COMITE D'ETAT
COMMUNICATION DES TECHNOLOGIES DE L'INFORMATION ET DES TÉLÉCOMMUNICATIONS EN OUZBÉKISTAN
Université de Tachkent Technologies de l'Information

Pour tenir compte de la protection
Head. Département _____
_____

"_____" _____ 2013

Baccalauréat en études supérieures
sur le thème: «Analyse des Problèmes de sécurité dans les réseaux informatiques, les organisations connecté au réseau Internet»

Diplômé _____	Aripov O.N
(Signature)	(Nom)
Rukovoditel_____	Ganiev SK
(Signature)	(Nom)
Consultant VDS_____	Qodirov F.M
(Signature)	(Nom)
Commentateur_____	_____
(Signature)	(Nom)

Tashkent 2013.

Faculté
technologies
de l'information

APPROUVÉ
Doyen de la Faculté
_____
(Signé)
_____
(Date)

Ministère de la
"Sécurité de
l'information"

APPROUVÉ
Head. Département
_____
(Signé)
_____
(Date)

Groupe
AXu 231-09

DÉCLARATION

Je vous demande d'approuver le sujet de la finale de qualification

Analyse des problèmes de sécurité dans les réseaux informatiques, les organisations connecté au réseau Internet

(Nom de l'objet)

En tant que responsable de la demande d'approuver le

Ganiev Salim Karimovich professeur. **Tél: 238-65-09**

(Nom,prénom,deuxième prénom,degré,grade universitaire,la position,le numéro de téléphone)

Chef de l'œuvre finale de qualification: "JE SUIS D'ACCORD"

Ganiev Salim Karimovich

(Signature) (Nom et Prénom)

Étudiant: **Aripov Otabek Narimandzhonovich**

(Signature) (Nom et Prénom)

Téléphone principal: 238-65-09

(domicile) (travail)

Note: l'application est stockée dans le département avant de mettre le travail dans le sac.

COMITE D'ETAT
COMMUNICATION DES TECHNOLOGIES DE L'INFORMATION ET DES TÉLÉCOMMUNICATIONS EN OUZBÉKISTAN
Université de Tachkent Technologies de l'Information

Faculté ___ IT____ Département _____ "Sécurité de l'information"
Direction 5523500 - "Sécurité de l'information"

APPROUVÉ
Head. Département de _____
(Signé)
"_____" _____ 2013.

TÂCHE

le travail final de qualification
Aripova Otabek Narimandzhonovich
(Nom, prénom, initiale)

1. Le thème: Analyse des problèmes de sécurité dans les réseaux informatiques, les organisations connecté au réseau Internet
2. Approuvé par ordre de l'université à partir de 2013 11.02. № 145-07
3. La date d'achèvement des travaux finis 01.06.2013
4. Contexte du travail du scientifique - livres techniques, des matériaux et de la résolution interneta du Président de la République d'Ouzbékistan № 13 (513) à partir 02.04.2012, № -1836 23.10. 2012 № 167 du 05.09.2005.
5. Le contenu de l'œuvre finale de qualification (la liste des points à développer), Résumé, Introduction, aperçu, le corps, la santé et la sécurité, Conclusion, Bibliographie.
6. La liste des fichiers de présentation graphiques.
7. Date de délivrance de l'emploi 02.01. 2013.

Chef _____
(Signé)
Groupe a pris _____
(Signé)

8. Consultant sur certaines sections de l'œuvre finale

Partie	Nom et Prénom Meneur	Signature Date	
		Réglage émis	Quête reçue
1. Principal	Professeur. S.K.Ganiev	11.02.2013	11.02.2013
2. Vie de sécurité	Qodirov F.M	18.05.2013	18.05.2013
3. Consultant	Professeur. S.K.Ganiev		

9. Tableau d'avancement

№	Le nom de la section	Période d'exécution	La marque sur l'exécution de la tête
1.	Sélection de la littérature	2.01.2013 - 12.01.2013	
2.	Familiarisation avec le réseau informatique de l'organisation des technologies de l'information.	14.01.2013 - 31.01.2013	
3.	L'analyse comparative des firewalls distribués.	01.02.2013 - 28.02.2013	
4.	Sélection de pare-feu en fonction de la taille de la société.	01.03.2013 - 13.04.2013	
5.	Conclusion	15.04.2013 - 30.04.2013	
6.	Description de la sécurité de la vie	18.05.2013 - 25.05.2013	
7.	Présentation	01.05.2013 - 15.05.2013	
8.	Développement de présentation	16.05.2013 - 30.05.2013	

Elève sortant _____ "_____" _____ 2013

(Signé)

Chef _____ "_____" _____ 2013

(Signé)

Dans cette dernière qualification travail problèmes information sur la sécurité des réseaux informatiques d'organisations connectées à Internet. Les solutions de base à l'aide de Firewalls pour assurer la sécurité du réseau informatique. Les détails sont relevées mesure de Firewalls et des recommandations pour leur utilisation, en fonction de la taille de l'organisation. Le document souligne également les questions de sécurité.

В данной выпускной квалификационной работе рассмотрены проблемы информационной безопастности компютерной сети организации, подключенной к сети Интернет. Приведены основные решения при использовании межсетевых экранов для обеспечения безопасности компьютерной сети. Подробно расматриваются степень распространения межсетевых экранов и рекомендации по их применению в зависимости от размера организации. В работе также освещены вопросы безопасности жизнедеятельности.

Ушбу битирув малакавий ишда Интернет тармогига уланган ташкилот компьютер тармогининг хавфсизлиги муаммолари курилган. Компьютер тармоги хавфсизлигини таьминлашда тармокларо экранлардан фойдаланишдаги асосий ечимлар келтирилган. Тармокларо экранларнинг таркалиш даражаси ва уларнинг ташкилот катталигига боглик холда ишлатилиши буйича тавсиялар батафсил курилган. Ишда хаёт фаолияти хафсизлиги масалалари хам ёритилган.

TABLE DES MATIERES

LISTE DES ABREVIATIONS ET SYMBOLES 7

INTRODUCTION 8

1. EXAMEN PARTIE. L'INFORMATION ORGANISATION DE LA SECURITE D'UN RESEAU INFORMATIQUE 10

1.1 Les problèmes du réseau informatique de sécurité de l'information organisation 10

1.2 Méthodes du réseau informatique de l'organisation de protection des accès non autorisés.....16

2. MAIN PARTIE. LES DECISIONS CLES DU RESEAU INFORMATIQUE DE L'USE FIREWALLS SÉCURITÉ ORGANISATION 20

2.1 Classification de firewalls 20

2.2 Architecture de firewalls et leur configuration 27

2.3 Sélection d'une configuration de Firewalls pour protéger l'organisation du réseau de données 29

3. VIE DE SÉCURITÉ.....45

3.1 Types et les conditions de droit du travail 45

3.2 Base ergonomique pour la protection du travail 48

3.3 En milieu de travail 49

3.4 Prodiguer les premiers soins 50

3.5 Comment soigner les plaies et contusions 51

3.6 Electrocution 53

3.7 Brûlures 55

3.8 Empoisonnement par des produits chimiques 56

CONCLUSION 59

LISTE DES SOURCES UTILISEES 60

LISTE DES ABREVIATIONS ET SYMBOLES

CSR	Le réseau informatique de l'organisme
IB	sécurité de l'information
SO	système d'exploitation
logiciel	logiciel
NSD	accès non autorisé
SOIB	Système de sécurité de l'information
SGBD	Système de gestion de base de données
CPU	unité centrale de traitement
CA	Certification Authority
CGI	Common Gateway Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DSA	Digital Signature Algorithm
FTP	File Transport Protocol
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
IDS	Intrusion Detection System
IIS	Internet Information Services
KSK	Key Signing Key
MAC	Media Access Control
MAC	Message Authentication Code
MD5	Message Digest v5
NAT	Network Address Translation
NTP	Network Time Protocol
NTP	Network Time Protocol
OSI	Open System Interconnection
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, Adleman
SEP	Secure Entry Point
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TOS	Trusted OC
VPN	Virtual Private Network
URL	Uniform Resource Locator

INTRODUCTION

Vingt-et-unième siècle - l'ère de la technologie de l'information, sciemment informé par notre président Islam Karimov. La République d'Ouzbékistan dans les années de l'indépendance dans le domaine de l'informatisation connaît une ère de changement évolutif. Modernes de l'information - technologies de communication créant commodité et en même temps, de nouveaux problèmes sont créés.

