مقدمة : في العصر الرقمي الذي نعيش فيه , اصبح الأمن السيبراني (cyber Security) و الخصوصية من أولويات الأفراد و المؤسسات على حد سواء , من هنا تبرز أهمية شبكة VPN(الشبكة الإفتراضية الخاصة) التي توفر حلا فعالا لحماية البيانات و ضمان تصفح أمن على الأنترنت . اخفاء الهوية , و حماية المعلومات من الاختراق أثناء نقلها عبر الأنترنت. بالإضافة إلى ذلك نستخدم شبكة VPN للوصول الى المحتوى جغرافيا و توفير بيئة عمل آمنة للموظفين عن بعد , مما يعزز الكفاءة و الإنتاجية في المؤسسات . في ظل هذه الفوائد أصبحت شبكة VPN أداة أساسية في مواجهة التحديات الرقمية و تحقيق الآمان و المرونة في الإستخدام الإلكتروني تقنية الشبكات الخاصة الافتراضية VPN العامة: الشبكات الخاصة الافتراضية VPN: مهما كان اتصال الحاسوب بالإنترنت، سلكيا أو لا سلكيا "Wi-Fi"، فان تشفير خدمة الـ VPN للبيانات تمنع الرقابة والتتبع. وبالتالي فإن شبكة VPN تسمح لك بتصفح الإنترنت بشكل مجهول وآمن من أي مكان. وتعمل الشبكات الافتراضية الخاصة على حمايتك من خلال إنشاء نفق مشفر يربط جهاز الكمبيوتر الخاص بك بشبكة الإنترنت، وبنقاط اتصال Wi-Fi وغيرها من الشبكات. إذاً الشبكة الخاصة الافتراضية تنشئ اتصال شبكة خاصًا بين الأجهزة من خلال الإنترنت. وتُستخدم VPN في نقل البيانات بأمان مع إخفاء الهوية عبر الشبكات العامة. وتعمل عن طريق إخفاء عناوين IP وتشفير البيانات بحيث تكون غير قابلة للقراءة إلا من قِبل الشخص المصرح باستلامها. وبذلك فإن خلاصة القول إن الـ VPN هي شبكة افتراضية خاصة مبنيّة داخل شبكة الانترنت العام التقنيات الرئيسية في 1-2 : VPN بروتوكولات النفق: تعتمد الشبكات الافتراضية الخاصة على بروتوكولات النفق لتغليف البيانات وتشفيرها لضمان نقلها بأمان. من بين البروتوكولات الشائعة: ـ OpenVPN : بروتوكول مفتوح المصدر يتميز بمستوى أمان عالٍ ويدعم معايير تشفير متعددة. ـ IPSec (أمان بروتوكول الإنترنت): غالبًا ما يقترن بـ L2TP أو IKEv2 لتوفير تشفير قوي وتبادل مفاتيح آمن. ـ WireGuard : بروتوكول حديث وخفيف يوفر سرعات أعلى وقاعدة كود مبسطة. ـ PPTP (بروتوكول النفق نقطة إلى نقطة): بروتوكول أقدم يتميز بالسرعة لكنه أقل أمانًا مقارنة بالخيارات الأحدث. ـ SSTP (بروتوكول نفق المقبس الآمن): بروتوكول طورته مايكروسوفت ويعمل بشكل جيد مع الجدران النارية. 2.1. معايير التشفير : تعتمد الشبكات الافتراضية الخاصة على التشفير لحماية البيانات AES (معيار التشفير المتقدم): عادةً AES-256 لضمان مستوى عالٍ من الأمان . 2.2 .I. تقنيات الخوادم : ـ الخوادم المموهة: مصممة لتجاوز آليات حظر الشبكات الافتراضية الخاصة. 