حماية الشبكات و الفضاء السيبراني

- الشبكات و الفضاء السيبراني
- ضمان اهداف الامن السيبراني
- مبدأ AAA
- تقنيات وأنواع الجدران النارية
- أنواع الشبكة الخاصة الافتراضية
- أنظمة وتقنيات حماية الشبكات
- اختبارات الشبكة

الشبكات و الانترنت

- الشبكة: تتكون من أجهزة كمبيوتر متصلة مع بعضها البعض مثل اللابتوب و الأجهزة المكتبية والخوادم ، والهواتف الذكية و الطابعات و أجهزة إنترنت الأشياء (مثل الكاميرات).

- الإنترنت: تقنية تربط الشبكات ببعضها البعض وتبني شبكة إضافية متعمقة.

الامن السيبراني ضمن الفضاء السيبراني

الفضاء السيبراني: يتكون من الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، الى جانب المعالِجات وأجهزة التحكم المرتبطة بها.

حماية الأجهزة والأصول المعلوماتية داخل الفضاء السيبراني يعرف بالأمن السيبراني.

أهداف الأمن السيبراني

السرية (Confidentiality)

تعني منع الوصول إلى ا لمعلومات إلا من الأ شخاص ا لمصرح لهم فقط سواءا عند تخزينها أو معالجتها أو عند نقلها عبر وسائل الاتصال وكذلك تحديد صلاحية التعديل والحذف والإضافة .

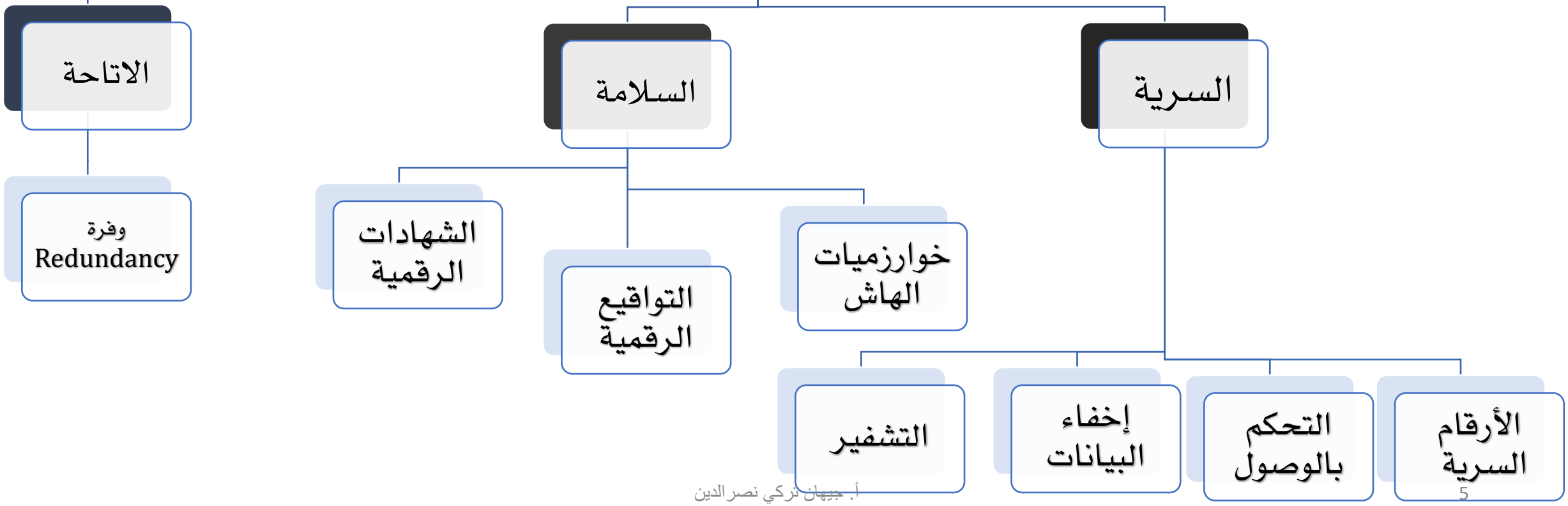
التكامل وسلامة المحتوى (Integrity)

المقصود بها أن تكون المعلومة صحيحة عند إدخالها وكذلك أثناء تنقلها بين الأجهزة في الشبكة والتأكد أنه لم يمسها أي تغيير وذلك باستخدام مجموعة من الأساليب والأنظمة

التوافر وا تاحة (Availability)

تعني بقاء المعلومة متوفرة للمستخدم وإمكانية الوصول إليها في أي وقت وعدم تعطل ذلك نتيجة لخلل في أنظمة إدارة قواعد المعلومات والبيانات أو وسائل الإتصال .