De la part de notre état est donné une grande attention dans le domaine de l'information - technologie de communication. Par exemple, dans la région a été faite un petit nombre de lois et de documents.

Actuellement, la grande majorité des réseaux combinée à travers l'Internet. Donc, il est évident que pour le fonctionnement sécuritaire d'un tel grand système, il est nécessaire de prendre certaines précautions, comme avec pratiquement n'importe quel ordinateur, vous pouvez accéder à n'importe quel réseau d'une organisation, et le risque augmente de manière significative pour la raison que, pour lui de pénétrer sur un ordinateur ne nécessite pas d'accès physique.

Selon les données de l'Institut de la sécurité informatique (Computer Security Institute) à la suite d'une étude récente, 70% des organisations ont été piraté firewalls, en outre, 60% des tentatives de piratage détectés provenaient des réseaux internes des organisations.

Compte tenu de ces faits, il est sûr de dire que le problème de la sécurité des réseaux reste un non résolu et aujourd'hui, comme la grande majorité des entreprises n'ont pas résolu les questions de sécurité, avec le résultat qu'ils ont une perte financière.

Types d'organisations sont complètement satisfaits avec un ensemble typique de mesures de protection, sélectionnés sur la base de la représentation des risques typiques ou même sans aucune analyse. Vous pouvez faire une analogie entre l'individu et la construction d'obtenir un appartement dans le domaine du logement de masse. Dans le premier cas, vous devez prendre beaucoup de

décisions à émettre un grand nombre de documents, dans le second - assez pour décider avec seulement quelques paramètres.

Les petites organisations se connecter à l'Internet n'est pas confronté à la question de la sécurité de l'information sont souvent absolument pas préparés à la situation changeante. Dans de nombreux cas, les utilisateurs de réseaux sociaux ne sont même pas conscients du fait que leurs données étaient soudainement disponible pour tout utilisateur d'Internet.

Une solution aux problèmes de sécurité de connexion à l'Internet est l'utilisation de firewalls. Firewalls - un système logiciel et matériel, situé à la jonction du réseau interne de l'entreprise et les données Internet et de contrôle entre les réseaux.

Dans ce travail de qualification finale sur la base de l'analyse de Firewalls existants formulé des recommandations pour leur duree de surfaces selon le de la taille de l'organisation.

1. EXAMEN PARTIE. L'INFORMATION ORGANISATION DE LA SECURITE D'UN RESEAU INFORMATIQUE

1.1 Les problèmes du réseau informatique de sécurité de l'information organisation

Les nouvelles technologies de l'information sont mises en œuvre activement dans toutes les sphères de l'économie nationale. L'émergence de réseaux de données locaux et mondiaux fourni aux utilisateurs d'ordinateurs de nouvelles capacités d'échange d'informations rapide. Si jusqu'à récemment, ces réseaux ont été créés uniquement dans spécifique et étroitement ciblées pour (réseaux universitaires, les départements militaires, etc), le développement de l'Internet et des systèmes connexes a conduit à l'utilisation de réseaux de données mondiaux dans la vie quotidienne de presque chaque personne. Avec le développement et la complexité des moyens, méthodes et formes de l'automatisation du traitement de l'information accroît la dépendance de la société sur le degré de sécurité, il utilise la technologie de l'information.

La pertinence et l'importance du problème de la sécurité de l'information en raison des facteurs suivants:

- Les niveaux actuels de croissance et de développement de la sécurité de l'information sont loin derrière le niveau et le rythme de développement des technologies de l'information.
- Forte croissance des ordinateurs personnels utilisés dans une variété d'activités humaines. Selon la société d'études Gartner Dataquest est actuellement plus d'un milliard d'ordinateurs personnels dans le monde. Et le prochain milliard sera atteint en 2009.
- L'expansion spectaculaire des utilisateurs avec un accès immédiat aux ressources informatiques et des ensembles de données;

Disponibilité du matériel informatique, et la plupart de tous les ordinateurs personnels, a conduit à la propagation de la culture informatique dans la population

générale. Ceci, à son tour, a conduit à de nombreuses tentatives d'ingérence dans le travail des systèmes gouvernementaux et commerciaux, avec malice, et de purement «pour le plaisir». Beaucoup de ces tentatives ont réussi et a causé des dommages considérables aux propriétaires de l'information et des systèmes informatiques. Selon des rapports officieux de jusqu'à 70% de tous les anti violations commises par les soi-disant pirates, ont représenté script-kiddies, dans une traduction littérale - Enfants jouant avec des scripts. Les enfants les appellent, parce qu'ils ne sont pas des experts en informatique, mais savent comment utiliser les outils logiciels prêts à l'emploi qui extraient des sites pirates sur Internet, pour mener des actions destructrices.

• Une augmentation significative du volume des informations collectées, stockées et traitées par des ordinateurs et d'autres équipements d'automatisation;

Selon les experts à l'heure actuelle environ 70-90% du capital intellectuel de l'entreprise sont stockées sous forme numérique - les fichiers texte, les tableurs, les bases de données.

• Multiples vulnérabilités dans les logiciels et plates-formes de réseau;

Le développement rapide des technologies de l'information a ouvert de nouvelles opportunités d'affaires, mais aussi conduit à l'émergence de nouvelles menaces. Produits logiciels modernes en raison de la concurrence dans la vente d'automne avec des erreurs et des défauts. Développeurs, y compris ses produits toutes sortes de fonctions pas eu le temps de faire un systèmes logiciels créés de débogage de qualité. Erreurs et omissions qui pourraient subsister dans ces systèmes conduisent à des violations accidentelles et intentionnelles de sécurité de l'information. Par exemple, la plupart des causes de la perte accidentelle d'informations sont les défaillances dans le logiciel et le matériel, et la majorité des attaques contre les systèmes informatiques sont basés sur les bogues et défauts dans le logiciel. Par exemple, au cours des six premiers mois après la sortie du système d'exploitation serveur de Microsoft Windows Server 2003 trouvé 14 vulnérabilités, dont 6 sont critiques. Malgré le fait qu'au fil du temps, Microsoft développe paquets qui éliminent les lacunes constatées, les utilisateurs ont le temps

de souffrir d'atteintes à la sécurité de l'information qui ont eu lieu en raison des erreurs restantes. La même situation se produit avec des logiciels d'autres sociétés. Alors que ce ne sont pas résolus de nombreux autres problèmes, le manque de sécurité constitue un obstacle sérieux au développement des technologies de l'information.

• Le développement rapide de l'Internet, presque n'empêche pas les failles de sécurité des systèmes de traitement de l'information dans le monde entier.

Cette mondialisation permet aux pirates à partir de pratiquement n'importe où dans le monde où il ya Internet, des milliers de miles, pour mener à bien une attaque sur le réseau de l'entreprise.

• Les méthodes modernes de stockage, traitement et transmission de l'information ont contribué à l'émergence de menaces liées à la possibilité de perte, la corruption et la divulgation de données destinés ou appartenant à des utilisateurs finaux.

Par exemple, actuellement dans le secteur bancaire plus de 90% de tous les crimes liés à l'aide de systèmes de traitement automatisés de données.

Sous la menace de sécurité signifie un danger possible (réel ou potentiel existant) la commission d'un acte (action ou inaction) dirigée contre l'objet de protection (sources d'information), préjudiciable au propriétaire ou à l'utilisateur, qui se manifeste en danger de distorsion, la divulgation ou perte d'information.

