

والأمان هدفت هذه الدراسة إلى إظهار مرونة وفعالية تقنية VPN وبروتوكولات (VPN) حول الشبكة الافتراضية الخاصة (2018) من حيث التكلفة والأمان، حيث تم تصميمها لمعالجة المشاكل المحيطة بالأعمال والاتجاه نحو زيادة العمل عن بعد (VPN) والعمليات الموزعة عالمياً على نطاق واسع؛ حيث يمكن للمستخدمين الوصول إلى الموارد والخدمات بشكل آمن. كما صنفت ومجموعة من خوارزميات التشفير والمصادقة والتكامل، وخلصت الدراسة إلى أنه من (VPN) هذه الدراسة الأنواع المختلفة لـ باستخدام (VPN) المهم أن تتناسب المعايير المختارة احتياجات العميل. (2019) تحليل شبكة الأمان الافتراضية الخاصة ناقشت هذه الدراسة معايير مختلفة مثل أمان البيانات والكفاءة وجودة الشبكة باستخدام تقنية الشبكة الافتراضية OpenVPN وخلصت هذه الدراسة إلى أن هناك أماناً متزايداً للبيانات يمكن إثباته من خلال نتيجة اختبار البيانات، (OpenVPN) الخاصة مع عن طريق إرسال البيانات في شكل اسم مستخدم وكلمة المرور، والنتيجة التي تم الحصول عليها (Wireshark) باستخدام برنامج لا يمكن (OpenVPN) يمكن رؤية واكتشاف اسم مستخدم وكلمة مرور ولكن بعد استخدام (OpenVPN) هي أنه قبل استخدام وبالتالي فهي آمنة، كما قامت الدراسة بقياس (OpenVPN) الكشف عن بيانات كلمة المرور، أي أن البيانات تم تشفيرها بواسطة جودة الخدمة، ف لوحظ انخفاض جودة الشبكة وزيادة معاملات التأخير وكذلك انخفاض معدل النقل وعرض النطاق الترددي وذلك بسبب عملية التشفير والتغليف التي تستغرق وقتاً طويلاً، هيكلية البحث: ٩ المبحث الأول: الأمن السيبراني والشبكة في تعزيزه • المطلب الثاني: VPN الافتراضية الخاصة • المطلب الأول: الأمن السيبراني ودور الشبكة الافتراضية الخاصة • VPN مميزات وعيوب الشبكة الافتراضية الخاصة • المطلب الثالث: المخاوف والتهديدات الأمنية للشبكة الافتراضية الخاصة المبحث الثاني: مفهوم الأمان والخصوصية في الشبكة الافتراضية ١٠ VPN المطلب الرابع: أنواع الشبكات الافتراضية الخاصة المبحث الأول: الأمن السيبراني والشبكة VPN المطلب الأول: بروتوكولات الشبكة الافتراضية • VPN الخاصة VPN نموذج قائم على الاشتراكات، أي يجب على المستخدم الاشتراك وطلب الخدمة من مزود VPN الافتراضية الخاصة تعتبر الخاص وإخفاء هوية المستخدم على مواقع الويب والتطبيقات والخدمات IP يتم تغيير عنوان VPN والتسجيل، وعند استخدام من نقطة إلى نقطة بين جهاز المستخدم وخادم ما، ويتم استمرار نقل البيانات عبر VPN التي تتعقب المستخدمين؛ ويتم اتصال اتصال خاص مما يسمح للمستخدم بالعمل على الطريق أو من المنزل خلال اتصال آمن بهذا الخادم البعيد. أي أن الهدف هو إضافة مستوى من الأمان عند تبادل البيانات من خلال الأنفاق وذلك بتشفير البيانات من جانب المرسل VPN الأساسي من وتوجيهها عبر النفق ومن ثم فك التشفير من جانب المستقبل؛ كما يمكن توسيع الشبكات الخاصة عبر الشبكات العامة مع الحفاظ على الأمن،