ضمان اهداف الامن السيبراني



مفاهيم ضمان السرية

الأرقام السرية

التحكم في الوصول : التحكم في الوصول إلى مبنى ، وغرفة ، ونظام ، وقاعدة بيانات ، وملف ، ومعلومات باستخدام تقنيات التحكم في الوصول لحماية السرية.

التشفير: تحويل البيانات من شكل قابل للقراءة إلى شكل مُرمَّز لا يمكن قراءته أو معالجته إلا بعد فك تشفيره.

إخفاء البيانات: تقنية لحجب و إخفاء البيانات داخل صورة، صوت او ملفات نصية أخرى حتى يتم إخفاء أن هناك اتصال أو تبادل معلومات يتم في الخفاء، ولا يكون على علم بهذا الاتصال إلا الأشخاص المعنيين.

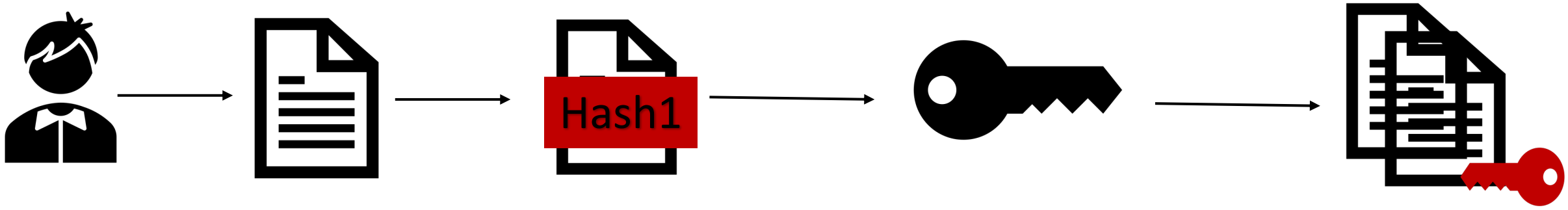
مفاهيم ضمان السلامة

الهاش: وسيلة لضمان نزاهة البيانات وعدم تغييرها تأخذ مدخلات بأي طول وتخرج نص له طول معين على حسب الدالة، و من المستحيل أن تكون قيمة الهاش هي نفسها لمجموعتين مختلفتين من البيانات و لا يمكن استرجاع النص الصريح مثل كلمات المرور.

التوقيع الرقمي: هو طابع مصادقة إلكتروني ومشفّر على معلومات رقمية مثل رسائل البريد الإلكتروني أو المستندات الإلكترونية ويؤكد التوقيع صدور المعلومات من الموقّع وعدم تعرّضها لأي تغيير ومن خصائصه انها لا يمكن انكاره ولا يعاد استخدامه.

الشهادات الرقمية: تشبه الشهادات الواقعية، وهي وثيقة رقمية تحتوي على مجموعة من المعلومات التي تقود إلى التحقق من هوية الشخص أو المنظمة أو الموقع الإلكتروني و تشفر المعلومات التي يحتويها جهاز الخادم.