La mise en œuvre d'une menace de sécurité peut avoir les objectifs suivants:[11]

• Violation de la confidentialité des informations. Les informations stockées et traitées dans un réseau d'organisations informatiques des entreprises (RSE) peut être d'une grande valeur pour son propriétaire. Son utilisation par d'autres cause des dommages importants aux intérêts du propriétaire;

• Violation de l'intégrité de l'information. La perte de l'intégrité de l'information (en tout ou en partie, est compromise, la désinformation) - une menace proche de sa divulgation. Des informations précieuses peuvent être

perdues ou compromis par sa suppression ou modification non autorisée. Les dégâts de ces actions peut être beaucoup plus qu'une violation de la confidentialité;

• Violation de la performance RSE de (partielle ou complète) (violation de disponibilité). Rayé des listes ou des modes incorrects de modification des composantes de la RSE, leur modification ou leur remplacement peut conduire à des résultats erronés, l'échec de la RSE de la circulation de l'information ou de l'échec en service. Exonération des flux d'information ne reconnaît pas l'une des parties à la communication de la cession ou de recevoir des messages. En gardant à l'esprit qu'ils peuvent contenir des rapports importants, les commandes, la coordination financière, etc, dans ce cas, les dommages peuvent être importants.

Par conséquent, garantir la sécurité des systèmes et réseaux informatiques est l'un des principaux domaines de la technologie de l'information.

Système d'information d'entreprise (réseau) - le système d'information, à laquelle peut être cercle restreint de personnes définies par le propriétaire ou l'accord des participants de ce système d'information (à partir de la loi sur la signature électronique numérique).

Organisations en réseau d'ordinateurs (RSE) sont distribués des systèmes informatiques, le traitement automatisé de l'information. Le problème de la sécurité de l'information est au cœur de ces systèmes informatiques. Assurer la sécurité de la RSE consiste à organiser l'opposition à toute intrusion non autorisée dans le processus de fonctionnement de la RSE, ainsi que les tentatives de modification, de vol, la désactivation ou la destruction de ses composantes, à savoir la protection de toutes les composantes de la RSE-Matériels, logiciels, données et du personnel [7]

Considérons, comme dans la situation actuelle est la question de la sécurité de l'information dans les communications d'entreprise. Le cabinet d'études Gartner Group identifie quatre niveaux de maturité en termes de sécurité de l'information

Niveau 0:

BI dans l'entreprise ne le fait, la société n'a pas connaissance de l'importance des problèmes de sécurité de l'information;

Le financement n'est pas disponible;

IB est mis en œuvre par des moyens réguliers des systèmes d'exploitation, bases de données et applications (protection par mot de passe, l'accès simultané aux ressources et services).

L'exemple le plus typique est une entreprise avec une petite équipe engagée dans, par exemple, l'achat / vente de marchandises. Tous les problèmes techniques sont à la charge de l'administrateur du réseau, qui est souvent un étudiant. Ici, la chose importante est que tout fonctionnait.

Niveau 1:

IB est considéré par la direction comme un problème purement "technique", il n'y a pas de programme unique (concept, politique) du système de gestion de la sécurité de l'information (SOIB) de la société;

Le financement fait partie de l'IT globale - budget;

IB est mis en œuvre au moyen de zéro + outils de sauvegarde, anti-virus, Firewalls, l'organisation de VPN (remèdes traditionnels).

2 et 3 niveaux:

IB est considéré par la direction comme un ensemble de mesures organisationnelles et techniques, on est conscient de l'importance de la sécurité de l'information aux processus de travail ont approuvé le programme de développement de la société SOIB de leadership;

Le financement est en cours d'un budget distinct;

IB est mis en œuvre par l'intermédiaire du premier niveau + outils d'authentification forte, outils d'analyse des courriels et du contenu Web, IDS (Système de Détection d'Intrusion), le moyen de l'analyse de la sécurité, SSO (fonds d'authentification unique), PKI (Public Key Infrastructure) et les mesures d'organisation (audit interne et externe , analyse des risques, la politique de sécurité de l'information, les règlements, les procédures, les règlements et les lignes directrices).

3 diffère du niveau de la deuxième suit:

IB fait partie de la culture d'entreprise, a été nommé CISA (officier supérieur sur les questions de sécurité de l'information);

Le financement est en cours d'un budget distinct, qui, selon la firme de recherche analyste de Datamonitor dans la plupart des cas ne dépasse pas 5% du budget informatique;

IB est mis en œuvre par l'intermédiaire du système de gestion de second rang + IB, CERT (groupe de réponse aux incidents atteintes à la sécurité de l'information), SLA (accord de niveau de service).

Ainsi, une approche sérieuse pour assurer la sécurité de l'information apparaît uniquement sur les 2-E les niveaux 3 m. Et le 1er et partiellement niveau 0 de maturité selon cette classification, nous avons l'approche dite «au coup par coup" à la sécurité de l'information. Approche «fragmentée» vise à contrer les menaces clairement définies dans les conditions données. A titre d'exemples d'une telle approche peut fournir contrôle, des outils de chiffrement accès unique autonome, spécialisée logiciel antivirus it.p.

L'avantage de cette approche est la grande sélectivité à une menace spécifique. Un inconvénient majeur de cette approche est l'absence d'un environnement de traitement sécurisé unique. Mesures fragmentaires de sécurité de l'information protéger les objets KS spécifiques uniquement sur la menace spécifique. Même un petit changement dans la menace des espèces conduit à une perte d'efficacité de la protection. Des sociétés telles statistiques Gartner - 85% (0 - 30% 1 - 55%). Partir de 2005.

Organisations les plus graves, pertinents pour les 2e et 3e niveaux de classification de maturité de Gartner, utilisent l'approche «intégrée» à la sécurité de l'information. La même approche et d'offrir une grande entreprise impliqués professionnellement dans la protection de l'information.

Une approche intégrée est basée sur la résolution d'un complexe tâches individuelles sur un seul programme. Cette approche est actuellement le principal de créer un environnement sûr pour le traitement de l'information dans les systèmes d'entreprise qui rassemble les mesures disparates pour contrer les menaces. Il s'agit notamment des morales organisation des moyens légaux, éthiques, programmatiques et techniques de sécurité de l'information. Une

approche intégrée rassemble un certain nombre de systèmes autonomes en les intégrant dans le système soi-disant sécurité intégrée.

Méthodes pour résoudre les problèmes de sécurité sont très étroitement liés au niveau de développement de la science et de la technologie et, surtout, avec le niveau de soutien technologique. Une tendance typique de développement de la technologie moderne est le processus d'intégration totale. Cette tendance a couvert la microélectronique et des télécommunications, des signaux et des canaux, des systèmes et des réseaux. Comme exemples circuits VLSI, les données de connexion réseau um multifonctionnel intégré.

Quelle que soit la forme, ou d'appliquer une approche globale et intégrée, il vise toujours à résoudre un certain nombre de problèmes spécifiques à leur relation étroite avec l'utilisation de moyens techniques communs, des logiciels de communication. Par exemple, en ce qui concerne la sécurité de l'information le plus évident d'entre eux est le défi de limiter l'accès à l'information, l'information de fermeture technique et cryptographique, ce qui limite les niveaux des systèmes d'alarme fausse émissions matériel, et de sécurité. Toutefois, si la décision et les autres tâches tout aussi importantes. Par exemple, la perte de dirigeants d'entreprises, des membres de leur famille ou d'employés clés doit remettre en question l'existence même de l'entreprise. Ce sont aussi les catastrophes naturelles, les accidents, terrorisme, etc systèmes de sécurité conséquent, un objectif pour assurer la sécurité complète de l'information ne peut intégrées, indifférents à la forme de menaces à la sécurité et assurer la protection requise en permanence, à la fois dans le temps et dans l'espace, dans le cadre de la préparation, le traitement, la transmission et le stockage de l'informati

1.2 Méthodes du réseau informatique de l'organisation de protection des accès non autorisés

Il existe plusieurs approches pour résoudre les problèmes de protection de la RSE est connecté à l'Internet à partir de tout accès non autorisé. La première

approche consiste à renforcer la protection de tous les systèmes existants, le libre accès à Internet. Cette approche est appelée «la sécurité au niveau de l'hôte." Il peut comprendre la formation des utilisateurs et les administrateurs travaillent dans un environnement hostile, le resserrement protection par mot de passe (l'introduction ou le durcissement des restrictions sur la longueur minimum, le caractère, la composition et l'expiration du mot) ou l'introduction d'aucune méthode d'authentification par mot de passe, le resserrement de l'accès au système, le resserrement exigences du logiciel en cours d'utilisation, y compris les systèmes d'exploitation, et l'inspection régulière de toutes les exigences imposées.

