

2018) حول الشبكة الافتراضية الخاصة (VPN) وبروتوكولات VPN والأمان هدفت هذه الدراسة إلى إظهار مرونة وفعالية تقنية (VPN) من حيث التكلفة والأمان، حيث تم تصميمها لمعالجة المشاكل المحيطة بالأعمال والاتجاه نحو زيادة العمل عن بعد والعمليات الموزعة عالمياً على نطاق واسع؛ حيث يمكن للمستخدمين الوصول إلى الموارد والخدمات بشكل آمن. كما صنفت هذه الدراسة الأنواع المختلفة لـ (VPN) ومجموعة من خوارزميات التشفير والمصادقة والتكامل، وخلصت الدراسة إلى أنه من المهم أن تتناسب المعايير المختارة احتياجات العميل. (2019) تحليل شبكة الأمان الافتراضية الخاصة (VPN) باستخدام OpenVPN ناقشت هذه الدراسة معايير مختلفة مثل أمان البيانات والكفاءة وجودة الشبكة باستخدام تقنية الشبكة الافتراضية الخاصة مع (OpenVPN)، وخلصت هذه الدراسة إلى أن هناك أماناً متزايداً للبيانات يمكن إثباته من خلال نتيجة اختبار البيانات باستخدام برنامج (Wireshark) عن طريق إرسال البيانات في شكل اسم مستخدم وكلمة المرور، والنتيجة التي تم الحصول عليها هي أنه قبل استخدام (OpenVPN) يمكن رؤية واكتشاف اسم مستخدم وكلمة مرور ولكن بعد استخدام (OpenVPN) لا يمكن الكشف عن بيانات كلمة المرور، أي أن البيانات تم تشفيرها بواسطة (OpenVPN) وبالتالي فهي آمنة، كما قامت الدراسة بقياس 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، هيكلياً البحث: ٤ المبحث الأول: الأمن السيبراني والشبكة الافتراضية الخاصة • المطلب الأول: الأمن السيبراني ودور الشبكة الافتراضية الخاصة VPN في تعزيزه • المطلب الثاني: مميزات وعيوب الشبكة الافتراضية الخاصة • المطلب الثالث: المخاوف والتهديدات الأمنية للشبكة الافتراضية الخاصة VPN • المطلب الرابع: أنواع الشبكات الافتراضية الخاصة VPN ٥ المبحث الثاني: مفهوم الأمان والخصوصية في الشبكة الافتراضية الخاصة VPN • المطلب الأول: بروتوكولات الشبكة الافتراضية الخاصة VPN المبحث الأول: الأمن السيبراني والشبكة الافتراضية الخاصة تعتبر VPN نموذج قائم على الاشتراكات، أي يجب على المستخدم الاشتراك وطلب الخدمة من مزود VPN والتسجيل، وعند استخدام VPN يتم تغيير عنوان IP الخاص وإخفاء هوية المستخدم على مواقع الويب والتطبيقات والخدمات التي تتعقب المستخدمين؛ ويتم اتصال VPN من نقطة إلى نقطة بين جهاز المستخدم وخادم ما، ويتم استمرار نقل البيانات عبر اتصال خاص مما يسمح للمستخدم بالعمل على الطريق أو من المنزل خلال اتصال آمن بهذا الخادم البعيد. أي أن الهدف الأساسي من VPN هو إضافة مستوى من الأمان عند تبادل البيانات من خلال الأنفاق وذلك بتشفير البيانات من جانب المرسل وتوجيهها عبر النفق ومن ثم فك التشفير من جانب المستقبل؛ كما يمكن توسيع الشبكات الخاصة عبر الشبكات العامة مع الحفاظ على الأمن،