التوقيع الرقمي



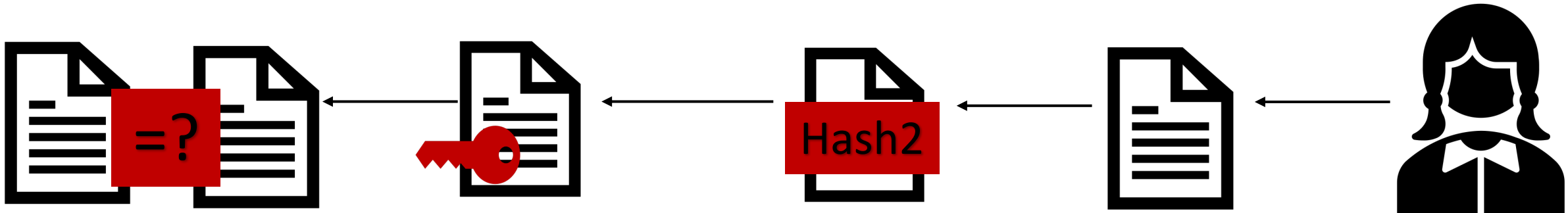
المرسل

الرسالة الاصلية

سيقوم المرسل بعمل هاش للرسالة الاصلية

تشفير قيمة الهاش للرسالة الاصلية باستخدام المفتاح الخاص بالمرسل

يقوم المرسل بتجمع الرسالة الاصلية وهاش الرسالة و مفتاحه العام ويرسله الى المستقبلة



تقوم المستقبلة بقراءة الرسالة الاصلية المُرسلة ولتتأكد ان الرسالة من المرسل تقوم بحساب قيمة الهاش لها

الرسالة الاصلية

الرسالة بعد حساب قيمة الهاش لها من المستقبلة

تقوم المستقبلة بفتح تشفير رسالة المرسل باستخدام مفتاحه العام

تقوم المستقبلة بمقارنة قيمة الهاش للرسالتين للتأكد من انها من المرسل

مفاهيم ضمان التوافر

الزيادة بطريقة ن+1: زيادة ن+1 تؤكد على توافر النظام في حال تعطل مكون من المكونات. المكونات المتعددة (ن) تحتاج لأن يكون له اعلى الأقل مكون احتياطي واحد(+1)

مثال: السيارة لها اربع إطارات(ن) ولها اطار واحد على الأقل زائد(+1) في حال تعطل احد الاطارات.

ن

1+

مبدأ AAA

AUTHENTICATION

المصادقة: هي اثبات هوية المستخدم او النظام. مثل اسم المستخدم وكلمة السر.

AUTHORIZATION

التفويض: صلاحيات المستخدم داخل النظام بعد ما تتم المصادقة.

(ماذا يستطيع المستخدم ان يفعل داخل النظام).

ACCOUNTING

المتابعة: متابعة ما يفعله المستخدمون داخل النظام.

جدران الحماية

أجهزة أو برامج تشكل حاجز بين شبكتك الداخلية الموثوقة والشبكات الخارجية غير الموثوق بها ، مثل الإنترنت، تستخدم مجموعة من القواعد المحددة للسماح أو منع حركة المرور.

- جدار حماية فحص الحزم
- جدار حماية فحص الحالة
- جدار حماية البروكسي
- جدار الحماية على المضيف
- جدار الحماية الهجين

جدار حماية فحص الحزم و فحص الحالة

جدار حماية فحص الحزم: جزء من الراوتر يسمح او يحجب حركة مرور الشبكة بناء على معلومات الطبقة الثالثة والرابعة مثل IP المصدر و IP الوجهة والبروتوكول ورقم المنفذ للمصدر والوجهة.

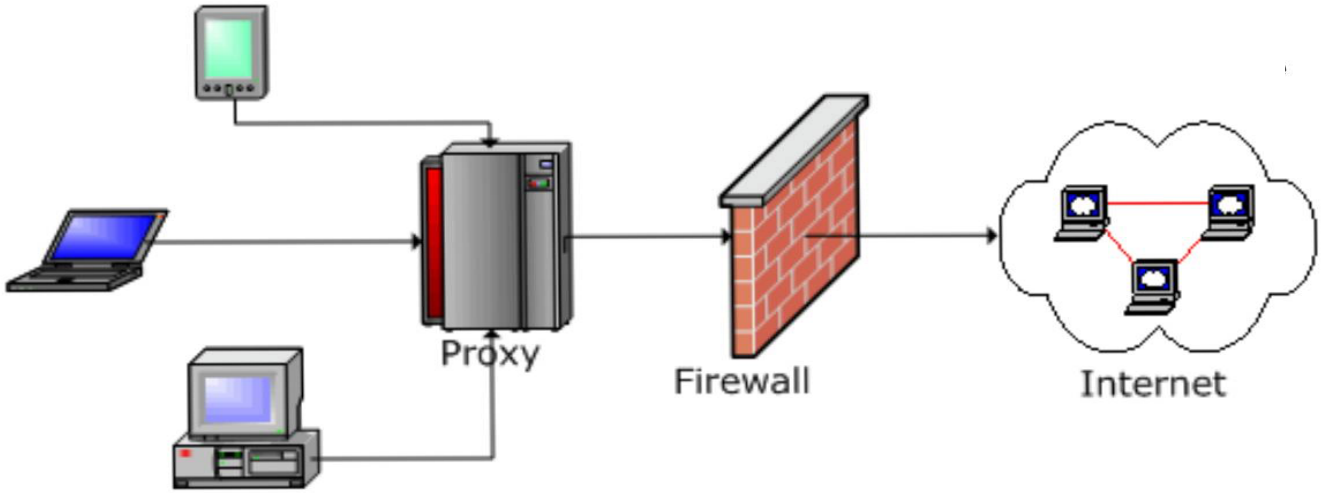
له تأثير منخفض على أداء الشبكة وسهل التنفيذ ومدعوم من قبل معظم أجهزة الراوتر و أقل تكلفة. ولكنه عرضة لانتحال IP.