Cette approche présente plusieurs inconvénients: [8]

- Mode procédures du système compliqué, et peut-être des actions pour lesquelles ils sont utilisés, généralement interdite. Cela peut conduire à une réduction de la productivité des utilisateurs, ainsi que de leur mécontentement.
- Pour les administrateurs système se trouve une charge supplémentaire très importante sur le système de soutien. Même pour des systèmes relativement petits contenant quelques dizaines de voitures, la tâche de maintenir un niveau de sécurité peut exiger un effort disproportionné.
- Les exigences de sécurité peuvent entrer en conflit avec les exigences de l'utilisation du système et l'un d'eux devra donner la préférence au détriment des autres. En règle générale, les exigences de bon fonctionnement du système de préférence au détriment des exigences de sécurité.

L'avantage de cette approche est que, en dehors de la question de la protection de l '«ennemi extérieur», il résout également le problème du système de sécurité interne. Comme une grande partie des incidents (environ 80%) en matière de sécurité vient de salariés ou anciens salariés de l'entreprise, cette approche peut être très efficace pour augmenter la sécurité globale du système.

La deuxième approche est la plus radicale. Il Réseau de travail, l'entreprise n'est pas physiquement connecté à Internet. Pour interagir avec l'Internet, une ou plusieurs machines dédiées qui ne contiennent pas d'informations confidentielles. Les avantages de cette approche sont évidents: le réseau de travail n'est pas

connecté à Internet, la menace d'accès non autorisé à partir de l'Internet, car il n'est pas dans son principe. Dans le même temps, cette approche comporte certaines limites et des inconvénients. Limitation dans certains cas acceptable, le manque d'accès à l'Internet à partir du lieu de travail des employés. Les inconvénients de cette approche découle de la présence de systèmes vulnérables connectés à l'Internet, qui peut être attaqué comme "déni de service" et de vol de services (y compris peut être utilisé pour pirater d'autres systèmes). Une variante de cette approche consiste à distinguer les protocoles. Par exemple, pour accéder aux ressources d'information de la pile de protocole utilisé IPX / SPX, et d'accéder à l'Internet - TCP / IP. Ainsi, par exemple, des serveurs Novell Netware, sera invisible pour l'attaquant et ne peut être attaqué directement à partir d'Internet. Cette approche a aussi des limites. Par exemple, il n'est pas acceptable pour le réseau dans lequel utiliser TCP / IP pour accéder aux ressources internes. Un autre inconvénient est le fait que l'utilisateur du système sont visibles et accessibles par Internet et peut être utilisé comme un tremplin pour de futures attaques sur les serveurs.

Une troisième approche est appelée «la sécurité au niveau du réseau" est administré restrictions d'accès aux réseaux de connexion. Ceci permet le contrôle de mise au point et des moyens de protection au niveau des points de connexion de deux ou plusieurs réseaux, par exemple un point de connexion à l'Internet RSE. À ce stade, il ya un système dédié et - firewall - et qui contrôle l'échange d'informations entre les deux réseaux et filtrer les informations conformément aux procédures spécifiées établies par la politique de sécurité de l'entreprise. Toutes les communications qui ont lieu entre l'Internet et le réseau interne passe à travers le Firewalls. Une organisation peut avoir des avantages importants de ce modèle de sécurité. Le seul système qui agit comme un Firewalls peut vous protéger contre des dizaines d'accès non autorisé ou des centaines de systèmes qui sont cachés derrière elle, sans leur imposer les exigences de sécurité supplémentaires. L'avantage de cette approche est la concentration des moyens de protection et de contrôle à un moment donné, le changement minimum dans les procédures internes

des utilisateurs du système d'information, une assez grande facilité d'administration et peut-être un meilleur niveau de protection. Une limitation de cette approche est qu'elle vise uniquement à protéger contre les menaces externes à partir des attaquants distants.

Considérons maintenant un CSR typique en termes de son applicabilité aux méthodes décrites ci-dessus de protection. Typiquement, il se compose d'ordinateurs clients fonctionnant sous divers systèmes Unix basé sur Microsoft Windows XP ou rarement Windows NT Workstation, Server Microsoft Windows NT Server, Novell Netware, et / ou, et éventuellement d'autres périphériques réseau tels que les imprimantes réseau, les concentrateurs commutateurs et des routeurs avec des télécommandes, etc

L'utilisation exclusive du modèle de sécurité au niveau de l'hôte, dans ce cas, peut ne pas être acceptable, en raison de la grande complexité (et peut-être impossible) l'ajustement du niveau des systèmes de protection utilisés selon les besoins. Les questions de sécurité dans les réseaux basés sur des systèmes Microsoft ont été ci-dessus.

2. MAIN PARTIE. LES DECISIONS CLES DU RESEAU INFORMATIQUE DE L'USE FIREWALLS SÉCURITÉ ORGANISATION

2.1 Classification de firewalle

Firewalls (fig. 2.1) sont des dispositifs ou des systèmes qui contrôlent le flux du trafic réseau entre des réseaux ayant des exigences différentes en matière de sécurité.

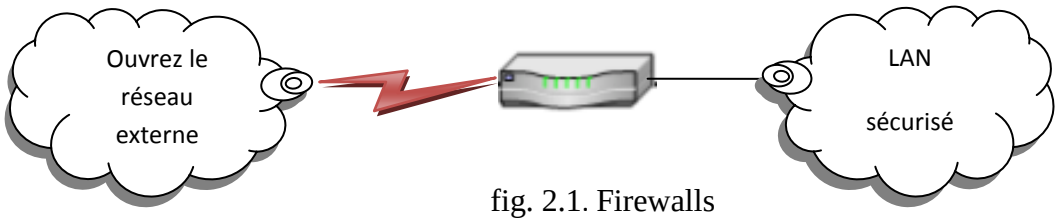


fig. 2.1. Firewalls

Dans la plupart des applications modernes firewalls et leur environnement sont discutés dans le contexte des communications sur l'Internet et, par conséquent, l'utilisation de la pile de protocole TCP / IP. Toutefois, les firewalls sont utilisés dans des environnements de réseau qui ne nécessitent pas de connexion Internet. Par exemple, de nombreux firewalls de réseau d'entreprise des sociétés posent pour limiter les connexions vers et depuis le réseau interne de traiter l'information à différents niveaux de sensibilité, comme l'information financière ou de l'information à la clientèle. Mettre firewalls pour contrôler les communications avec ces domaines, l'organisation peut empêcher l'accès non autorisé aux systèmes et les ressources appropriées dans les zones sensibles. Ainsi, l'utilisation d'un fire-walls offre un niveau supplémentaire de sécurité qui ne peut être atteint autrement.

Actuellement, il existe plusieurs types de firewalls. fig. 2.2 montre le modèle stack moyen de OSI. Une de protocole de comparer leurs capacités est de lister les niveaux du modèle OSI, que ce type de firewalls peut analyser le modèle OSI est une abstraction d'un réseau entre les systèmes informatiques et les périphériques réseau. Considérer que les niveaux du modèle OSI liés aux firewalls.

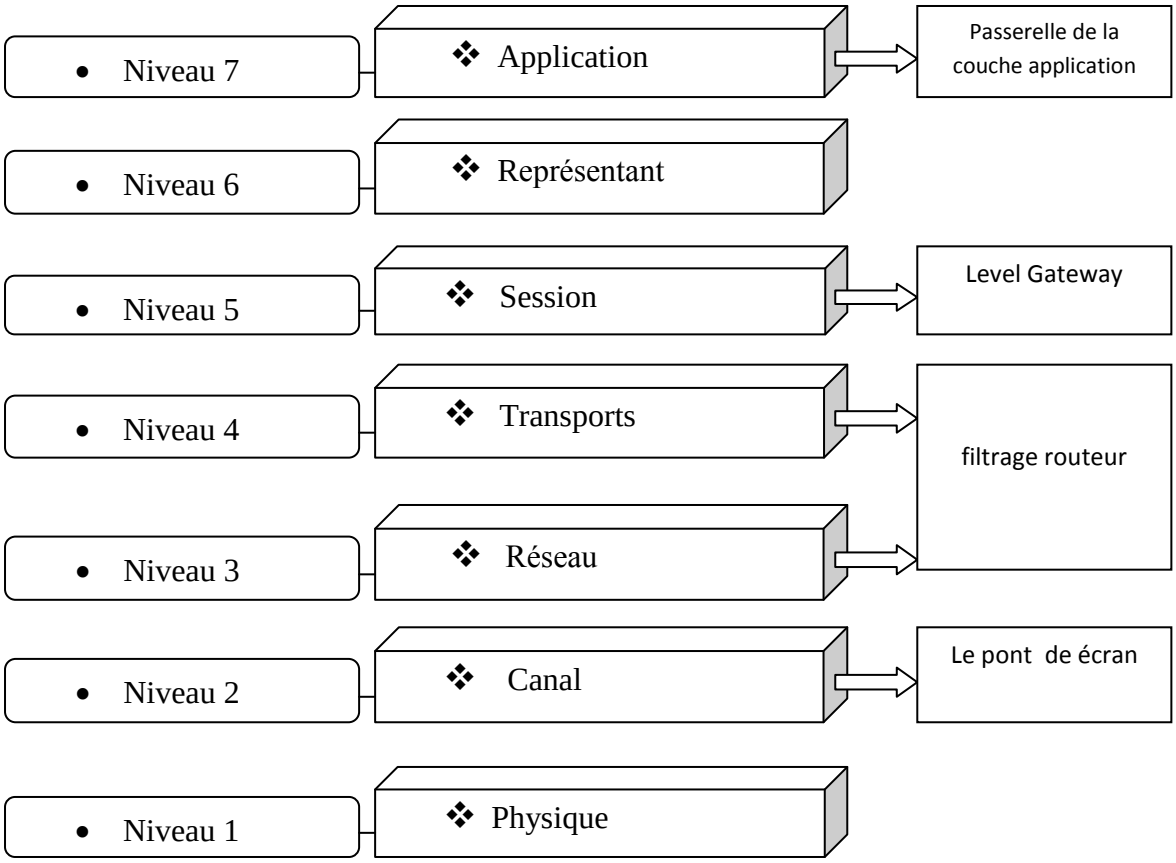


Figure 2.2. La pile de protocoles du modèle OSI.

Le niveau 1 représente les connexions réelles matérielles physiques et des médias tels que Ethernet.

Niveau 2 - le niveau auquel le trafic de réseau transmis sur le réseau local (LAN). C'est aussi la première couche ayant la capacité de répondre à ce qui est possible d'identifier une seule machine. Les adresses sont attribuées aux interfaces réseau et sont appelées adresses MAC (Media Access Control). Ethernet - adresse appartenant au réseau Ethernet-carte est un exemple de MAC -adresse de niveau 2.

Le niveau 3 est le responsable de l'acheminement du trafic réseau sur le WAN. L'adresse Internet de couche 3 appelé les adresses IP, les adresses ont

tendance à être unique, mais dans certaines circonstances, comme la traduction d'adresse réseau (NAT) peuvent avoir des situations où différents systèmes physiques ont la même adresse IP de la couche 3.

Niveau 4 identifie l'application de réseau spécifique, et une session de communication en plus de l'adresse de réseau, le système peut avoir un grand nombre de séances de la couche 4 avec d'autres systèmes d'exploitation. La terminologie relative à la famille de protocoles TCP / IP, inclut le concept de ports qui peuvent être vus comme le point de départ des sessions de fin: le numéro de port source identifie une session de communication sur le système source, le numéro de port de destination identifie la destination d'une session de communication. Des niveaux plus élevés (5, 6 et 7) représentent les systèmes des utilisateurs finaux et la demande.

Combler les Firewalls. Ce Firewalls de classe, d'exploitation sur le 2ème niveau du modèle OSI, également connu sous le nom transparent (stealth), caché, firewall de l'ombre.

Firewall de transition sont relativement nouveaux et représentent une voie prometteuse de développement des technologies de Firewalls. le filtrage du trafic est réalisé par eux dans la couche de liaison, à savoir, Firewalls travaillent avec des cadres (cadre, cadre).

Les avantages de ces firewalls sont:

- Pas besoin de modifier les paramètres du réseau de l'entreprise, aucune configuration supplémentaire des interfaces réseau Firewalls.
- Hautes performances. Parce que c'est un dispositif simple, ils ne consomment pas beaucoup de ressources. Des ressources sont nécessaires pour améliorer la capacité ou machines, ou pour plus d'une analyse en profondeur des données.
- Transparence. La clé de ce dispositif est sa fonction au niveau 2 modèle OSI. Cela signifie que l'interface réseau n'a aucune adresse IP. Cette fonction est plus importante que la facilité d'installation. Aucune adresse IP de l'appareil n'est pas disponible dans le réseau et n'est pas visible pour le monde extérieur. Si un

Firewalls n'est pas disponible, comment l'attaquer? Les attaquants ne savent même pas qu'il existe un Firewalls qui contrôle chacun de leur forfait.

Filtrage des routeurs. Le filtrage de paquets du Firewalls (Packet - filtrage firewall) - firewall, qui est un routeur ou un ordinateur qui exécute le logiciel qui est configuré de telle manière à filtrer certains types de paquets entrants et sortants. Le filtrage de paquets est basé sur les informations contenues dans l'en-tête TCP-IP-paquet (expéditeur et du destinataire adresses et leurs numéros de ports, etc):

- Travailler au niveau 3;
- Aussi connu comme un firewall basé sur le port;
- Chaque paquet est comparée à la liste des règles (l'adresse de la destination source / destination, le port, la source /);
- Economique, rapide (productive en raison de la simplicité), mais la moins sécurisée;
- La technologie d'il ya 20 ans;
- Exemple: la liste de contrôle d'accès (ACL, des listes de contrôle d'accès) routeur;

Level Gateway (passerelle Circuit-niveau) - firewall qui élimine la communication directe entre un client autorisé et l'hôte externe (figure 2.3). D'abord, il fait confiance client reçoit une demande de certains services et, après validation de la session demandée établit une connexion à un serveur externe.

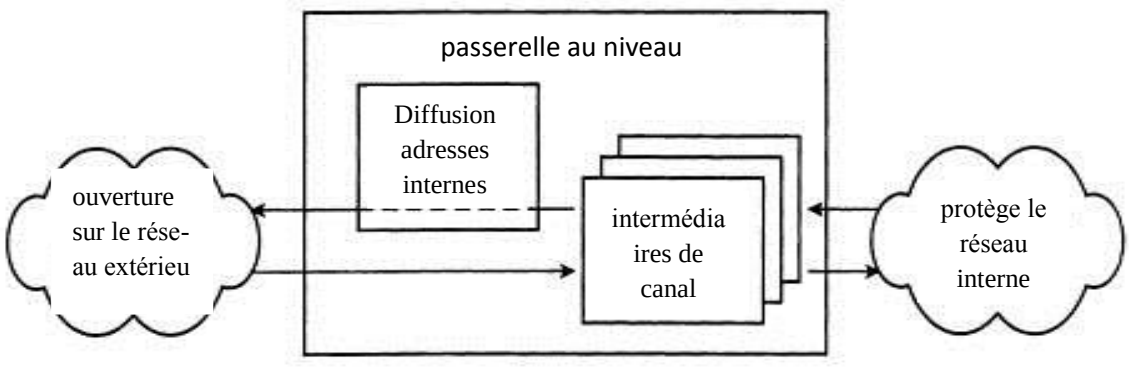


Fig. 2.3. Le schéma de fonctionnement passerelle au niveau circuit

Après cela, la passerelle copie simplement les paquets dans les deux directions, ne réalisant pas leur filtrage. A ce niveau, il est possible d'utiliser la

traduction d'adresses réseau (NAT, la traduction d'adresses réseau). Des adresses internes en cours de diffusion à tous les paquets à partir de l'intérieur vers l'extérieur. Ces paquets adresses IP des ordinateurs - expéditeurs réseau interne automatiquement converties en une adresse IP associée avec le firewall de dépistage. En conséquence, tous les paquets provenant du réseau interne sont intheir Firewalls, ce qui empêche un contact direct entre l'intérieur et le réseau externe. Adresse IP de la passerelle au niveau circuit est le seul adresse IP actif, qui se situe à l'extérieur du réseau:

- Alimenté par 4 niveaux;
- Envoie connexions TCP basé sur le port;
- Peu coûteux, mais plus sûr que le filtre de paquets;
- exigent généralement l'utilisateur ou la configuration du programme pour compléter le travail;
- Exemple: SOCKS firewall.

passerelle de la couche application (passerelles de niveau application) - entre les firewall, ce qui supprime la communication directe entre un client autorisé et l'hôte externe, le filtrage de tous les paquets entrants et sortants à la couche d'application du modèle OSI (fig. 2.4).

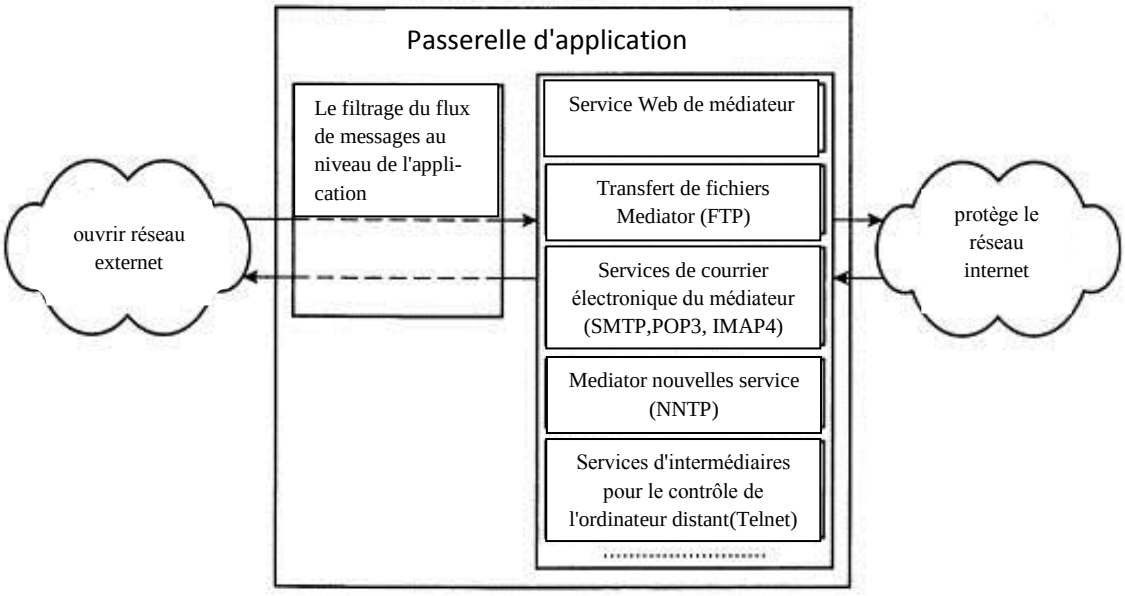


Figure 2.4. Le schéma de fonctionnement de la passerelle d'application

Associé à l'intermédiaire du programme d'application redirigé à travers les informations de passerelle générés par le service spécifique TCP / IP.

Caractéristiques:

- L'identification et l'authentification des utilisateurs lorsqu'ils tentent d'établir une connexion à travers le Firewalls;
- Filtrer le flux de messages, par exemple, l'analyse dynamique de virus et de chiffrage d'informations transparent;
- L'exploitation forestière et la réponse aux événements;
- Mise en cache des données demandées à partir du réseau externe.

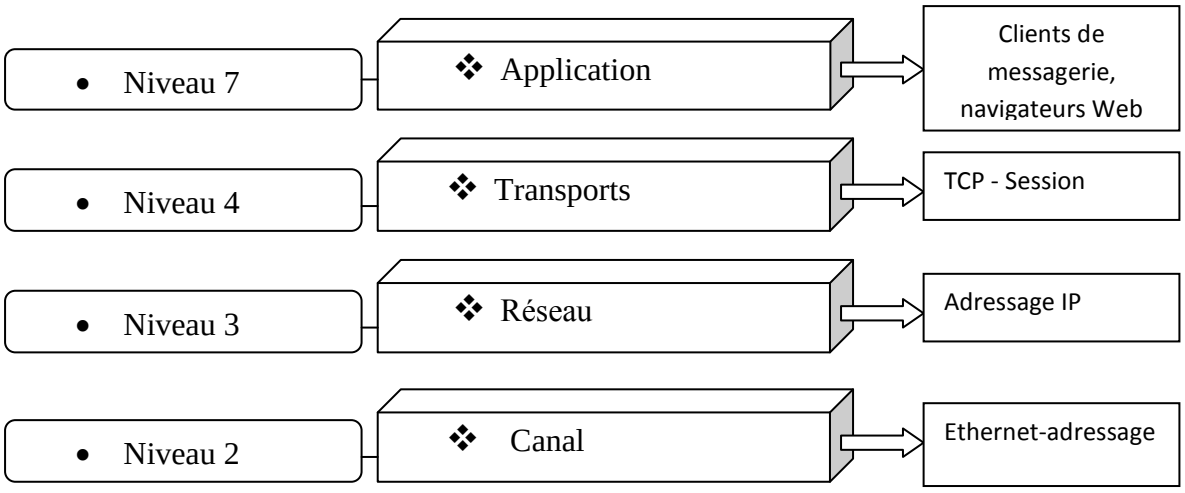
A ce niveau, il ya la possibilité de recourir à la médiation (Proxy).

Nettoyées chaque protocole de couche d'application peut être saisi par le programme - HTTP-médiateur, FTP-médiateur, etc Mediator chacun services TCP / IP est axé sur le traitement des messages et exerce les fonctions de protection, bien que spécifique au service. Ainsi que la passerelle au niveau circuit, l'application intercepte de la passerelle par des agents de dépistage appropriés paquets entrants et d'envoi, les copies et transmet l'information à la passerelle, et agit comme un serveur proxy, éliminant ainsi le lien direct entre l'interne et le réseau externe (voir Figure 2.5). Cependant, les intermédiaires utilisés par la passerelle d'application, ont des différences importantes par le canal d'intermédiaires passerelles de niveau. Tout d'abord, les intermédiaires de la passerelle d'application liés aux applications logicielles spécifiques, serveurs), et d'autre part, ils peuvent filtrer le flux de messages au modèle de niveau d'application doux.

Caractéristiques:

- Fonctionne au niveau 7;
- Des applications spécifiques;
- Moyennement cher et plus lent, mais plus sûr et permet l'enregistrement des utilisateurs;
- Exige que l'utilisateur ou la configuration du programme pour terminer le travail;

- Exemple: (http) proxy Web;
- La pile de protocole TCP / IP renvoie aux niveaux du modèle OSI comme



suit:

Fig. 2.5. Les niveaux de la relation de la pile de protocole TCP / IP et OSI.

Firewalls modernes fonctionnent à l'un de ces niveaux. Initialement Firewalls ont analysé un plus petit nombre de niveaux, est maintenant plus puissant d'entre eux couvre un plus grand nombre de niveaux. En termes de fonctionnalités, le firewall être obligé d'analyser plus de niveaux, plus complet et plus efficace. En raison du niveau de couverture supplémentaire augmente également l'occasion de peaufiner la configuration du Firewalls. La capacité d'analyser des niveaux supérieurs permet le Firewalls pour fournir des services axés sur l'utilisateur, telles que l'authentification de l'utilisateur. Firewalls qui fonctionne aux niveaux 2, 3 et 4, ne traite pas de cette authentification.

