و الخصوصية من أولويات الأفراد و (cyber Security) مقدمة : في العصر الرقمي الذي نعيش فيه , اصبح الأمن السيبراني الشبكة الإفتراضية الخاصة) التي توفر حلا فعالا لحماية البيانات و)VPN المؤسسات على حد سواء , من هنا تبرز أهمية شبكة ضمان تصفح أمن على الأنترنت . اخفاء الهوية , و حماية المعلومات من الاختراق أثناء نقلها عبر الأنترنت. بالإضافة إلى ذلك للوصول الى المحتوى جغرافيا و توفير بيئة عمل آمنة للموظفين عن بعد , مما يعزز الكفاءة و الإنتاجية في VPN نستخدم شبكة أداة أساسية في مواجهة التحديات الرقمية و تحقيق الآمان و المرونة في VPN المؤسسات . في ظل هذه الفوائد أصبحت شبكة مهما كان اتصال :VPN العامة: الشبكات الخاصة الافتراضية VPN الإستخدام الإلكتروني تقنية الشبكات الخاصة الافتراضية للبيانات تمنع الرقابة والتتبع. وبالتالي فإن شبكة VPN فان تشفير خدمة الـ ،"Wi-Fi" الحاسوب بالإنترنت، سلكيا أو لا سلكيا تسمح لك بتصفح الإنترنت بشكل مجهول وآمن من أي مكان. وتعمل الشبكات الافتراضية الخاصة على حمايتك من خلال VPN وغيرها من الشبكات. إذاً الشبكة Wi-Fi إنشاء نفق مشفر يربط جهاز الكمبيوتر الخاص بك بشبكة الإنترنت، وبنقاط اتصال في نقل البيانات بأمان مع إخفاء VPN الخاصة الافتراضية تنشئ اتصال شبكة خاصًا بين الأجهزة من خلال الإنترنت. وتُستخدم وتشفير البيانات بحيث تكون غير قابلة للقراءة إلا من قِبل IP الهوية عبر الشبكات العامة. وتعمل عن طريق إخفاء عناوين هي شبكة افتراضية خاصة مبنيّة داخل شبكة الانترنت العام VPN الشخص المصرح باستلامها. وبذلك فإن خلاصة القول إن الـ بروتوكولات النفق: تعتمد الشبكات الافتراضية الخاصة على بروتوكولات النفق لتغليف البيانات 1-2 : VPN التقنيات الرئيسية في بروتوكول مفتوح المصدر يتميز بمستوى أمان : OpenVPN ـ :وتشفيرها لضمان نقلها بأمان. من بين البروتوكولات الشائعة لتوفير تشفير قوي IKEv2 أو L2TP أمان بروتوكول الإنترنت): غالبًا ما يقترن بـ) IPSec ـ .عالٍ ويدعم معايير تشفير متعددة بروتوكول) PPTP ـ .بروتوكول حديث وخفيف يوفر سرعات أعلى وقاعدة كود مبسطة : WireGuard ـ .وتبادل مفاتيح آمن بروتوكول نفق المقبس) SSTP ـ .النفق نقطة إلى نقطة): بروتوكول أقدم يتميز بالسرعة لكنه أقل أمانًا مقارنة بالخيارات الأحدث الآمن): بروتوكول طورته مايكروسوفت ويعمل بشكل جيد مع الجدران النارية. 2.1. معايير التشفير : تعتمد الشبكات الافتراضية .I. 2.2 . لضمان مستوى عالٍ من الأمان AES-256 معيار التشفير المتقدم): عادةً) AES الخاصة على التشفير لحماية البيانات آليات المصادقة لتأمين .I. 2.3 .تقنيات الخوادم : ـ الخوادم المموهة: مصممة لتجاوز آليات حظر الشبكات الافتراضية الخاصة شكل بسيط من المصادقة يُستخدم :(PSK) الاتصالات، تعتمد الشبكات الافتراضية الخاصة على: ـ المفاتيح المشتركة مسبقًا تمر جميع حركة المرور عبر الشبكة :(Full Tunneling) تقنيات توجيه البيانات ـ النفق الكامل .I .غالبًا في الإعدادات الصغيرة الافتراضية، مما يزيد الخصوصية إلى الحد الأقصى. تضمن عدم حدوث تسرب للبيانات من خلال فصل الاتصال بالإنترنت تلقائيًا تجاوز القيود الجغرافية: الوصول إلى محتوى محجوب حسب المنطقة مثل خدمات البث. 2. 2.5. I VPN إذا انقطع اتصال العمل عن بُعد: توفير وصول آمن إلى شبكات الشركات. حماية شبكات الواي فاي العامة: تأمين البيانات على الشبكات غير VPN) تُعتبر بوابات – .2 VPN أجهزة التوجيه وبوابات .I. 3.1 ،الآمنة. 3. النظرة الفيزيائية : من الناحية الفيزيائية – VPN خوادم .I. 3.2 ،أجهزة شبكة تعمل كنقاط دخول أو خروج للاتصالات عبر الشبكة الافتراضية الخاصة (Gateways بتشغيل آلاف VPN توجد هذه الخوادم في مراكز البيانات وتعمل كوسيط بين المستخدم وشبكة الإنترنت. ـ يقوم مقدمو خدمات الخوادم حول العالم لتوفير اتصالات سريعة وآمنة وقادرة على تجاوز القيود الجغرافية. ـ في بعض الحالات، يتم استبدال الخوادم VPN أجهزة الحواسيب المكتبية والمحمولة: تحتاج إلى برامج .I. 3.3 .الفعلية بخوادم افتراضية، خاصة في البيئات السحابية ،VPN المعدات التشفيرية ـ تستخدم بعض الأنظمة معالجات مخصصة لإجراء عمليات التشفير وفك التشفير الخاصة بـ .I .