2.3 .I. آليات المصادقة لتأمين الاتصالات، تعتمد الشبكات الافتراضية الخاصة على: ـ المفاتيح المشتركة مسبقًا (PSK): شكل بسيط من المصادقة يُستخدم غالبًا في الإعدادات الصغيرة. I. تقنيات توجيه البيانات ـ النفق الكامل (Full Tunneling): تمر جميع حركة المرور عبر الشبكة الافتراضية، مما يزيد الخصوصية إلى الحد الأقصى. تضمن عدم حدوث تسرب للبيانات من خلال فصل الاتصال بالإنترنت تلقائيًا إذا انقطع اتصال 2 .2.5 .I VPN. تجاوز القيود الجغرافية: الوصول إلى محتوى محجوب حسب المنطقة مثل خدمات البث. العمل عن بُعد: توفير وصول آمن إلى شبكات الشركات. حماية شبكات الواي فاي العامة: تأمين البيانات على الشبكات غير الآمنة. 3. النظرة الفيزيائية : من الناحية الفيزيائية، 3.1 .I. أجهزة التوجيه وبوابات 2 VPN. – تُعتبر بوابات VPN) VPN Gateways) أجهزة شبكة تعمل كنقاط دخول أو خروج للاتصالات عبر الشبكة الافتراضية الخاصة، 3.2 .I. خوادم VPN – توجد هذه الخوادم في مراكز البيانات وتعمل كوسيط بين المستخدم وشبكة الإنترنت. ـ يقوم مقدمو خدمات VPN بتشغيل آلاف الخوادم حول العالم لتوفير اتصالات سريعة وآمنة وقادرة على تجاوز القيود الجغرافية. ـ في بعض الحالات، يتم استبدال الخوادم الفعلية بخوادم افتراضية، خاصة في البيئات السحابية. 3.3 .I. أجهزة الحواسيب المكتبية والمحمولة: تحتاج إلى برامج VPN مثبتة. I. المعدات التشفيرية ـ تستخدم بعض الأنظمة معالجات مخصصة لإجراء عمليات التشفير وفك التشفير الخاصة بـ VPN، مما يحسن الأداء ويقلل من الضغط على المعالجات العامة. 3.5. ـ مزودو خدمات الإنترنت (ISP): تمر بيانات الـ VPN عبر بنية مزودي خدمات الإنترنت قبل الوصول إلى خوادم الـ VPN. ونقاط الوصول، والألياف الضوئية التي تنقل البيانات. 4. 1-إنشاء الاتصال يبدأ المستخدم الاتصال عبر جهازه (عميل VPN). ثم يتم إرسال الطلب إلى خادم VPN عبر البنية التحتية للشبكة (مثل أجهزة التوجيه والكابلات). 2 ـالنفق الخاص بـ VPN:يُعتبر النفق اتصالًا منطقيًا، ولكن البيانات تُنقل فعليًا عبر أجهزة التوجيه والمحولات والكابلات على شبكة الإنترنت. 3-التشفير والنقل :يتم تشفير البيانات على جهاز المستخدم، حيث يتم فك تشفيرها بواسطة خادم VPN وإرسالها إلى الوجهة النهائية. يعتمد الجانب الفيزيائي لشبكات VPN على: البنية التحتية للشبكة (الخوادم، الكابلات، أجهزة التوجيه). أجهزة التوجيه، الهواتف الذكية). مراكز البيانات لاستضافة خوادم 1 – 3 .VPNعرض افتراضي من الناحية الافتراضية، تعمل الشبكة الافتراضية الخاصة (VPN – Virtual Private Network) كوسيط بين المستخدم

والإنترنت عبر إنشاء بيئة رقمية آمنة وموثوقة تتيح نقل البيانات بشكل مشفر عبر الشبكات العامة. يُركز الجانب الافتراضي لـ VPN على البروتوكولات، والأنظمة البرمجية التي تُسهل العمليات دون الحاجة إلى تغييرات فيزيائية كبيرة. 1.5. 3 ـ
1-1المكونات الافتراضية لشبكة VPN البروتوكولات هي مجموعة من القواعد التي تحدد كيفية إنشاء الاتصال ونقل البيانات بين المستخدم وخادم ـ WireGuard: بروتوكول خفيف وسريع مصمم ليكون بديلاً متطورًا للبروتوكولات التقليدية. ـ