Indépendamment de l'architecture du Firewalls peut avoir des services supplémentaires. Ces services comprennent la traduction d'adresses réseau (NAT), le soutien de Dynamic Host Configuration Protocol (DHCP) et le cryptage, étant ainsi le filtrage niveau de la passerelle VPN-point final et le contenu de l'application.

De nombreux Firewalls modernes peuvent fonctionner comme une passerelle VPN. Ainsi, une organisation peut envoyer en clair le trafic réseau sur le

système, qui se trouve derrière un Firewalls, le système distant, situé derrière le VPN-passerelle d'entreprise, Firewalls crypte le trafic et le transmet au VPN passerelle à distance, qui sera le décoder et de donner au système cible. Beaucoup de Firewalls le plus populaire aujourd'hui combiner ces caractéristiques.

De nombreux Firewalls comprennent également des technologies de filtrage des contenus divers active. Ce mécanisme diffère de la fonction de Firewalls classique que Firewalls a maintenant également la possibilité de filtrer les données réelles d'application à 7 qui s'étendent à travers. Par exemple, ce mécanisme peut être utilisé pour détecter les virus dans le fichier joint au message électronique. Il peut également être utilisé pour filtrer le contenu technologique actif le plus dangereux au Web, comme Java, JavaScript et ActiveX. Ou il peut être utilisé pour filtrer le contenu ou un mot clé afin de limiter l'accès aux sites ou domaines inappropriés. Toutefois, le filtre des composants, Firewalls intégré, ne doit pas être considéré comme le seul mécanisme possible pour le filtrage de contenu, peut-être similaire à l'utilisation de filtres en utilisant la compression, le cryptage et d'autres technologies.

2.2 Architecture de firewalls et leur configuration

Les Firewalls peuvent être configurées dans l'une des nombreuses architectures qui offrent différents niveaux de sécurité différents pour les coûts d'installation et l'efficacité de la maintenance. Les organisations devraient revoir leur profil de risque, et sélectionner l'architecture appropriée. La section suivante décrit l'architecture typique du Firewalls et de donner des exemples de politiques de sécurité pour eux.

Hôte connecté à deux segments du réseau, et il est un hôte qui a plus d'une interface de réseau et chaque interface de réseau connecté à un segment de réseau physique distinct. L'exemple le plus courant est l'hôte connecté aux deux segments.

Le Firewalls sur la base de l'hôte connecté à deux segments de réseau - est un Firewalls avec deux cartes de réseau, chacune d'elles est connectée à un réseau

séparé (figure 2.6). Par exemple, une carte réseau est connecté à un réseau externe ou non fiable, et l'autre - sur le réseau intérieur ou sécurisé.

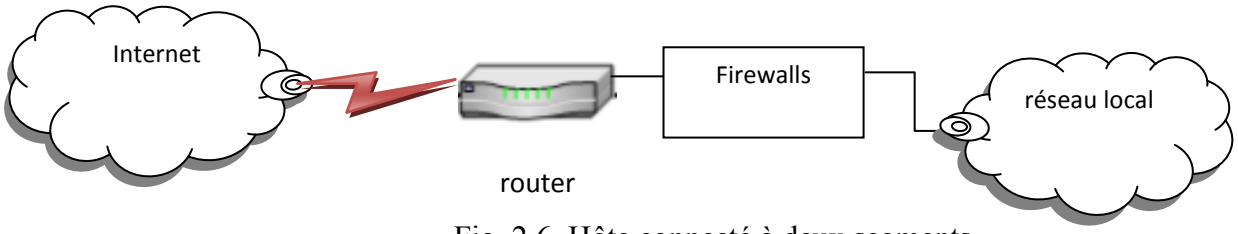


Fig. 2.6. Hôte connecté à deux segments

Dans cette configuration, le principe fondamental de la sécurité est d'empêcher le routage direct du trafic sur le réseau de confiance n'est pas approuvé - le Firewalls doit toujours être au même intermédiaire.

Routage doit être désactivé sur le Firewalls du type IP-paquets d'un réseau ne pouvaient pas passer à un autre réseau.

Cette configuration est probablement l'un des moins cher et le plus courant dans le réseau local connexion dial-up d'entreprise à l'Internet. Prenez la machine sur laquelle vous installez FreeBSD, et ensuite sur le routage est interdit, en outre configuré de manière appropriée dans le noyau filtre de paquets (ipfw).

Accueil blindé et blindé type d'architecture d'hôte utilisé par l'hôte (appelé un bastion), qui peut se connecter de n'importe quel hôte externe, mais refuser l'accès à tous les autres, les hôtes moins sûres domestiques. Ce routeur de filtrage est configuré de telle sorte que toutes les connexions au réseau interne du réseau externe sont envoyés au bastion.

Si la passerelle est un filtrage de paquets est réglé, le bastion doit être configuré de sorte que toutes les connexions de réseaux externes passent à travers elle pour empêcher la connexion directe entre le réseau informatique et l'organisation de l'Internet.

Sous-réseau filtré et l'architecture du réseau projeté substantiellement coïncide avec l'architecture hôte à écran, mais ajoute une autre ligne de défense, à l'aide d'un réseau dans lequel un bastion est séparé du réseau interne.

Sous-réseau filtré doit être mis en œuvre par l'ajout de réseau périmètre afin de séparer le réseau interne de l'extérieur. Cela garantit que même si une

attaque réussie sur le bastion, l'attaquant ne sera pas en mesure de répercuter sur le périmètre du réseau, en raison du fait que, entre le réseau interne et le périmètre, il ya un autre routeur de filtrage.

2.3 Sélection d'une configuration de Firewalls pour protéger l'organisation du réseau de données

Firewalls optimales pour les petites et moyennes entreprises avec de faibles exigences en matière de sécurité

Cette section présente le matériel répandu et Firewallsx logiciels et fournit des recommandations pour leur utilisation, en fonction de la taille de l'organisation, le niveau de solutions de sécurité et de coût requis. Dans la première partie du document, solutions qui sont optimales pour les petites et moyennes entreprises avec de faibles exigences en matière de sécurité, et le second - solutions pour les petites et moyennes entreprises et les succursales qui ont besoin d'une protection fiable.

Sélection

À l'heure actuelle le choix de Firewalls est très large, allant de la simple (et gratuit) Firewalls Windows, hébergé sur la machine protégée de Firewalls haute performance avec Stateful Packet Inspection, une valeur de dizaines de milliers de dollars. Comment choisir la meilleure option pour une entreprise en particulier? Lors du choix d'un Firewalls doit tenir compte de deux facteurs principaux: les exigences de sécurité et de coût.

Les exigences de sécurité sont en constante évolution. L'administrateur doit combiner la protection et la commodité de l'accès des utilisateurs aux données, ainsi que pour tenir compte des limitations fondamentales des programmes dans lesquels les auteurs accordent peu d'attention à la sécurité de la machine hôte et le réseau.

Valeur limite. Prix - barrière entre les désirs et la réalité. Le principal obstacle à haute sécurité - les coûts qui sont ou peuvent être prêts à assumer

l'utilisateur. Le niveau de protection offert par un routeur large bande simple pour les petits bureaux / bureaux à domicile inspection des paquets, soit nettement moins que dans l'application de Firewalls industriel avec stateful packet inspection et de contrôle au niveau de l'application. En général, plus le coût du Firewalls, plus la sécurité. Le niveau de sécurité est conforme aux coûts encourus par l'organisation (sur un achat ponctuel de matériel et de logiciel, ou pour payer des consultants en gestion des solutions peu coûteuses).

Solutions présentés dans la section et le marché de Firewalls est extrêmement vaste et diversifié, de sorte qu'il est impossible d'évaluer chaque fournisseur. Pour commander quelques tableaux, choisis plusieurs fournisseurs de couvrir tout le spectre de la fiabilité et du coût de l'inspection de paquets du Firewalls traditionnel aux dispositifs d'inspection de paquets mixtes et applications visant à répondre aux menaces à la (gestion de la menace universelle, UTM) universel. Cet article présente des fournisseurs tels que Cisco Systems, Network Engines, RimApp, SonicWall et Symantec.