جدار حماية فحص حزم حسب الحالة: يتم فحص حركة المرور باستخدام معلومات الاتصال المحفوظة في جدول الحالة.

في كل مرة يتم فيها إنشاء اتصال TCP أو UDP للاتصالات الواردة أو الصادرة ، يسجل جدار الحماية المعلومات في جدول الحالة لهذا التدفق المحدد. فعندما يتم الاتصال بين جهاز داخل شبكة المنظمة وخادم خارجي يصبح الاتصال وتبادل المعلومات مسموحًا. أدائه افضل من جدار حماية فحص الحزم وغير معرض لانتحال IP.

جدار حماية بروكسي و الشخصي و الهايبرد

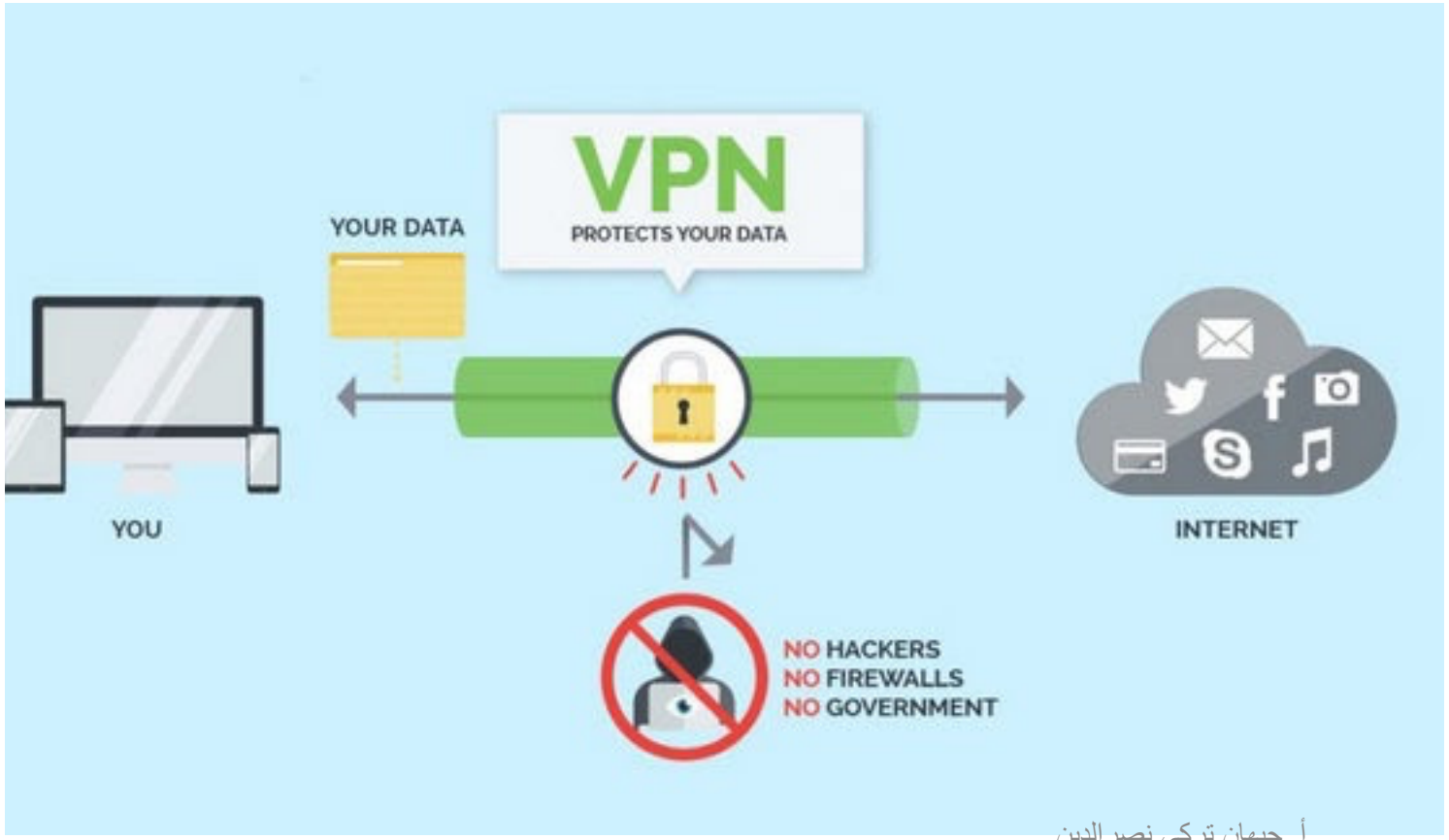
جدار الحماية البروكسي: نظام أمان للشبكة يحمي موارد الشبكة عن طريق تصفية الرسائل في الطبقة ٣ و ٤و ٥و ٧ و يعمل كوسيط بين العملاء الداخليين داخل الشبكة الموثوقة والخوادم على الإنترنت.



جدار الحماية المستند إلى المضيف (الخادم والشخصي) – جهاز كمبيوتر شخصي أو خادم به برنامج جدار حماية يعمل عليه.

جدار الحماية الهجين : مزيج من أنواع جدار الحماية المتنوعة. يجمع جدار حماية فحص الحالة وجدار حماية بوابة التطبيق (البروكسي).

الشبكة الخاصة الافتراضية



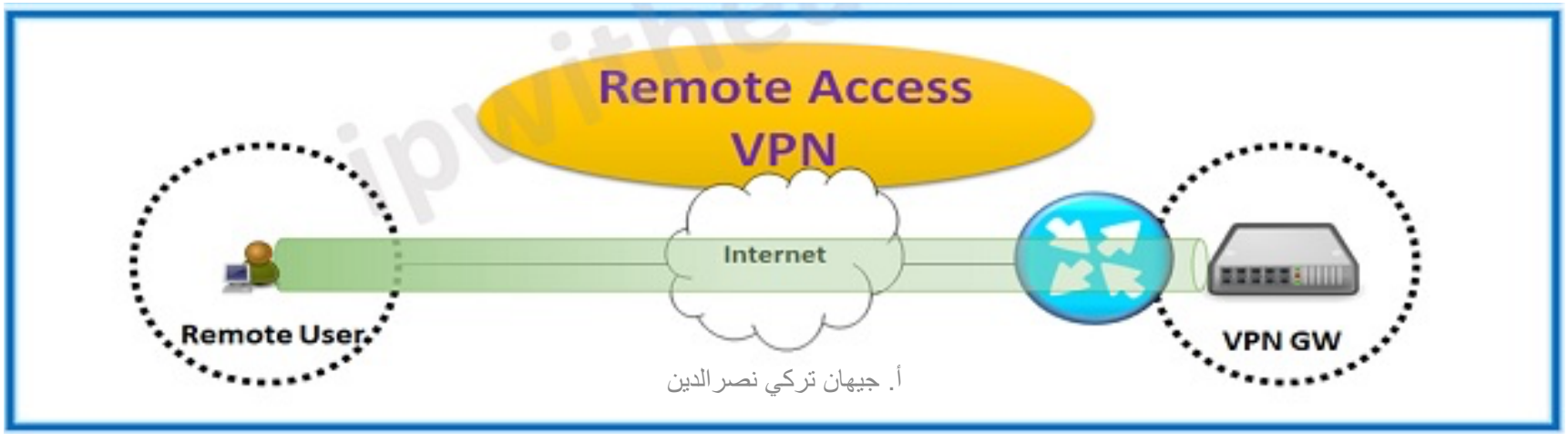
هي شبكة خاصة تنشأ على الشبكة العامة (الانترنت) و توفر امان عالي باستخدام بروتوكول التشفير المتقدم والمصادقة للحفاظ على سرية البيانات ولها قابلية التطوير بحيث يمكن اضافة المستخدمين دون الحاجة لتوسيع البنى التحتية.