مثبتة عبر بنية VPN تمر بيانات الـ :(ISP) مما يحسن الأداء ويقلل من الضغط على المعالجات العامة. 3.5. ـ مزودو خدمات الإنترنت ونقاط الوصول، والألياف الضوئية التي تنقل البيانات. 4. 1-إنشاء .VPN. مزودي خدمات الإنترنت قبل الوصول إلى خوادم الـ عبر البنية التحتية للشبكة (مثل VPN ثم يتم إرسال الطلب إلى خادم .(VPN الاتصال يبدأ المستخدم الاتصال عبر جهازه (عميل يُعتبر النفق اتصالًا منطقيًا، ولكن البيانات تُنقل فعليًا عبر أجهزة التوجيه:VPN أجهزة التوجيه والكابلات). 2 ـ النفق الخاص بـ والمحولات والكابلات على شبكة الإنترنت. 3-التشفير والنقل :يتم تشفير البيانات على جهاز المستخدم، حيث يتم فك تشفيرها على: البنية التحتية للشبكة (الخوادم، VPN وإرسالها إلى الوجهة النهائية. يعتمد الجانب الفيزيائي لشبكات VPN بواسطة خادم عرض افتراضي1 – 3 .VPN الكابلات، أجهزة التوجيه). أجهزة التوجيه، الهواتف الذكية). مراكز البيانات لاستضافة خوادم كوسيط بين المستخدم (VPN – Virtual Private Network) من الناحية الافتراضية، تعمل الشبكة الافتراضية الخاصة

والإنترنت عبر إنشاء بيئة رقمية آمنة وموثوقة تتيح نقل البيانات بشكل مشفر عبر الشبكات العامة. يُركز الجانب الافتراضي للـ VPN ـ 3 .5.1 على البروتوكولات، والأنظمة البرمجية التي تُسهل العمليات دون الحاجة إلى تغييرات فيزيائية كبيرة. المكونات الافتراضية لشبكة VPN 1–1 البروتوكولات هي مجموعة من القواعد التي تحدد كيفية إنشاء الاتصال ونقل البيانات بين ـ المستخدم وخادم WireGuard: التقليدية للبروتوكولات متطورًا بديلاً ليكون وسريع مصمم خفيف بروتوكول. ـ L2TP/IPSec: النفق بروتوكول بين يجمع (L2TP) والتشفير (IPSec). للـ الافتراضي الجانب في الأساسية الركيزة هو التشفير AES (Advanced Encryption Standard): تطبيقات في شائع غالبًا يُستخدم بت للأمان العالي. شائع معيار VPN، – للأجهزة المحمولة VPN لضمان إنشاء اتصال آمن بين المستخدم والخادم. 3–1–3 النفق: Handshake Encryption ـ مما يجعل البيانات غير قابلة للقراءة، VPN الافتراضي ـ النفق الافتراضي هو مسار مشفر يتم إنشاؤه بين جهاز المستخدم وخادم من قبل أي جهة خارجية. ـ يتم إنشاء هذا النفق عبر الإنترنت باستخدام البروتوكولات والتشفير، في البيئة الافتراضية، المصادقة لضمان فصل :(Session Management) باستخدام كلمات مرور أو شهادات رقمية. ـ إدارة الجلسات :(Authentication) I. :الافتراضية باستخدام VPN المستخدمين ومنع أي تداخل. توجيه البيانات الافتراضي يتم توجيه حركة المرور من خلال خوادم أو خدمة مدمجة في VPN من الناحية الافتراضية؟ 1. إنشاء الاتصال يقوم المستخدم بتشغيل تطبيق VPN كيفية عمل 2–3 الافتراضي. 2. التفاوض على التشفير:يتفق جهاز المستخدم والخادم على VPN النظام. يتم إرسال طلب إنشاء الاتصال إلى خادم بروتوكول التشفير والمفاتيح اللازمة لتأمين الاتصال. 3. إنشاء النفق يتم إنشاء مسار افتراضي لنقل البيانات، ويُستخدم التشفير ثم VPN لضمان أن البيانات المرسلة والمستقبلة غير قابلة للاختراق. 4. نقل البياناتيتم توجيه البيانات من المستخدم إلى خادم إخفاء الهوية .I. 5.3 .قبل إرسالها إلى الإنترنت المفتوح VPN إلى وجهتها النهائية. 5. يتم فك تشفير البيانات من قبل خادم التجاوز الافتراضي للقيود: يسمح للمستخدمين بالوصول .VPN الحقيقي بعنوان خادم IP الافتراضي: عن طريق استبدال عنوان تحديد التهديدات ومشاكل الأمان المتعلقة بالشبكات الافتراضية الخاصة–4 (a .إلى محتوى محظور أو خاضع لقيود جغرافية لضمان الخصوصية والأمان عبر الإنترنت. ومع ذلك، فإنها ليست خالية (VPN) تم تصميم الشبكات الافتراضية الخاصة (VPN) 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 4–1 i توفر مستوى أمان ضعيف وتكون عرضة لهجمات حديثة (مثل الهجمات بالقوة الغاشمة). كلمات مرور ضعيفة، PPTP الخاص بالمستخدم، عدم IP في إخفاء عنوان VPN عندما يفشل الـ : IP تسريبات البيانات وكشف الهوية تسريبات عنوان VPN ضارة: بعض خدماتVPN ثغرات برمجية: تطبيقات 4–2 1، VPN إذا فشلت الاتصال بالـ : Kill Switch وجود ميزة VPN: المجانية أو المشبوهة قد تحتوي على برمجيات خبيثة أو تجمع وتبيع بيانات المستخدمين. 1 3–4 تهديدات متعلقة بخوادم