अध्याय–8
ई बिजनेस सुरक्षा, गोपनीयता, और कानूनी आवश्यकताएं

यहाँ कई रणनीतियां है जो कि आपके जोखिम को कम करने में मदद करती हैं जब आप और आपके ग्राहक ऑनलाइन बिजनेस करते वक्त सामना करते हैं। इन खतरों से अवगत रहिये और इससे पहले की ये समस्या न बन जाये हमें उनसे निपटने के लिए कदम उठाने होंगे।

अपने ग्राहकों की सुरक्षा

ग्राहकों को धोखाधड़ी के खिलाफ संरक्षित करना जरुरी है क्योकि यह ऑनलाइन व्यापार मे विश्वास जमाने के लिए अतिआवश्यक हैं। वेबसाइट के सुरक्षित उपयोग के लिए सुरक्षा प्रमाणन और एन्क्रिप्शन प्रौद्योगिकी का उपयोग किया जाना चाहिए। सुरक्षा में किसी भी प्रकार की कमी को ग्राहको को तुरंत सूचित किया जाना आवश्यक होता है। सभी ग्राहकों अपनी जानकारी गोपनीय रखना चाहते हैं। जब आप अपने ग्राहकों को इलेक्ट्रॉनिक संदेश भेजते हैं, तो यह सुनिश्चित करले कि वह उनकी आवश्यकताओं के अनुरुप हो।

8.1 सुरक्षा

अपने ग्राहकों की तथा अपने कार्यों की ऑनलाइन सुरक्षा सुनिश्चित करने के लिए ये जरूरतें है।

- **व्यापार सुरक्षित रखें और साइबर सेफ रहे**– जानें कैसे अपने व्यापार और निजी जानकारी की रक्षा करें।
- **भुगतान कार्ड उद्योग सुरक्षा मानक परिषद** – अगर आप अपने व्यापार में डेबिट और क्रेडिट कार्ड इस्तेमाल करते है, तो उनकी सुरक्षा जानकारी को लागू करने के बारे में जानना चाहिए।

8.2 इंट्रानेट और एक्स्ट्रानेट सुरक्षा प्रणालिया

सुरक्षा होल्स (कमी) का पता करने के लिए एक्सट्रानेट और इंट्रानेट की विभीन्न तकनीके उपलब्ध हैं। एक विशेष तकनीक को चुनने से पहले यह जरूरी है कि उस सिस्टम की सुरक्षा के बारे में पता होना आवश्यक हैं। सिस्टम सुरक्षा के लिये निम्नलिखित बाते महत्वपूर्ण हैं:

- **प्रमाणीकरण (Authentication)** – प्रमाणीकरण यह सुनिश्चित करता है की जो निकाय (ऐन्टीटी) सन्देश भेज रही है, प्राप्त कर रही है या सिस्टम तक पहुँच रही है, यह ओथेन्टिक है। और उसे कार्य करने के लिए विशेष अधिकार प्राप्त है।

- **गोपनीयता (Privacy)** – इसमे केवल एक नियत प्राप्तकर्ता ही एन्क्रिप्टेड संदेश देख सकता हैं।
- **सामग्री अखंडता (Content Integrity)** – सामग्री अखंडता यह गारंटी देता है कि जो सन्देश भेजा गया है, वह किसी अन्य पक्ष द्वारा बदला नहीं गया है।
- **गैर परित्याग (Non- Repudiation)** – गैर परित्याग यह बताता है कि सन्देश भेजने वाला यह दावा नही कर सके की उसने यह सन्देश नही भेजा है।
    - **उपयोग की सरलता** – यह सुनिश्चि करता है कि सुरक्षा व्यवस्था किसी भी एप्लीकेशन के लिए सरलता से उपयोग मे लिया जा सकता है।

8.3 इंट्रानेट और एक्स्ट्रानेट के लाभ

इंट्रानेट और एक्स्ट्रानेट लागत को कम करने और कई मायनों में संचालन में सुधार, करते हैं, जिनमें शामिल हैं:

- **जानकारी के वितरण की लागत को कम करना** – इंट्रानेट नीतियों, प्रक्रियाओं, और कर्मचारियों तक कंपनी न्यूज का कर्मचारियों तक वितरण तेजी से और आसानी से करती है। एक्सट्रानेट ऑनलाइन कैटलॉग और मूल्य सूचियों का वितरण सस्ता और आसान बनाती है।
- **प्रशासनिक लागत कम** – इंट्रा/एक्सट्रानेट की इंटरैक्टिव क्षमताओं के माध्यम से उपयोगकर्ता उन कार्यों को स्वयं करने मे सक्षम हो गए हैं जिनमे प्रशासनिक सहायता की जरूरत पड़ती थी।
- **सुधार के सहयोग** –इंट्रा / एक्स्ट्रानेट का उपयोग कर उपयोगकर्ताओं आभासी, ऑनलाइन टीमों के लिए अधिक उत्पादक बन गया है।

8.4 एक इंट्रानेट और एक्सट्रानेट में आए सुरक्षा जोखिमों के प्रकार

इंट्रानेट और एक्स्ट्रानेट सुरक्षा उल्लंघनों रूपों की एक किस्म ले सकते हैं। उदाहरण के लिए:

- कोई अनधिकृत व्यक्ति, जैसे एक ठेकेदार या आगंतुक, कम्पनी के कंप्यूटर सिस्टम तक पहुँच सकता है।
- सिस्टम का उपयोग करने के लिए एक कर्मचारी या आपूर्तिकर्ता अधिकृत करता है जिससे एक उद्देश्य दुसरे उद्देश्य के लिए उपयोग हो सकता है। उदाहरण के लिए, एक इंजीनियर गोपनीय वेतन जानकारी प्राप्त करने के लिए मानव संसाधन डेटाबेस में घुस सकता है।
- अधिकृत उपयोगकर्ता को भेजी जाने वाली गोपनीय जानकारी पकडी जा सकती है।
- उपयोगकर्ता इंटरनेट या एक्स्ट्रानेट पर भौगोलिक दृष्टि से अलग कार्यालयों के बीच दस्तावेजों को साझा कर सकते हैं चूकि यह तार पर भेजे जाते है जिस वजह से घर के कंप्यूटर से कॉर्पोरेट इंट्रानेट तक पहुँचने में संवेदनशील डेटा का खुलासा कर सकते हैं।
- इलेक्ट्रॉनिक मेल ट्रांजिट के दौरान खुलासा किया जा सकता है।

8.5 फायरवॉल और उनके विकास

फायरवॉल एक नेटवर्क सुरक्षा उपकरण है जो कि एक अविश्वसनीय क्षेत्र (उदाहरण के लिए, इंटरनेट) और एक विश्वसनीय क्षेत्र (उदाहरण के लिए, एक निजी या कॉर्पोरेट नेटवर्क) के बीच यातायात प्रवाह के लिए नेटवर्क पहुँच को खारिज कर देता है। फायरवॉल नेटवर्क में, सीमांकन बिंदु या सिपाही के रूप में कार्य करता है, और सूचना का संचार इसी के माध्यम से होता हैं।

इसके माध्यम से नेटवर्क मे सूचना प्रवाह की अनुमति या अस्वीकृति प्रदान की जाती हैं। फायरवॉल एक सकारात्मक नियंत्रण मॉडल पर आधारित है, जिसमे परिभाषित निती के आधार पर यातायात नेटवर्क मे अनुमति प्रदान की जाती है और बाकी अन्य सभी यातायात निषेध कर दिया जाता हैं।

8.6 फायरवॉल के प्रकार

प्रॉक्सी फायरवॉल

फायरवॉल डिवाइस का एक प्रारंभिक प्रकार, प्रॉक्सी फायरवॉल एक विशिष्ट अनुप्रयोग के लिए किसी एक नेटवर्क से अन्य के बीच प्रवेश द्वार के रूप में कार्य करता है। प्रॉक्सी सर्वर अतिरिक्त कार्यक्षमता प्रदान कर सकते हैं जैसे सामग्री कैशिंग और सुरक्षा जो नेटवर्क के बाहर से सीधे कनेक्शन को रोकने के द्वारा प्राप्त होते हैं। बहरहाल, यह थुरूपुट (throughput) क्षमताओं और समर्थन करने वाले एप्लीकेशन्स पर प्रभाव डाल सकते हैं।

स्टेटफुल निरीक्षण फायरवॉल

स्टेटफुल निरीक्षण फायरवॉल पोर्ट और प्रोटोकॉल के आधार पर यातायात को ब्लॉक या अनुमति प्रदान करता है। यह एक कनेक्शन के स्टार्ट से लेकर बंद तक सभी गतिविधि पर नजर रखता है। फिल्टरिंग निर्णय दोनों प्रशासक परिभाषित नियमों के साथ ही संदर्भ के आधार पर बनते है जो पिछले कनेक्शन और एक ही कनेक्शन से संबंधित पैकेट से जानकारी का उपयोग करने के लिए संदर्भित करता है।

एकीकृत खतरा प्रबंधन (UTM) फायरवॉल

एक यूटीएम डिवाइस आमतौर पर, शिथिल युग्मित रास्ते में, एक स्टेटेफुल निरीक्षण फायरवॉल और एंटीवायर घुसपैठ की रोकथाम के साथ के कार्यों को जोड़ती है। यह अतिरिक्त सेवाओं और क्लाउड प्रबंधन को भी शामिल करता है। यूटीएम सादगी और उपयोग की आसानी पर ध्यान केंद्रित करता है।

अगली पीढ़ी के फायरवॉल (NGFW)

फायरवॉल सरल पैकेट फिल्टरिंग और स्टेटेफुल निरीक्षण से परे विकसित किया गया है। ज्यादातर कंपनियां अगली पीढ़ी फायरवॉल उन्नत मैलवेयर और आवेदन–परत हमलों जैसे आधुनिक खतरे ब्लॉक करने के लिए परिनियोजित कर रहे हैं। अगली पीढ़ी फायरवॉल मे यह सब शामिल करना आवश्यक है।

- मानक फायरवॉल क्षमताऐं जैसे स्टेटफुल निरीक्षण
- एकीकृत घुसपैठ की रोकथाम
- जोखिम भरें एप्लिकेशन देखने और ब्लॉक करने के लिए एप्लिकेशन जागरूकता और नियंत्रण
- भावी जानकारी फीड के लिए पथ नवीनीकरण
- सुरक्षा खतरों को दूर करने की तकनीके

8.7 फायरवॉल फिल्टरिंग तकनीके

फायरवॉल दोनों घर और कॉर्पोरेट नेटवर्क की रक्षा करने के लिए उपयोग किया जाता है। सभी जानकारी जो की इंटरनेट के माध्यम से अपने नेटवर्क या कंप्यूटर प्रणाली के लिए आ रही है एक विशिष्ट फायरवॉल प्रोग्राम या हार्डवेयर डिवाइस उन्हें फिल्टर करता है। संभावित रूप से फायरवॉल तकनीकों के कई प्रकार हैं जो की हानिकारक जानकारी को रोकने के काम आती हैं।

- **पैकेट फिल्टर:** प्रत्येक पैकेट नेटवर्क में प्रवेश करने या नेटवर्क को छोड़ने पर स्वीकार करता है या उपयोगकर्ता–परिभाषित नियमों के आधार पर खारिज करता है। पैकेट फिल्टरिंग काफी प्रभावी और उपयोगकर्ताओं के लिए पारदर्शी है लेकिन इसे कॉन्फिगर करने मैं मुश्किल आती है।
- **अनुप्रयोग गेटवे:** सुरक्षा तंत्र, FTP और टेलनेट सर्वर जैसे विशिष्ट अनुप्रयोगों पर लागू होता है।यह बहुत प्रभावी है, लेकिन यह कार्य क्षमता को कम कर सकता है।
- **सर्किट स्तर गेटवे:** यह सुरक्षा तंत्र को लागू करता है जब एक टीसीपी या यूडीपी कनेक्शन स्थापित होते है। एक बार जब कनेक्शन बन गया है, तो पैकेट आगे की जाँच के लिए बिना होस्ट के बीच प्रवाह कर सकते हैं।
- **प्रॉक्सी सर्वर:** सभी संदेश को नेटवर्क में प्रवेश करने और छोड़ने से रोकता है। प्रॉक्सी सर्वर प्रभावी ढंग से नेटवर्क पते को छुपाता है।

फायरवॉल निजी जानकारी की रक्षा करने में रक्षा की पहली पंक्ति में माना जाता है। अधिक से अधिक सुरक्षा के लिए, डेटा एन्क्रिप्टेड किया जा सकता है।

8.8 क्रिप्टोग्राफी

क्रिप्टोग्राफी बारीक कूटलिपि और क्रिप्ट विश्लेषण के विषयों से संबंधित है। क्रिप्टोग्राफी तकनीक में ऐसे छवि के साथ शब्द विलय, और भंडारण या पारगमन में जानकारी छिपाने के लिए अन्य तरीके भी शामिल है। इस क्षेत्र का अभ्यास करने वाले व्यक्तियों को क्रिप्टोग्राफर्स के रूप में जाना जाता है। निम्नलिखित चार उद्देश्यों के साथ क्रिप्टोग्राफी जुड़ी हुई है:

1) **गोपनीयता** –इस जानकारी को किसी भी अनायास के द्वारा नहीं समझा जा सकता।
2) **वफादारी** –इस जानकारी को भंडारण के मध्य या पारगमन में नहीं बदला जा सकता और ना ही बिना रिसीवर का पता लगाए कुछ परिवर्तन किया जा सकता है।
3) **गैर–परित्याग** –सृजन या सूचना के प्रसारण के बाद में निर्माता उसके सूचना या उसके इरादों में इनकार नहीं कर सकता है।
4) **प्रमाणीकरण** –प्रेषक और रिसीवर एक दूसरे की पहचान और जानकारी की उत्पत्ति / गंतव्य पुष्टि कर सकते है।

8.9 डिजिटल हस्ताक्षर

डिजिटल हस्ताक्षर संदेश प्रमाणीकरण की सार्वजनिक कुंजी हैं। भौतिक दुनिया में, हस्तलिखित या टाइप संदेशों पर हस्तलिखित हस्ताक्षर का उपयोग करना आम बात है। संदेश से हस्ताक्षरकर्ता को बाध्य किया जाता है। इसी तरह, डिजिटल हस्ताक्षर एक तकनीक है जो एक व्यक्ति / संस्था को डिजिटल डाटा से बांधता है। इस बाइंडिंग को स्वतंत्र रूप से रिसीवर या किसी भी तीसरे पक्ष द्वारा अच्छी तरह से सत्यापित किया जा सकता है। डिजिटल हस्ताक्षर एक क्रिप्टोग्राफिक वैल्यू होती है जोकि डेटा और गुप्त कुंजी से कैलकुलेट की जाती हैं जो संदेश हस्ताक्षरकर्ता को ही पता होती है। इसकी आवश्यकता, व्यावसायिक अनुप्रयोगों में बहुत महत्वपूर्ण है।

8.10 वर्चुअल प्राइवेट नेटवर्क (वीपीएन)

वीपीएन या वर्चुअल प्राइवेट नेटवर्क, एक नेटवर्क कनेक्शन है जो आपको एक सुरक्षित सार्वजनिक इंटरनेट से दूरस्थ स्थान पर स्थित निजी नेटवर्क से कनेक्शन बनाने के लिए सक्षम बनाता है। एक वीपीएन के साथ, सभी नेटवर्क यातायात (डेटा, आवाज, और वीडियो) मेजबान डिवाइस (ग्राहक) और वीपीएन प्रदाता सर्वर के बीच सुरक्षित आभासी सुरंग के माध्यम से चला जाता है,

और वह एन्क्रिप्टेड है। वीपीएन प्रौद्योगिकी जैसे एन्क्रिप्शन, सुरंग प्रोटोकॉल, डेटा एनकैप्सूलेशन, और प्रमाणित कनेक्शन निजी नेटवर्क के लिए एक सुरक्षित कनेक्शन को उपलब्ध कराने के लिए और अपनी पहचान की रक्षा करने के लिए सुविधाओं के संयोजन का उपयोग करते है।
वीपीएन कनेक्शन तकनीकी रूप से आपको एक लोकल एरिया नेटवर्क (लैन), जो कई कार्यालयों में उपयोग में आता है, लेकिन एक वायर्ड कनेक्शन की आवश्यकता के बिना सभी लाभ देता है। प्रारंभिक वीपीएन अलग–अलग कर्मचारियों को उनके कंपनी के नेटवर्क को सुरक्षित दूरस्थ स्थान से उपयोग के लिए स्थापित किए गए थे, इसलिए इसका नाम वर्चुअल प्राइवेट नेटवर्क है। कंपनी के नेटवर्क से जोड़ने के बाद, व्यक्ति कंपनी के संसाधन और सेवाओं का उपयोग बिल्कुल उस कर्मचारी के तरीके से कर सकता है जैसे कर्मचारी कंपनी के अंदर से कर सकते हैं। तब से, वीपीएन को इंटरनेट पर किसी भी डिवाइस के बीच सुरक्षित संचार का एक ही स्तर प्रदान करने के लिए विकसित किया है। आज, वीपीएन उपभोक्ताओं के बीच अपनी ऑनलाइन गोपनीयता की रक्षा, उनके ब्राउजिंग सत्र को सुरक्षित, और वेबसाइटों को अन्यथा अवरुद्ध या सेंसर कर रहीं सामग्री से अप्रतिबंधित पहुँच पाने के लिए एक साधन के रूप में तेजी से लोकप्रिय है।

8.11 वीपीएन के प्रकार

वीपीएन वास्तुकला उपयोग के उद्देश्य, और पहुंच से भिन्न होते हैं। पहुंच के दो बुनियादी प्रकारः साइट के लिए साइट वीपीएन और रिमोट एक्सेस वीपीएन हैं।
साइट के लिए साइट वीपीएन इसका उपयोग कॉरपोरेट वातावरण में किया जाता है। एक साइट के लिए साइट वीपीएन एक ही कंपनी की या अलग कंपनियों में से दो या दो से अधिक लोकल एरिया नेटवर्क (लैन) की सुरक्षित एन्क्रिप्टेड कनेक्शन सुनिश्चित करता है। इसका मतलब है कि दो भौगोलिक दृष्टि से अलग कार्यालय लगभग एक एकल लैन और उन में एक साथ काम कर रहे लोग इस नेटवर्क में डेटा का उपयोग कर सकते हैं।
रिमोट एक्सेस वीपीएन रिमोट एक्सेस वीपीएन एक निजी नेटवर्क के लिए एक व्यक्ति को कंप्यूटर से कनेक्ट करता है । वीपीएन के इस प्रकार को फिर से दो समूहों में बांटा जा सकता हैं।

- **कॉर्पोरेट वीपीएन** – कॉर्पोरेट वीपीएन व्यापार यात्रियों को नेटवर्क पर उनकी कंपनी के नेटवर्क और दूर से संसाधनों का उपयोग और सेवाओं के लिए कनेक्ट करने के लिए अनुमति देते हैं। एक उपयोगकर्ता वीपीएन के लिए उसकी डिवाइस कंपनी से जोड़ता है, वीपीएन सोचता है कि उपयोगकर्ता का कंप्यूटर वीपीएन के रूप में एक ही स्थानीय नेटवर्क पर है।
- **निजी वीपीएन** – व्यक्तिगत वीपीएन कॉर्पोरेट वीपीएन के रूप में ही निजी और सुरक्षित कनेक्शन उपभोक्ताओं को प्रदान करते हैं। हालांकि, निजी वीपीएन निजी संसाधनों का उपयोग करने के लिए निजी नेटवर्क से कनेक्ट करने के लिए इस्तेमाल की अनुमति नहीं देते हैं।

इंटरनेट पर किसी भी सौदे के समय सुरक्षा एक अनिवार्य हिस्सा है। अपनी सुरक्षा से समझौता होने पर ग्राहक ई–व्यापार में उसकी / उसके विश्वास बड़ी जल्दी खो सकता है। सुरक्षित ई–भुगतान / लेनदेन के लिए निम्न आवश्यकताए हैं:

- **गोपनीय** – अनाधिकृत व्यक्ति के लिए सूचना सुलभ नहीं होनी चाहिए। प्रसारण के दौरान यह पकड़ा जाना चाहिए।
- **वफादारी** – नेटवर्क पर प्रसारण के दौरान सूचना नहीं बदली जानी चाहिए।
- **उपलब्धता** – जहाँ भी और जब भी समय सीमा के भीतर आवश्यक जानकारी उपलब्ध नहीं है, निर्दिष्ट किया जाना चाहिए।

- **प्रामाणिकता** – आवश्यक जानकारी से उपयोगकर्ता को प्रमाणित करने के लिए एक तंत्र होना चाहिए।
- **एन्क्रिप्शन** – जानकारी एन्क्रिप्टेड और केवल अधिकृत उपयोगकर्ता द्वारा डिक्रिप्ट की जानी चाहिए।

8.12 सुरक्षा सुनिश्चित करने के उपाय

- **एन्क्रिप्शन** – नेटवर्क पर प्रसारित किये जा रहे डाटा की सुरक्षा करने के लिए यह एक बहुत प्रभावी और व्यावहारिक तरीका है। प्रेषक एक गुप्त कोड का उपयोग कर डेटा एनक्रिप्ट और निर्दिष्ट रिसीवर उसी या अलग गुप्त कोड का उपयोग कर डेटा डिक्रिप्ट कर सकते हैं।
- **डिजिटल हस्ताक्षर** – डिजिटल हस्ताक्षर जानकारी की प्रामाणिकता सुनिश्चित करता है। डिजिटल हस्ताक्षर (ई–हस्ताक्षर) एन्क्रिप्शन और पासवर्ड के माध्यम से प्रमाणीकृत है।
- **सुरक्षा प्रमाण पत्र** –सुरक्षा प्रमाण पत्र, एक व्यक्ति की वेबसाइट या उपयोगकर्ता की पहचान सत्यापित करने के लिए एक अद्वितीय डिजिटल आईडी है।

महत्वपूर्ण बिंदु

- फायरवॉल एक नेटवर्क सुरक्षा युक्ति है जो अनुदान या यातायात के लिए नेटवर्क के उपयोग को खारिज कर दिए गए एक अविश्वसनीय क्षेत्र (उदाहरण के लिए, इंटरनेट) और एक विश्वसनीय जोन के बीच बहती है (उदाहरण के लिए, एक निजी या कॉर्पोरेट नेटवर्क)।
- प्रॉक्सी सर्वर प्रभावी ढंग से नेटवर्क का सही पता छुपाती है।
- क्रिप्टोग्राफी बारीक कूटलिपि और क्रिप्ट विश्लेषण के विषयों से संबंधित है।
- डिजिटल हस्ताक्षर संदेश प्रमाणीकरण की सार्वजनिक कुंजी हैं।
- क्रिप्टोग्राफी गोपनीयता, अखंडता, गैर–अस्वीकरण और प्रमाणीकरण, इन् चार उद्देश्यों के साथ जुड़ा है।
- वीपीएन या वर्चुअल प्राइवेट नेटवर्क एक नेटवर्क कनेक्शन है जो आपको एक सुरक्षित सार्वजनिक इंटरनेट पर एक दूरस्थ स्थान पर स्थित निजी नेटवर्क से कनेक्शन बनाने के लिए सक्षम बनाता है।
- सुरक्षा प्रमाण पत्र एक व्यक्ति की वेबसाइट या उपयोगकर्ता की पहचान सत्यापित करने के लिए इस्तेमाल की जाने वाली अद्वितीय डिजिटल आईडी है।

अभ्यासार्थ प्रश्न

वस्तुनिष्ठ प्रश्नः

प्रश्न 1. सुरक्षित ई–भुगतान के लिए आवश्यक जरुरते हैं:

अ गोपनीय　　ब अखंडता

स प्रामाणिकता　　द उपरोक्त सभी

प्रश्न 2. UTM का मतलब है

अ यूनिवर्सल खतरा प्रबंधन　　ब एकीकृत खतरा प्रबंधन
स एकीकृत सीमा प्रबंधन　　द इनमे से कोई नहीं

प्रश्न 3. NGFW का मतलब है

अ न्यू–जनरल फायरवॉल　　ब अगला–जनरल फायरवॉल
स अगली पीढ़ी फायरवॉल　　द इनमें से कोई नहीं

अति लघुत्तरात्मक प्रश्न

प्रश्न 1. डिजिटल हस्ताक्षर को परिभाषित कीजिये।
प्रश्न 2. इंट्रानेट को परिभाषित कीजिये।
प्रश्न 3. सामग्री अखंडता को परिभाषित कीजिये।
प्रश्न 4. गोपनीयता को परिभाषित कीजिये।
प्रश्न 5. प्रॉक्सी सर्वर का उपयोग क्या है?

लघुत्तरात्मक प्रश्न

प्रश्न 1.एन्क्रिप्शन का उद्देश्य क्या है?
प्रश्न 2. ई–कॉमर्स में सुरक्षा आवश्यक क्यों है?
प्रश्न 3. ऐक्सट्रानेट और इसके उपयोग क्या है?
प्रश्न 4. प्रमाणीकरण क्या है?
प्रश्न 5. प्रॉक्सी फायरवॉल का उपयोग क्या है?
प्रश्न 6. क्रिप्टोग्राफी क्या है?

निबन्धात्मक प्रश्न

प्रश्न 1. वीपीएन क्या है और इसके विभिन्न प्रकार समझाइये।
प्रश्न 2. फायरवॉल क्या है और इसके उपयोग बताइये।
प्रश्न 3. फायरवॉल फिल्टरिंग की विभिन्न तकनीक बताइये।
प्रश्न 4. ऐक्सट्रानेट और इंट्रानेट का लाभ की व्याख्या कीजिये।

उत्तरमाला

उत्तर 1: द　　**उत्तर** 2: ब　　**उत्तर** 3: स