أنواع الشبكة الخاصة الافتراضية

Remote access الوصول عن بعد: هو اتصال مؤقت بين المستخدمين والمقر الرئيسي ، وعادة ما يستخدم للوصول إلى تطبيقات مركز البيانات.

لها بوابة VPN واحدة و تستخدم IPSEC and SSL

يعد الكمبيوتر الشخصي للكمبيوتر الشخصي مسؤولاً عن إنشاء VPN. يقوم المستخدم البعيد بتشغيل عميل VPN الذي يربطه ببوابة VPN داخل شبكة المؤسسة.



أنواع الشبكة الخاصة الافتراضية

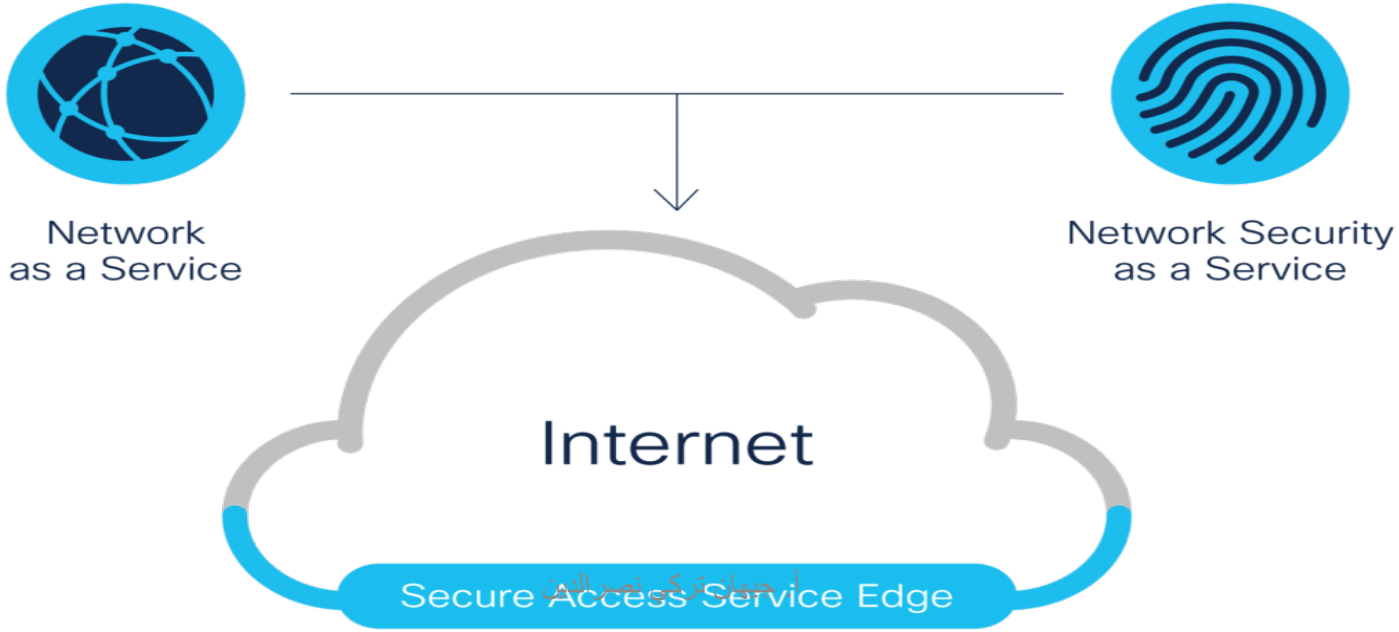
Site-to site من موقع لآخر :هو اتصال دائم بين شبكتين أو أكثر ، مثل شبكة الشركة وشبكة المكتب الفرعي.

لها بوابتين VPN وتستخدم IPSEC

بوابة VPN الاولى مسؤولة عن تغليف وتشفير حركة المرور الصادرة من موقع معين وإرسالها عبر نفق VPN عبر الإنترنت إلى بوابة VPN نظيرة في الموقع الآخر. عند الاستلام ، تقوم بوابة VPN النظيرة بتجريد الرؤوس وفك تشفير المحتوى وترحيل الحزمة نحو المضيف الهدف داخل شبكتها الخاصة.

حافة خدمة الوصول الآمن
Secure Access Service Edge

مصطلح يجمع العديد من خدمات الشبكات و تقنيات الأمان في عرض واحد والهدف منه هو تقديم خدمة شبكات آمنة في مكان يتصل منه المستخدمين.



أنظمة و تقنيات حماية الشبكات

حماية الشبكات

تطبيقات امان البريد الالكتروني: توفر حماية سريعة للبريد الإلكتروني و تمنع الهجمات الواردة وتتحكم في الرسائل الصادرة لمنع فقدان البيانات الحساسة.

مكافح الفايروسات: برامج توفر الحماية للأنظمة من البرمجيات الضارة مثل الفايروسات والديدان وبرمجيات الفدية والتجسس الموجودة في الانظمة والشبكة.

تقسيم الشبكة: يسمح بتصنيف حركة المرور في الشبكة و تعيين صلاحيات الوصول بناء على الأجهزة، وفرض السياسيات بشكل اسهل.

امان التطبيقات: الاجراءات الامنية على مستوى التطبيق والتي تهدف الى منع البيانات او الاكواد البرجمية داخل التطبيق من السرقة و الاختراق.

حماية الشبكات

امان السحابات: مجموعة واسعة من التقنيات والسياسات والتطبيقات المطبقة للدفاع عناوين IP والخدمات والتطبيقات والبيانات الضرورية الأخرى عبر الإنترنت.

نظام منع التسلل: يقوم بعملية تحليل الحزم بناء على التوقيع ويقوم بتنفيذ ردة فعل معينة مثل عمل اسقاط للحزم الضارة.

امان الاجهزة المحمولة: التدابير المصممة لحماية المعلومات الحساسة المخزنة او المرسلة على و الى أجهزة الكمبيوتر المحمولة والهواتف الذكية والأجهزة اللوحية وغيرها .

امان الويب: التحكم في استخدام الموظفين للويب، ومنع تهديدات الويب ، ومنع الوصول إلى مواقع الويب الضارة.

اختبارات أمان الشبكة

اختبار دوري على الشبكة يكشف عن نقاط الضعف والتهديدات والمخاطر المحتملة، هدفه ضمان عمل الشبكة بالشكل المتوقع وإمكانية مواجهة التهديدات.

- اختبار الاختراق
- فحص الشبكة
- فحص الثغرات
- اختراق كلمات السر
- فحص السلامة
- كاشف الفايروسات

اختبارات امان الشبكة

اختبار الاختراق Penetration testing : يحاكي الهجمات الضارة ويحدد احتمالية حدوثها و العواقب المحتملة الناتج عنها.

فحص الشبكة Network scanning: برامج تختبر اتصال أجهزة الكمبيوتر و تستكشف المنافذ المفتوحة والمصادر المتوفرة

فحص الثغرات Vulnerability scanning: برامج تحدد نقاط الضعف في الأنظمة مثل التهيئة الخاطئة او التعريف الخاطئ، و الأرقام السرية الفارغة او احتمالية حدوث هجمات حجب الخدمة.

اختبارات امان الشبكة

اختراق كلمات السر Password cracking: برامج تستخدم لاختبار واكتشاف كلمات المرور الضعيفة التي يجب تغييرها.

فحص السلامة Integrity check: يكتشف نظام التحقق من السلامة التغييرات في النظام ويبلغ عنها.

كاشف الفايروسات Virus Detection: برامج تكتشف وتحدد وتزيل الفايروسات والبرامج الضارة الاخرى من الأنظمة.

للتواصل

@GehanTN