L2TP/IPSec: يجمع بين بروتوكول النفق (L2TP) والتشفير (IPSec). التشفير هو الركيزة الأساسية في الجانب الافتراضي لـ VPN، – AES (Advanced Encryption Standard): معيار شائع يُستخدم غالبًا بـ 256 بت للأمان العالي. شائع في تطبيقات VPN للأجهزة المحمولة. ـ Handshake Encryption: لضمان إنشاء اتصال آمن بين المستخدم والخادم. 3-1-3النفق الافتراضي ـ النفق الافتراضي هو مسار مشفر يتم إنشاؤه بين جهاز المستخدم وخادم VPN، مما يجعل البيانات غير قابلة للقراءة من قبل أي جهة خارجية. ـ يتم إنشاء هذا النفق عبر الإنترنت باستخدام البروتوكولات والتشفير، في البيئة الافتراضية، المصادقة (Authentication): باستخدام كلمات مرور أو شهادات رقمية. ـ إدارة الجلسات (Session Management): لضمان فصل المستخدمين ومنع أي تداخل. توجيه البيانات الافتراضي يتم توجيه حركة المرور من خلال خوادم VPN الافتراضية باستخدام: .I 3-2 كيفية عمل VPN من الناحية الافتراضية؟ 1. إنشاء الاتصال يقوم المستخدم بتشغيل تطبيق VPN أو خدمة مدمجة في النظام. يتم إرسال طلب إنشاء الاتصال إلى خادم VPN الافتراضي. 2. التفاوض على التشفير:يتفق جهاز المستخدم والخادم على بروتوكول التشفير والمفاتيح اللازمة لتأمين الاتصال. 3. إنشاء النفق يتم إنشاء مسار افتراضي لنقل البيانات، ويُستخدم التشفير لضمان أن البيانات المرسلة والمستقبلة غير قابلة للاختراق. 4. نقل البياناتيتم توجيه البيانات من المستخدم إلى خادم VPN ثم إلى وجهتها النهائية. 5. يتم فك تشفير البيانات من قبل خادم VPN قبل إرسالها إلى الإنترنت المفتوح. 5.3 .I. إخفاء الهوية الافتراضي: عن طريق استبدال عنوان IP الحقيقي بعنوان خادم VPN. التجاوز الافتراضي للقيود: يسمح للمستخدمين بالوصول إلى محتوى محظور أو خاضع لقيود جغرافية. 4 (a-تحديد التهديدات ومشاكل الأمان المتعلقة بالشبكات الافتراضية الخاصة (VPN) تم تصميم الشبكات الافتراضية الخاصة (VPN) لضمان الخصوصية والأمان عبر الإنترنت. ومع ذلك، فإنها ليست خالية من التهديدات والثغرات. تكوينات غير صحيحة قد يؤدي التكوين غير الصحيح إلى: ـ أنفاق غير مشفرة تعرض البيانات الحساسة. ـ إعداد أذونات غير صحيحة يسمح بوصول غير مصرح به. استخدام بروتوكولات قديمة بعض البروتوكولات، مثل PPTP، توفر مستوى أمان ضعيف وتكون عرضة لهجمات حديثة (مثل الهجمات بالقوة الغاشمة). كلمات مرور ضعيفة 4-1 i تسريبات البيانات وكشف الهوية تسريبات عنوان IP : عندما يفشل الـ VPN في إخفاء عنوان IP الخاص بالمستخدم، عدم وجود ميزة Kill Switch : إذا فشلت الاتصال بالـ 4-2 1 ،VPN ثغرات برمجية: تطبيقات VPNضارة: بعض خدمات VPN المجانية أو المشبوهة قد تحتوي على برمجيات خبيثة أو تجمع وتبيع بيانات المستخدمين. 1 3-4 تهديدات متعلقة بخوادم VPN: