب- مراقبة وتصفية حركة المرور الواردة والصادرة استنادًا إلى قواعد محددة مسبقًا .

ت- حظر جميع أشكال الحركة تلقائيًا.

ث- تشفير كل حركة مرور صادرة تلقائيًا.

٧. ما الذي يمكن أن يتضمنه تكامل جهاز ASA Cisco Series 5500 مع الشبكة بدون الحاجة إلى تركيبات إضافية؟

أ- جدار الحماية وIPS فقط

ب- جدار الحماية وVPN فقط

ت- جدار الحماية وIPS و VPN

ث- IPS و VPN فقط

٨. ما هي وظيفة خدمة AAA في أنظمة الأمان مثلASA Cisco ؟

أ- المصادقة فقط

ب- التصديق والتفويض فقط

ت- المصادقة والتفويض والمحاسبة

ث- التصديق والمحاسبة فقط

٩. يمكن الوصول إلى واجهة سطر الأوامر (CLI) على ASA Cisco عبر؟

أ- Telnet و SSH

ب- CLI وTFTP

ت- SNMP و SSH

ث- HTTP وFTP

١٠. توفر واجهة .....وصولا رسومي إلى Cisco ASA .

أ- SSH

ب- CLI

ت- SNMP

ث- GUI

الفصل الرابع

إعدادات ASA المتقدمة

في هذا الفصل سنتعرف على المواضيع التالية:

- مقدمة إعدادات ASA باستخدام ASDM
  - تحميل ASDM
  - إعداد الجهاز
  - الوصول إلى ASDM
  - التعرف على واجهات ASDM
  - شاشات وظيفية من ASDM
- إعدادات ASA VPN
- ملخص
- أسئلة المراجعة

❖ مقدمة اعدادات ASA باستخدام ASDM

- **ASDM (Adaptive Security Device Manage)** هو واجهة رسومية لإدارة أجهزة الأمان ASA. يسهل ASDM على المستخدمين تكوين وإدارة إعدادات الأمان والسياسات على أجهزة ASA بشكل أكثر سهولة مقارنة بالتكوين عبر واجهة سطر الأوامر.

قبل أن تتمكن من الوصول إلى وحدة التحكم الرسومية ASDM، يجب عليك تثبيت برنامج ASDMعلى الفلاش المحلي لجهاز الأمان ASA، يمكن لوحدة التحكم ASDM إدارة ملف جهاز الأمن فقط، لذلك ، إذا كنت بحاجة إلى إدارة أجهزة أمان متعددة ، يجب تثبيت برنامج ASDM على جميع أجهزة ASA من Cisco ومع ذلك ، يمكن أن تطلق محطة عمل واحدة مثيلات متعددة لعملاء ASDM لإدارة الأجهزة المختلفة ، اختياريًا، يمكنك الاستفادة من Cisco Security Manager (CSM) لتكوين تطبيقات متعددة في نفس الوقت.

تحتاج لضبط إعدادات ASA باستخدام ASDM الى :

١. جهاز ASA
٢. Consolecable
٣. جهاز كمبيوتر (لمحطة عمل الإدارة الخاصة بك)

• تحميل ASDM

قبل تحميل البرنامج في جهاز الأمان علينا أولا التحقق من وجوده في جهاز. يمكنك استخدام الأمر dir لتحديد ما إذا كان برنامج ASDM مثبتًا أم لا. اذا كان لا يحتوي جهاز الأمان على برنامج ASDM، فيجب عليك تحميل ملف صورة للبرنامج من خادم ملفات خارجي ، باستخدام الأمر copy لنقل ملف الصورة , كما هو موضح في المثال التالي حيث يتم نسخ ملف ASDM، المسمى asdm-621.bin ، من خادم TFTP الموجود في ١٩٢,١٦٨,١٠,١٠:

```
Chicago# copy tftp flash

Address or name of remote host []? 192.168.10.10

 Source filename []? asdm-621.bin

 Destination filename [asdm-621.bin]? asdm-621.bin

Accessing tftp://192.168.10.10/asdm-621.bin! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!...

Output omitted for brevity!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! .

 Writing file disk0:/asdm-621.bin ...
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

 Output omitted for brevity!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! .

 ٦٨٨٩٧٦٤bytes copied in 161.420 secs (36500 bytes/sec)
```

لتحقق من محتوى الفلاش المحلي بعد تحميل الملف بنجاح استخدم الامر dir كما هو موضح في المثال التالي:

```
Chicago# dir

Directory of disk0/:

-   ١٢٦٠rw- 14524416 16:47:34 May 13 2009 asa821-k8.bin

- ٢٥١١rw- 6889764 17:38:14 May 13 2009 asdm-621.bin

 ٦٢٨٨١٧٩٢bytes total (46723072 bytes free)
```

- **إعداد الجهاز**

عند الوصول إلى ملف ASDM ، يقوم Cisco ASA بتحميل أول صورة ASDM يعثر عليها من الفلاش المحلي ، في حالة وجود عدة صور ASDM في الفلاش ، استخدم أمر asdm image وحدد موقع صورة ASDM التي تريد تحميلها ، وهذا يضمن أن الجهاز يقوم دائمًا بتحميل الصورة المحددة عند بدء تشغيل ASDM في المثال التالي:

- تم إعداد الجهاز لاستخدام asdm-621.bin كملف صورة ASDM

```
Chicago(config)# asdm image disk0:/asdm-621.bin
```

- يعمل جهاز الأمان كخادم ويب لمعالجة ملف طلبات العملاء ، يجب عليك تمكين خادم الويب على الجهاز باستخدام الأمر:

```
http server enable
```

يتجاهل جهاز الأمان الطلبات الواردة حتى عنوان IP لعميل ASDM موجود في الشبكة الموثوقة للوصول إلى محرك .HTTP المسؤول يُمكّنه

- تكوين ASA لقبول اتصالات HTTPS باستخدام الأمر http للسماح بالوصول إلى ASDM من أي مضيف على الشبكة الداخلية ٢٤/١٩٢,١٦٨,١,٠ باستخدام الأمر:

```
http 192.168.1.0 255.255.255.0 inside
```

• الوصول إلى ASDM

للوصول لواجهة برنامج ASDM اتبع الخطوات التالية:

١. افتح متصفحًا على جهاز الكمبيوتر (محطة الإدارة) واختبر وصول HTTPS إلى ASA عن طريق إدخال https://192.168.1.1.

ملاحظة: العنوان ١٩٢,١٦٨,١,١ هو عنوان جهاز الأمان ASA.

٢. بعد إدخال عنوان URL أعلاه، من المفترض أن ترى تحذيرًا أمنيًا بشأن شهادة أمان موقع الويب. انقر فوق متابعة إلى هذا الموقع ثم ستظهر صفحة الترحيب كما هو موضح في الصورة (٧).

صورة (٧): صفحة الترحيب

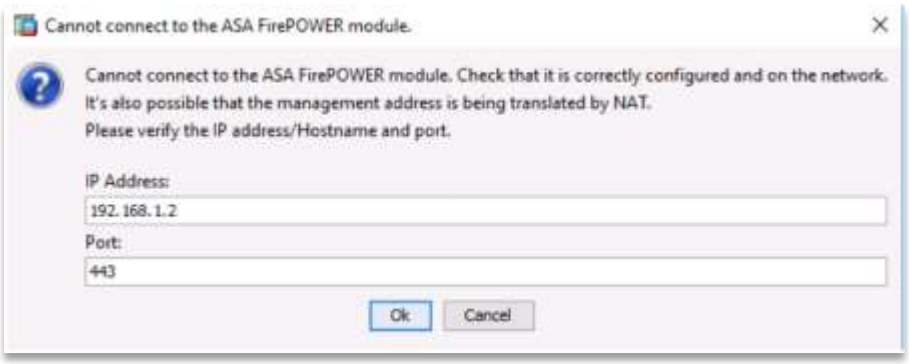
في هذه الشاشة يمكنك اختيار أحد الخيارات التالية:

- تثبيت ASDM على جهاز كمبيوتر.
- يعمل ASDM كتطبيق محلي على جهاز الكمبيوتر.
- تثبيت ASDM كبرنامج جافا صغير يستند إلى مستعرض مباشرة من ASA.

٣. انقر فوق خيار تشغيل ASDM ثم انقر فوق متابعة لأي نوافذ تحذيرات أمنية أخرى.
٤. بعد ذلك سيظهر لك مربع الحوار الذي يطلب منك إدخال اسم المستخدم وكلمة المرور كما هو موضح في الصورة(٨). اترك هذه الحقول فارغة وانقر فوق "موافق" لأنه لم يتم ضبط اسم المستخدم وكلمة المرور مسبقا.

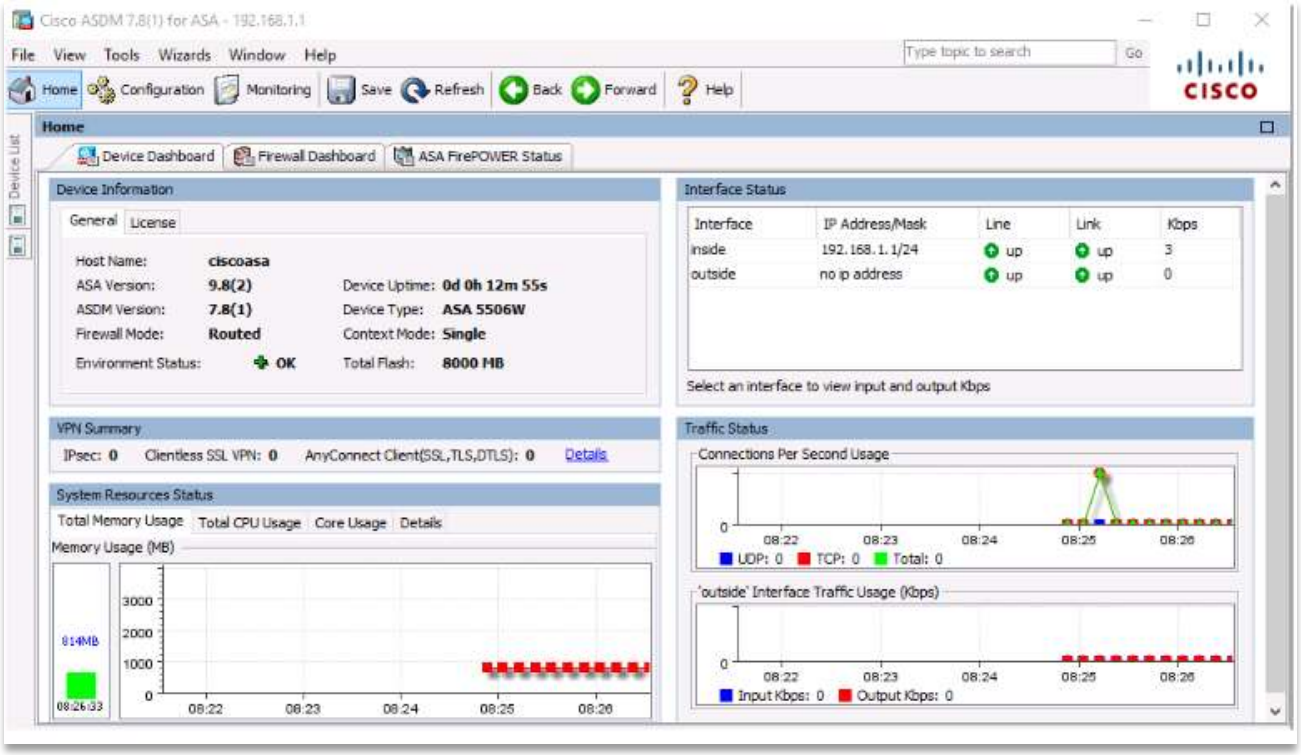
صورة (٨): مربع الحوار

٥. انقر فوق إلغاء الأمر (Cancel) في نافذة لا يمكن الاتصال (Cannot connect to the ASA FirePOWER) للمتابعة كما هو موضح في الصورة(٩).



صورة (٩): نافذة لا يمكن الاتصال

٦. سيتم عرض شاشة واجهة المستخدم الرسومية الأولية بمساحات وخيارات مختلفة كما هو موضح في الصورة(١٠).



صورة (١٠): شاشة واجهة المستخدم الرسومية

- **التعرف على واجهات ASDM**

يقسم ASDM الشاشة الأولية، المعروفة أيضًا باسم الشاشة الرئيسية، إلى الستة أقسام التالية:

١. معلومات الجهاز Device Information - تعرض معلومات الأجهزة والبرامج الخاصة بجهاز الأمان ، مثل الإصدار الحالي من نظام التشغيل ونوع الجهاز ، لو علامة التبويب الترخيص محددة ، يعرض ASDM الميزات التي تم تمكينها على جهاز الأمان.
٢. جلسات VPN (VPN sessions) - يعرض عدد IPSec النشط، و AnyConnect أنفاق SSL VPN (tunnels).
٣. حالة موارد النظام system Resources - توفر الحالة الحالية لاستخدام وحدة المعالجة المركزية والذاكرة على الجهاز.
٤. حالة الواجهة Interface Status - تعرض اسم الواجهة وعنوان IP المعين، كذلك يعرض معلومات الارتباط للواجهات المكونة حاليًا ومعدل المرور عبرهم.
٥. حالة حركة المرور - توفر معلومات حول عدد اتصالات TCP وUDP النشطة ومعدل المرور الذي يمر عبر الواجهة الخارجية.

٦. أحدث رسائل سجل نظام ASDM — لعرض أحدث رسائل سجل نظام ASDM الموجودة التي تم إنشاؤها بواسطة جهاز الأمن، يتم تعطيل Syslogging افتراضيًا ويحتاج إلى تمكينها لمراقبة السجل، عند التمكين، يرسل جهاز الأمان الرسائل إلى عميل ASDM.

يعرض ASDM ثلاث علامات تبويب إضافية على الشاشة الرئيسية، يشملوا

١. علامة التبويب Firewall Dashboard (لوحة معلومات جدار الحماية) - تعرض علامة التبويب Firewall Dashboard (لوحة معلومات جدار الحماية) معلومات إحصائية حول حركة المرور التي تمر عبر جهاز الأمان الخاص بك، يتضمن ذلك عدد الاتصالات وترجمات NAT والحزم المسقطة والهجمات وإحصائيات الاستخدام الأعلى.
٢. علامة التبويب "أمان المحتوى" - تعرض علامة التبويب "أمان المحتوى" معلومات حول أمن المحتوى والتحكم فيه SSM (CSC)، يظهر هذا الجزء فقط إذا كان CSC SSM مثبتة في جهاز الأمن التكيفي.
٣. علامة تبويب IPS - تعرض علامة التبويب "نظام منع التطفل" معلومات حول IPS.

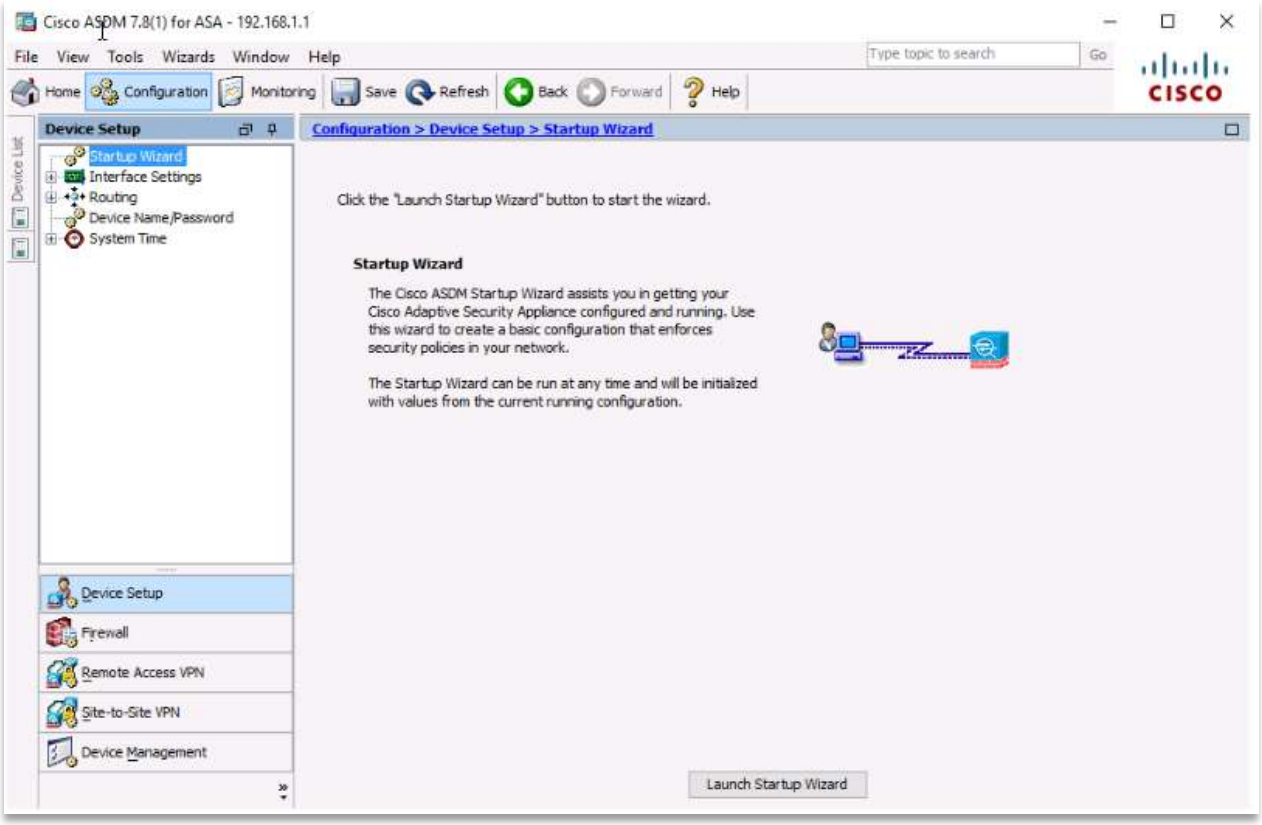
• شاشات وظيفية من ASDM

بالإضافة إلى الشاشة الرئيسية، تأتي واجهة ASDM مع الشاشتين الوظيفيتين التاليتين:

١. شاشة التكوين
٢. شاشة المراقبة

١. شاشة التكوين

تكون شاشة التهيئة مفيدة عندما يلزم التهيئة الجديدة أو الحالية. في الجانب الأيسر من الصورة (١١) خمسة إلى ستة رموز ميزات، اعتمادًا على إعداد الأجهزة للجهاز.



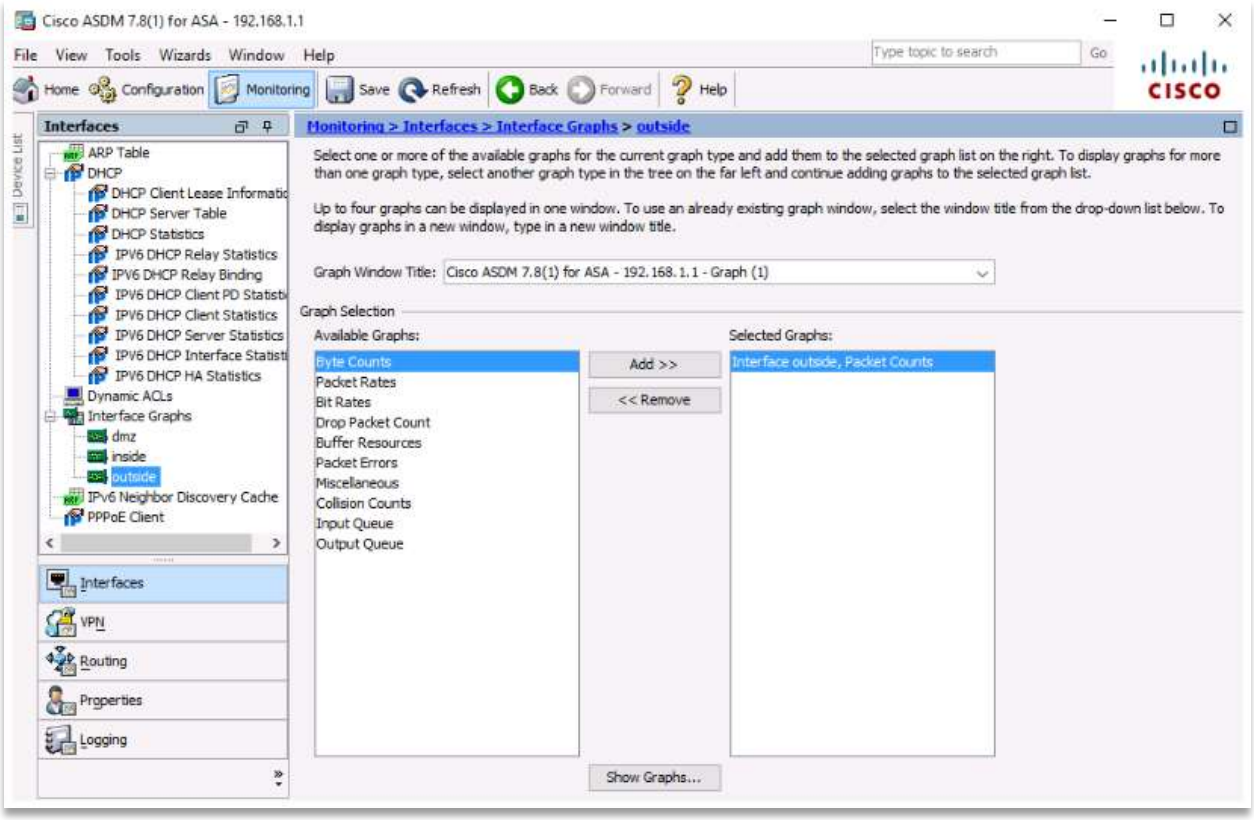
صورة (١١): شاشة التكوين

أيقونات الميزات في شاشة التكوين هي كما يلي:

- إعداد الجهاز - تكوين الواجهات والواجهات الفرعية على جهاز الأمان.
- جدار الحماية - مفيد في إنشاء سياسات أمان لتصفية وترجمة تتبع الحزم عبر الجهاز، يمكّنك أيضًا من تحديد تجاوز الفشل وجودة الخدمة وAAA والشهادات والعديد من الميزات الأخرى المتعلقة بجدار الحماية.
- Remote Access VPN - لإعداد اتصالات VPN للوصول عن بُعد مثل IPSec، L2TP عبر IPSec و Clientless SSL VPN وأنفاق AnyConnect.
- Site-to-site VPN - إعداد أنفاق VPN من موقع إلى موقع.
- IPS — إعداد سياسات لبطاقة SSM لمراقبة وإسقاط الحزم غير المصرح بها، هذا الرمز غير مرئي في حالة عدم وجود بطاقة SSM.
- إدارة الجهاز – هنا يمكن إعداد ميزات الجهاز الأساسية.

٢. شاشة المراقبة

تعرض شاشة المراقبة إحصائيات حول ميزات الأجهزة والبرامج الخاصة بجهاز الأمن، يوفر ASDM رسومًا بيانية في الوقت الفعلي لمراقبة صحة الجهاز وحالته على غرار شاشة التكوين، تعرض الصورة (١٢) شاشة المراقبة وهي تحتوي على خمسة أو ستة رموز، اعتمادًا على ما إذا كان لديك وحدة SSM مثبتة أم لا.



صورة (١٢): شاشة المراقبة

تم وصف أيقونات الميزات في شاشة المراقبة أدناه:

- الواجهات - تراقب الواجهات والواجهات الفرعية عن طريق الحفاظ على ARP وDHCP وجداول ACL الديناميكية. كما يوفر تمثيلًا رسومياً لاستخدام الواجهة وإنتاجية الحزمة.
- VPN - تراقب اتصالات VPN النشطة على جهاز الأمان. أنه يوفر الرسوم البيانية والتحليل الإحصائي لأنفاق الوصول عن بعد القائمة على موقع إلى موقع وIPSec و SSL VPN.
- IPS - يوفر معلومات إحصائية للحزم التي تمر عبر محرك IPS، هذا الرمز غير موجود إذا لم يتم تثبيت وحدة IPS.
- التوجيه - يعرض جدول التوجيه الحالي ويوفر معلومات عن EIGRP وجيران OSPF.

- الخصائص - تراقب الجلسات الإدارية النشطة مثل Telnet و SSH و ASDM، كما يوفر معلومات رسومية حول وحدة المعالجة المركزية والذاكرة وحظر استخدام الكتل، يوفر معلومات رسومية حول الترجمات النشطة و UDP / TCP يوفر معلومات رسومية لتدقيق IP و WCCP و CRL و ميزات DNS Cache.
- التسجيل - يعرض رسائل السجل كأحداث مباشرة، كما يعرض أيضًا رسائل السجل من مساحة عازلة.
- Trend Micro Content Security - يتيح لك ASDM مراقبة إحصائيات CSC SSM، بالإضافة إلى الميزات المتعلقة بـ CSC SSM مثل أنواع التهديدات التي تم اكتشافها بواسطة الوحدة النمطية، وسجلات الأحداث المباشرة للمراقبة في الوقت الفعلي ، والرسوم البيانية لاستخدام الموارد.

❖ اعدادات ASA VPN

Step 1. Configure an Identity Certificate

١. سنقوم بإنشاء شهادة هوية للأغراض العامة وموقعة ذاتيًا باسم sslvpnkey وأقوم بتطبيق هذه الشهادة على الواجهة "الخارجية" يمكنك شراء شهادة من خلال بائع مثل Verisign، إذا اخترت ذلك.

```
corpasa(config)#crypto key generate rsa label sslvpnkey
corpasa(config)#crypto ca trustpoint localtrust
corpasa(config-ca-trustpoint)#enrollment self
corpasa(config-ca-trustpoint)#fqdn sslvpn. mycompany.com
corpasa(config-ca-trustpoint)#subject-name CN=sslvpn.mycompany.com
corpasa(config-ca-trustpoint)#keypair sslvpnkey
corpasa(config-ca-trustpoint)#crypto ca enroll localtrust noconfirm
corpasa(config)# ssl trust-point localtrust outside
```

Step 2. Upload the SSL VPN Client Image to the ASA

٢. يمكنك الحصول على صورة العميل على موقع Cisco.com. عند اختيارك للصورة المراد تنزيلها على خادم tftp ، تذكر أنك ستحتاج إلى صورة منفصلة لكل نظام تشغيل يمتلكه المستخدمون لديك ، بعد تحديد برنامج العميل وتنزيله ، يمكنك نقله إلى ASA الخاص بك

```
corpasa(config)#copy  tftp://192.168.81.50/anyconnect-win-2.0.0343-k9.pkg
flash
```

بعد تحميل الملف إلى ASA، قم بتكوين هذا الملف ليتم استخدامه لجلسات webvpn لاحظ أنه إذا كان لديك أكثر من عميل واحد ، فقم بتهيئة العميل الأكثر استخدامًا ليكون له الأولوية القصوى ، في هذه الحالة ، نستخدم عميلاً واحدًا فقط ونعطيه أولوية قدرها ١.

```
corpasa(config)#webvpn
corpasa(config-webvpn)#svc image disk0:/anyconnect-win-2.3.0254-k9.pkg
1
```

Step 3. Enable AnyConnect VPN Access

```
corpasa(config)#webvpn
corpasa(config-webvpn)#enable outside
corpasa(config-webvpn)#svc enable
```

Step 4. Create a Group Policy

٤. تُستخدم نُهج المجموعة لتحديد المعلمات التي يتم تطبيقها على العملاء عند اتصالهم، في هذه الحالة، سننشئ سياسة مجموعة باسم SSLClient سيحتاج عملاء الوصول عن بُعد إلى تعيين عنوان IP أثناء تسجيل الدخول ، لذلك سنقوم أيضًا بإعداد تجمع DHCP لهم ، ولكن يمكنك أيضًا استخدام خادم DHCP إذا كان لديك واحد.

```
corpasa(config)#ip local pool SSLClientPool 192.168.100.1-192.168.100.50
mask 255.255.255.0
corpasa(config)#group-policy SSLCLient internal
corpasa(config)#group-policy SSLCLient attributes
corpasa(config-group-policy)#dns-server value 192.168.200.5
corpasa(config-group-policy)#vpn-tunnel-protocol svc
corpasa(config-group-policy)#default-domain value mysite.com
corpasa(config-group-policy)#address-pools value SSLClientPool
```

Step 5. Configure Access List ByPass

٥. باستخدام الأمر sysopt connect ، نطلب من ASA السماح لعملاء SSL / IPsec بتجاوز قوائم الوصول إلى الواجهة.

```
corpasa(config)#sysopt connection permit-vpn
```

Step 6. Create a Connection Profile and Tunnel Group

٦. عندما يتصل عملاء الوصول عن بعد بـ ASA ، فإنهم يتصلون بملف تعريف اتصال ، والذي يُعرف أيضًا باسم مجموعة النفق ، سنستخدم مجموعة النفق هذه لتحديد معلمات الاتصال المحددة التي نريدها استخدامها ، في حالتنا ، نقوم بتهيئة عملاء الوصول عن بعد هؤلاء لاستخدام عميل Cisco AnyConnect SSL ، ولكن يمكنك أيضًا تكوين مجموعات النفق لاستخدام IPsec و L2L وما إلى ذلك.

أولاً ، لنقم بإنشاء عميل SSL لمجموعة النفق:

```
corpasa(config)#tunnel-group SSLClient type remote-access
```

بعد ذلك ، سنقوم بتعيين السمات المحددة:

```
corpasa(config)#tunnel-group SSLClient general-attributes
corpasa(config-tunnel-general)#default-group-policy SSLCLient
corpasa(config-tunnel-general)#tunnel-group SSLClient webvpn-attributes
corpasa(config-tunnel-webvpn)#group-alias MY_RA enable
corpasa(config-tunnel-webvpn)#webvpn
corpasa(config-webvpn)#tunnel-group-list enable
```

لاحظ الاسم المستعار MY_RA هو المجموعة التي سيراها المستخدمون عند مطالبتهم بمصادقة تسجيل الدخول.

Step 7. Configure NAT Exemption

٧. نحتاج الآن إلى إخبار ASA بعدم قيام NAT بحركة المرور بين عملاء الوصول عن بُعد والشبكة الداخلية التي سيصلون إليها، أولاً ، سننشئ قائمة وصول تحدد حركة المرور ، ثم سنطبق هذه القائمة على بيان nat لواجهتنا.

```
corpasa(config)#access-list no_nat extended permit
ip 192.168.200.0 255.255.255.0 192.168.100.0 255.255.255.0
corpasa(config)#nat (inside) 0 access-list no_nat
```

Step 8. Configure User Accounts

٨. لآن نحن جاهزون لبعض حسابات المستخدمين، هنا سننشئ مستخدمًا ونخصص هذا المستخدم لشبكة VPN للوصول عن بُعد.

```
corpasa(config)#username hyde password l3tm3in
corpasa(config)#username hyde attributes
corpasa(config-username)#service-type remote-access
```

٩. الانتهاء: لا تنس حفظ التهيئة في الذاكرة.

```
corpasa#write memory
```

١٠. تحقق من التكوين الخاص بك عن طريق إنشاء جلسة وصول عن بعد واستخدم الأمر show التالي لعرض تفاصيل الجلسة.

```
corpasa #show vpn-sessiondb svc
```

إذا واجهت أي صعوبات، فاستخدم أوامر debug webvpn لتشخيص المشكلة.

❖ ملخص

يعد جهاز ASA جهاز حماية يتميز بكامل ميزاته للشركات الصغيرة والمكاتب الفرعية والبيئات الخاصة بالشركات العاملة عن بعد ، يوفر جهاز Cisco ASA جدار حماية عالي الأداء و SSL و IPsec VPN وخدمات شبكة ثرية في جهاز "توصيل وتشغيل" معياري ، باستخدام Cisco ASDM المتكامل ، يمكن نشر Cisco ASA بسرعة وإدارتها بسهولة ، مما يمكن الشركات من تقليل تكاليف العمليات ، يتميز Cisco ASA 5505 بمحول إيثرنت سريع من ١٠ منافذ ١٠/١٠٠ مرن ، حيث يمكن تجميع منافذه ديناميكيًا لإنشاء ما يصل إلى ثلاثة شبكات محلية ظاهرية منفصلة للاستخدام المنزلي والأعمال وحركة الإنترنت لتحسين تجزئة الشبكة وأمانها ، يوفر Cisco ASA 5505 منفذين للطاقة عبر الإيثرنت (PoE) ، مما يتيح إمكانية نشر مبسطة لهواتف IP من Cisco باستخدام إمكانات الاتصال الصوتي عبر بروتوكول الإنترنت (VoIP) التي تعمل بخاصية اللمس الصفري ، ونشر نقاط الوصول اللاسلكية الخارجية لتوسيع شبكة الاتصال. .

❖ أسئلة المراجعة

١. CSM (Manager Security Cisco) تُستخدم لتحليل حركة المرور في الوقت الفعلي على أجهزة ASA.

أ- صح

ب- خطأ

٢. تعرض علامة التبويب "حالة حركة المرور" معلومات حول عدد اتصالات TCP و UDPالنشطة ومعدل المرور.

أ- صح

ب- خطأ

٣. تعرض شاشة التكوين في ASDM إحصائيات حول ميزات الأجهزة والبرامج الخاصة بـجهاز الأمن

أ- صح

ب- خطأ

٤. أيقونة جدار الحماية ASDM مفيدة في إنشاء سياسات أمان لتصفية وترجمة تتبع الحزم عبر الجهاز.

أ- صح

ب- خطأ

٥. ما الذي يحتاج إليه لتحقيق الوصول إلى وحدة التحكم ASDM لأجهزة ASA؟

أ- كابل توصيل الطاقة

ب- كابل التحكم عن بعد (Console Cable)

ت- كابل الشبكة (Ethernet Cable)

ث- كابل الفلاش (Flash Cable)

٦. ما الذي يجب فعله إذا لم يكن برنامج ASDM مثبتًا على جهازASA ؟

أ- تشغيل برنامج التثبيت من الإنترنت

ب- نسخ ملف ASDM من خادم TFTP

ت- استخدام أمر dir للتحقق من وجوده

ث- تحديث نظام التشغيل

٧. للتحقق من محتوى الفلاش المحلي بعد تحميل ملف بنجاح، أي من الخيارات التالية تعد صحيحة؟

أ- استخدم أمر show flash

ب- استخدم أمر check flash

ت- استخدم أمر dir

ث- استخدم أمر verify flash

٨. ما هي وظيفة علامة التبويب "حالة الواجهة" في ASDM ؟

أ- تعرض حالة النظام والبرامج على جهاز ASA .
ب- توفر معلومات عن الاتصالات النشطة والعناوين IP المعينة للواجهات.
ت- توفر معلومات حول عدد اتصالات VPN النشطة.
ث- تعرض أحدث رسائل سجل النظام.

٩. **ماهي الأيقونة التي تمكنك من تكوين الواجهات والواجهات الفرعية على جهاز الأمان.**
أ- إعداد الجهاز
ب- جدار الحماية
ت- Remote Access VPN
ث- site-to-Site VPN

١٠. **من خلال أيقونة التسجيل يمكنك أن ..... ؟**
أ- تراقب اتصالات VPN النشطة على جهاز الأمان.
ب- تراقب الجلسات الإدارية النشطة مثل Telnet وSSH .
ت- تعرض رسائل السجل كأحداث مباشرة، كما يعرض أيًضا رسائل السجل من مساحة عازلة.
ث- مراقبة إحصائيات CSC SSM.

الفصل الخامس
إدارة الشبكة الآمنة

في هذا الفصل سنتعرف على المواضيع التالية:

- مقدمة
- اختبار شبكة الأمن
  - التحليل الأمني لتقنية المعلومات
  - أدوات اختبار أمان الشبكة
- تطوير سياسة الأمن الشامل
- ملخص
- أسئلة المراجعة

❖ مقدمة

أمان الشبكة هو أي نشاط مصمم لحماية بياناتك والمحافظة على تكاملها اثناء استخدام الشبكة، أي أنه مجموعة من التقنيات والأجهزة والعمليات التي تهدف إلى إدارة الأمان والحماية للبنية التحتية للشبكة.

- وتتضمن كلًا من تقنيات الأجهزة والبرامج.
- وتستهدف مجموعة متنوعة من التهديدات.
- كما تمنع الدخول الغير مصرح به من الوصول إلى شبكتك أو الانتشار بها.
- يعمل أمان الشبكة الفعال على إدارة الوصول إلى الشبكة.

يجمع أمان الشبكة بين طبقات متعددة من الدفاعات في الشبكة، تعمل كل طبقة من طبقات أمان الشبكة على تنفيذ السياسات وعناصر التحكم، كما يمكن للمستخدمين المصرح لهم الوصول إلى موارد الشبكة، ومنع الجهات الضارة من تنفيذ عمليات الاستغلال والتهديدات. لذلك يجب على كل مؤسسه حماية شبكتها ، ومن الاستراتيجيات الأمنية الرئيسية التي يمكن للمؤسسات اتخاذها لحماية شبكاتها:

١. استخدام جدران الحماية .(Firewalls)
٢. إجراء اختبارات الاختراق (Penetration Testing).
٣. تحديث البرامج والأنظمة.
٤. استخدام برامج مكافحة الفيروسات والبرامج الضارة.
٥. تقييد الوصول.
٦. استخدام شبكات افتراضية خاصة (VPNs).
٧. تشفير البيانات.
٨. توعية الموظفين.

❖ اختبار شبكة الأمن

يمكن للمخترقين اختراق المؤسسات من خلال ثغرات معينة في الشبكات، أو أنظمة تكنولوجيا المعلومات والتطبيقات والهواتف المحمولة، كما يمكنهم التلاعب بالبيانات الخاصة بالعمل أو العملاء واستغلالها، فلا توجد شركة بعيدة عن الاختراق، مهما كان حجمها أو أهميتها. كما يوجد العديد من الشركات على غير علم بالاختراق، هل أنت على علم بالثغرات في أنظمتك وتطبيقاتك، والتي تُمكن المخترقون من استغلالها؟ يمكن الإجابة على تلك الأسئلة من خلال اختبارات الاختراق والتحليل الأمني لتكنولوجيا المعلومات. يتم اختبار البنية التحتية لتكنولوجيا المعلومات من وجهة نظر المُخترق، ومحاكاة هجمات إلكترونية حقيقية ونُحدد الثغرات في تكنولوجيا المعلومات قبل أن يصل إليها المخترقون.

- **التحليل الأمني لتقنية المعلومات**

يقلل الاختبار الفعال للاختراق والتحليل الأمني لتكنولوجيا المعلومات من الثغرات المحتملة التي قد يستغلها المخترقون، كما يزيد من أمن الشبكات وأنظمة تكنولوجيا المعلومات وأجهزة الهواتف المحمولة الخاصة بك، كما يقدم نظرة عامة عن الثغرات الأساسية في نظامك، يمكن العمل على تحسين أمن البنية التحتية في بضع خطوات في الصورة (١٣):

صورة (١٣): التدابير الأمنية لتحسين أمن البنية التحتية

إذاً يقدم التحليل الأمني واختبار اختراق تكنولوجيا المعلومات ـ في بضع خطوات ـ تقييمًا موضوعيًّا وموثوقًا عن فعالية التدابير الأمنية لتكنولوجيا المعلومات، وعما إذا كان هناك مجال للتحسين كما هو موضح بالشكل السابق.

- **أدوات اختبار أمان الشبكة**

أدوات اختبار أمان الشبكة هي أدوات تفحص الشبكة بحثاً عن الثغرات الأمنية. وتوفر أدوات اختبار أمان الشبكة رؤية شاملة للوضع الأمني لشبكتك. كما تأتي أدوات اختبار أمان الشبكة الحديثة مع ميزات متنوعة لمساعدة مسؤولي الشبكة على تحديد الحالات الشاذة ومشكلات الأمان المحتملة ومراقبة أمان الشبكة وتتبعه عبر مواقع متعددة. ويمكن لأدوات اختبار أمان الشبكة أيضا حماية شبكتك الداخلية من التهديدات الخارجية.

ومن الأمثلة على أدوات اختبار اختراق الشبكة:

١. Astra Security
٢. NMAP
٣. Wireshark
٤. OpenVAS
٥. Metasploit
٦. Nikto
٧. PRTG Network Monitor
٨. Snort
٩. Intruder

❖ تطوير سياسة الأمن الشامل

يجب أن تؤدي السياسة الأمنية أغراضاً كثيرة، منها:

- حماية الموظفين والمعلومات.
- تحديد السلوك المتوقع من المستخدمين، ومدراء الأنظمة، والإدارة، وموظفي الأمن.
- تفويض موظفي الأمن بالمراقبة والرصد والتحري.
- تحديد تبعات المخالفات والتفويض باتخاذ اللازم حيالها.
- تحديد الموقف الأساسي المجمع عليه للمؤسسة فيما يختص بالأمن.
- المساعدة في خفض المخاطر إلى الحد الأدنى.
- المساعدة في متابعة الالتزام بالأنظمة والتعليمات والتشريعات.

تقدم سياسات وإجراءات أمن المعلومات إطاراً لأفضل الممارسات الممكن اتباعها من قبل جميع الموظفين ، وتساعد على التأكد من خفض المخاطر إلى الحد الأدنى، ومن أن الاستجابة تتم تجاه أية حوادث أمنية بصورة فاعلة ، وستساعد سياسات أمن المعلومات كذلك على إشراك الموظفين في جهود الجهة المعنية لتأمين أصولها المعلوماتية، كما ستساعد عملية تطوير هذه السياسات على تحديد أصول المعلومات لدى الجهة الحكومية ، وتُحدد سياسة أمن المعلومات أسلوب الجهة الحكومية في التعامل مع المعلومات وتعلن داخلياً وخارجياً أن المعلومات هي أحد أصول تلك الجهة، وهي ملك لها، ويتعني حمايتها من الوصول، والتعديل، والإفصاح، والإتلاف بشكل غير مصرح به.

