في IDS هي أنظمة أمنية تُستخدم لاكتشاف النشاط الضار على الشبكة. يمكن أن تساعد أنظمة (IDS) أنظمة كشف الاختراق حماية الشبكة من مجموعة متنوعة من الهجمات، قد تبحث تقنية تحليل السلوك عن مستخدم يحاول تسجيل الدخول إلى حساب اكتشاف IDS العديد من المزايا، الكشف المبكر: يمكن لأنظمة IDS باستخدام كلمة مرور خاطئة عدة مرات. تقدم أنظمة مع IDS إنشاء سجلات للنشاط المشبوهة، التكامل: يمكن دمج أنظمة IDS الهجمات في وقت مبكر، السجلات: يمكن لأنظمة مكلفة. هناك عدة أنواع من أنظمة IDS ما يلي: التكلفة: يمكن أن تكون أنظمة IDS أنظمة أخرى، تتضمن بعض سلبات أنظمة حركة مرور الشبكة بحثاً عن النشاط الضار. NIDS تراقب أنظمة: (NIDS) أنظمة كشف الاختراق المستندة إلى الشبكة، IDS النشاط على مستوى المضيف بحثاً عن النشاط HIDS تراقب أنظمة: (HIDS) أنظمة كشف الاختراق المستندة إلى المضيف السلوكيات المرئية للمستخدمين والأنظمة BIDS تراقب أنظمة: (BIDS) الضار. أنظمة كشف الاختراق المستندة إلى السلوك قادر على التعامل مع حجم الشبكة. أنظمة IDS حجم الشبكة: يجب اختيار نظام، IDS بحثاً عن النشاط الضار. عند اختيار نظام هي أداة أمنية مهمة (IPS) هي أنظمة أمنية تُستخدم لمنع النشاط الضار على الشبكة. أنظمة منع الاختراق (IPS) منع الاختراق بما في ذلك: مما يحمي الشبكة من IPS يمكن استخدامها للحماية من مجموعة متنوعة من الهجمات الإلكترونية. مزايا أنظمة مكلفة. أنواع أنظمة IPS ما يلي: التكلفة: يمكن أن تكون أنظمة IPS تتضمن بعض سلبات أنظمة IPS الأضرار. سلبات أنظمة حركة مرور الشبكة بحثاً عن النشاط NIPS تراقب أنظمة: (NIPS) بما في ذلك: أنظمة منع الاختراق المستندة إلى الشبكة IPS النشاط على مستوى المضيف بحثاً عن النشاط HIPS تراقب أنظمة: (HIPS) الضار. أنظمة منع الاختراق المستندة إلى المضيف باختلاف الحجم والميزات. الاحتياجات IPS يجب مراعاة العوامل التالية: الميزانية: تختلف تكلفة أنظمة IPS الضار. اختيار نظام أوجه التشابه كلاهما أنظمة IPS و IDS يلبي الاحتياجات الأمنية المحددة للمؤسسة. مقارنة أنظمة IPS الأمنية: يجب اختيار نظام أمنية تستخدم لمراقبة الشبكة بحثاً عن النشاط الضار. كلاهما يمكن أن يستخدم تحليل التوقيع أو تحليل السلوك لاكتشاف النشاط الضار.