قامت الهيئة الوطنية للأمن السيبراني بتطوير الضوابط الأساسية للأمن السيبراني بعد دراسة عدة معايير وضوابط للأمن السيبراني وقامت بإعدادها سابقاً عدة جهات ومنظمات (محلية ودولية) ، تهدف هذه الضوابط لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات (Threats)الداخلية والخارجية ، ولحماية الأصول المعلوماتية والتقنية للجهة يجب التركيز على الأهداف الأساسية للحماية، وهي:

- سرية المعلومة (Confidentiality)
- سلامة المعلومة (Integrity)
- توافر المعلومة (Availability)

وتأخذ هذه الضوابط بالاعتبار المحاور الأربعة الأساسية التي يرتكز عليها الأمن السيبراني، وهي:

- الإستراتيجية (Strategy)
- الأشخاص (People)
- الإجراء (Process)
- التقنية (Technology)

❖ ملخص

إستراتيجية الأمن السيبراني هي نهج موثق تجاه مختلف جوانب الفضاء السيبراني cyberspace يتم تطويرها في الغالب لتلبية احتياجات الأمن السيبراني للدول والمؤسسات من خلال معالجة كيفية حماية البيانات والشبكات والأنظمة التقنية والمستخدمين، عادة ما تغطي الإستراتيجية الفعالة جميع نقاط الهجوم المحتملة التي يمكن أن تستهدفها الأطراف المهاجمة، يحتل الأمن السيبراني مركز الصدارة في معظم الاستراتيجيات الإلكترونية لأن التهديدات الإلكترونية أصبحت أكثر تقدمًا وخطورة بسبب تقدم أدوات وتقنيات الاستغلال exploit tool.

❖أسئلة المراجعة

١. يمكن للمخترقين المجرميين اختراق المؤسسات من خلال ثغرات معينة في الشبكات، أو أنظمة تكنولوجيا المعلومات والتطبيقات والهواتف المحمولة.

أ- صح

ب- خطأ

٢. من توصيات إجراءات الحماية المناسبه.

أ- إيقاف تشغيل الجهاز.

ب- وضع جدران حماية.

ت- قفل الباب.

ث- حفظ البيانات في الاوراق

٣. يمكن توثيق وتحليل الثغرات لتحسين أمن البنية التحتية وذلك من خلال:

أ- استغلال الثغرات

ب- التقارير

ت- إجراءات المكافحة

ث- تجميع المعلومات

٤. يمكن للمهاجم استغلال الثغرات من خلال.....:

أ- تجميع المعلومات

ب- تحديد الثغرات

ت- معرفة نقاط الضعف في المؤسسة او الشركة

ث- جميع ما سبق.

٥. السياسة الأمنية الناجحه تسمح بالدخول الغير مصرح به من الوصول إلى شبكتك أو الانتشار بها.

أ- صح

ب- خطأ

٦. أمان الشبكة هو أي نشاط مصمم لحماية بياناتك والمحافظة على تكاملها اثناء استخدام الشبكة.

أ- صح

ب- خطأ

٧. يجب ان تضمن السياسة الأمنية حماية معلومات الموظفين والمعلومات الحساسة.

أ- صح

ب- خطأ

٨. **الضوابط الأربعة الأساسية التي يرتكز عليها الأمن السيبراني، هي:**

أ- الإستراتيجية والأشخاص والإجراء والتقنية

ب- الإستراتيجية والأشخاص

ت- الإستراتيجية والإجراء والتقنية

ث- الأشخاص والإجراء والتقنية

٩. **من الأمثلة على أدوات اختبار اختراق الشبكة:**

أ- Cisco Packet Tracer

ب- NetBeans

ت- Wireshark

ث- Word

١٠. **تساعد السياسة الامنية في خفض المخاطر إلى الحد الأدنى.**

أ- صح

ب- خطأ

المراجع

❖ المراجع

Ref 1: William Stallings - Cryptography and Network Security - Pearson – 2017.
Ref 2: William Stallings - Cryptography and Network Security: Principles and Practice 7th Global Edition.
المرجع ٣: التشفير وفك التشفير - مجلة العلوم الاقتصادية والسياسية، كلية الاقتصاد والتجارة، زليتن.
المرجع ٤: NIST (المعهد الوطني للمعايير والتكنولوجيا) - وثائق ومعايير NIST حول التشفير والتواقيع الرقمية - الولايات المتحدة الأمريكية.
Ref 5: Cisco. (n.d.). What is a virtual private network (VPN)? https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html#~types-of-vpns
Ref 6: Microsoft. (n.d.). What is a VPN? Why should I use a VPN? | Types of VPN connections. https://azure.microsoft.com/en-gb/resources/cloud-computing-dictionary/what-is-vpn#typesofvpn
Ref 7: Cisco. (n.d.). Cisco learning network | What is IPsec? Cisco Learning Network. https://learningnetwork.cisco.com/s/question/0D53i00000KszAJCAZ/ipsec-story
Ref 8: Cisco. (n.d.). Understand IPsec IKEv1 protocol. https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.html
Ref 9: Cisco. (2023, May 16). 8.4.1.2 Packet Tracer - Configure and verify a site-to-site IPsec VPN using CLI Answes. ITExamAnswers.net. https://itexamanswers.net/8-4-1-2-packet-tracer-configure-verify-site-site-ipsec-vpn-using-cli-answes.html

Ref 10: Cisco Systems - AAA Configuration Guide, Cisco ASA 7.2 - https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/aaa.html - Cisco - 2006

Ref 11: William Stallings - Cryptography and Network Security: Principles and Practice 7th Global Edition.

Ref 12: Cisco Systems - 9.3.1.1 Packet Tracer – Configuring ASA Basic Settings and Firewall Using CLI Answers - https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/aaa.html

Ref 13: Cisco Systems - CCNA Security Chapter 10 - Configure ASA Basic Settings and Firewall using ASDM - https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/aaa.html - Cisco - 2006

Ref 14: Jinson Varghese. (2024, December 22). 10 Best Network Security Testing tools in 2024. https://www.getastra.com/blog/security-audit/network-security-testing-tools/