L'accent principal dans l'examen de Firewalls réseau pour les entreprises de différentes tailles et les exigences de sécurité mis sur le niveau de protection, plutôt que les caractéristiques du routage et des fonctionnalités avancées de l'appareil. De nombreux fournisseurs de Firewalls de frais supplémentaires pour les fonctions avancées de routage qui n'affectent pas le niveau de sécurité. Par exemple, pas envisagé de routage à base de règles, la qualité du service, le niveau de transparence du réseau de contrôle de la communication et d'autres améliorations, qui ont peu d'effet sur la sécurité globale.

D'autre part, les produits de certains fournisseurs ont intégré la mise en cache Web, augmente considérablement la valeur globale de l'acquisition d'une organisation qui n'a pas besoin d'acheter une solution distincte pour mettre en cache. Le résultat est une amélioration des performances pour le Web et réduit le coût global de fonctionnement des canaux Internet. La présence de proxy Web augmente également la sécurité.Performances d'estimation de Firewalls et ci-

dessous un bref aperçu des caractéristiques qui sont pris en compte dans l'évaluation des Firewalls matériels.

Prix. Le coût de Firewalls spécifiques de différents fournisseurs peuvent varier considérablement. Les informations contenues dans ce rapport reflète le prix d'un ensemble standard de fonctionnalités sans modules supplémentaires qui doivent être achetés séparément. Les modules d'extension peuvent augmenter considérablement le prix indiqué.

Contrôle au niveau de la demande, selon l'état. Contrôle au niveau de la demande, selon l'état est de tester les deux têtes de protocole et des données d'application en utilisant un mécanisme de contrôle au niveau de l'application. Exemples - inspection en profondeur les données de la couche application et en-tête HTTP, données et en-tête SMTP, les données et les têtes de protocole de messagerie instantanée (IM).

Le contrôle du protocole d'application. Control Protocol Application (autrement, l'inspection des paquets en profondeur - deep packet inspection) vous permet d'analyser protocole de niveau application et de confirmer sa conformité avec l'IETF (Engineering Task Force Internet) pour les jeux d'instructions des protocoles. Exemples - contrôle protocoles DNS, FTP, POP3 et SMTP. Dans l'application de contrôle d'inspection de protocole de processus pour répondre aux conditions requises de toutes les données au niveau de l'application n'est pas satisfaite.

Packet Inspection du respect des conditions spécifiées.Cette méthode fournit un réseau de têtes de contrôle et de couches de transport dans le mécanisme de paquets Firewalls filtrant. Packet Inspection du respect des conditions spécifiées et utilisées dans presque tous les Firewalls modernes, et à un moment donné était la méthode standard de protection.

Windows authentification transparente. Merci au Firewalls d'authentification transparente reçoit les informations d'identification de l'utilisateur du système d'exploitation du client sans interférence. Un contrôle strict

des utilisateurs d'accès externes et les groupes effectuée sans demander des informations d'identification des utilisateurs.

Enregistrement de tous les noms d'utilisateur et des applications Web, et Winsock. L'exploitation forestière - une condition préalable à la préparation de rapports complets sur la conformité avec la loi et efficace coopération avec les forces de l'ordre. Une fois connecté noms d'utilisateur et les applications Winsock Firewalls reçoit les informations sur les applications et les ressources disponibles pour l'utilisateur lors de la connexion à travers le Firewalls.

Contrôle au niveau de l'application par les tunnels SSL (Secure Sockets Layer). Cette commande vous permet de vérifier la conformité avec les conditions spécifiées et d'analyser le protocole de connexion SSL dans un tunnel crypté. Firewalls, qui ne fournissent que l'inspection de paquets pour le respect de ces critères ne peuvent pas contrôler les titres et les données de la couche application dans les tunnels cryptés SSL.

Prise en charge de Microsoft Exchange Server. Firewalls avec prise en charge pour Exchange améliorer la sécurité pour les connexions distantes via Internet avec les services de change, y compris Outlook Web Access (OWA), Outlook Mobile Access (OMA), Exchange ActiveSync, Secure RPC Exchange et RPC sur HTTP. Cette fonctionnalité intègre des authentification à deux facteurs, tels que RSA SecurID de RSA Security.

La passerelle de commande et de trafic client VPN au niveau de l'application. En surveillant la passerelle et les connexions des clients VPN pour le Firewalls vérifie les paquets pour le respect des conditions spécifiées et les connexions de tunnel à travers PPTP, Layer Two Tunneling Protocol (L2TP) / IPsec IPsec ou au niveau de l'application. Contrôle de l'application des connexions VPN de couche à travers le canal pour empêcher la propagation de ces «vers» que Blaster et Sasser. Par exemple, Firewalls, ISA Server 2004, Microsoft assure que la procédure à distance standard de l'entreprise appels RPC (Remote Procedure Call) et blocs Blaster et des menaces similaires.

Détecter et prévenir les accès non autorisés. Méthodes pour détecter et empêcher l'accès non autorisé axée sur le réseau des anomalies et des couches de transport, menaçant ensemble de protocoles, TCP / IP Firewalls. La plupart des systèmes de détection, Firewalls et système de détection d'intrusion de prévention d'intrusion (IDS) / Système de prévention des intrusions (IPS) peuvent être configurés pour transférer les administrateurs d'alertes à l'activisme ou d'un avertissement à l'adoption de mesures visant à prévenir l'attaque. Dans la pratique, la plupart des Firewalls IDS / IPS interdisent tout accès non autorisé au moment de la détection.

Serveur VPN d'accès distant et la passerelle VPN. Serveur d'accès distant VPN accepte les connexions des clients à partir de systèmes VPN, et le système se connecte au réseau de l'entreprise. La passerelle VPN relie l'ensemble du réseau via un VPN inter-site-connexion.

VPN-client. Pour tout le client distant traditionnel connexions VPN besoin d'un programme client (un VPN SSL sans client est utilisé comme un navigateur client). La plupart des Firewalls autorisent les connexions PPTP et L2TP/IPsec avec Windows intégré VPN client de Microsoft. Certains Firewalls exigent supplémentaire (étendue) du logiciel client VPN, ce qui permet une vérification de la conformité aux exigences de sécurité client VPN, IPSec et des protocoles spéciaux pour le passage Network Address Translation NAT (Network Address Translation). Ces programmes sont fournis gratuitement, mais parfois ils doivent être achetés séparément.

Ports LAN 10/100-Mbps. Firewalls avec plusieurs ports Ethernet, dédié aux connexions locales, fournit une segmentation physique profonde des zones de sécurité. Certains Firewalls ont plusieurs ports Ethernet, mais limité le nombre de ports qui peuvent être utilisés pour se connecter à l'Internet.

Ports WAN. Certains Firewalls limitent le nombre de ports pour la connexion directe à Internet. Dans d'autres, à cette fin, vous pouvez utiliser n'importe quel nombre de ports.

Équilibrage de charge. Plusieurs Firewalls peuvent être connectés en parallèle et d'équilibrer les connexions entrantes et sortantes via le Firewalls. Idéalement, le composé uniformément distribué entre le Firewalls et les résultats de chaque dispositif sont en train de s'améliorer grâce à prévenir la surcharge des Firewallsx individuels.

Le nombre d'utilisateurs. Certains firewalls nombre limité d'utilisateurs ou adresses IP qui peuvent établir des connexions à travers le Firewalls. Ces Firewallsx sont autorisés à travailler avec un certain nombre d'utilisateurs, et, si la licence est dépassé seuil, une alerte est générée.

Les fonctions de transfert du dispositif de coupe-feu défaillant fonctionne correctement. Cette fonction permet de connecter deux ou plusieurs Firewalls afin qu'ils puissent servir à la place des dispositifs échoué composés. Les réservations peuvent être "froid" (sans charge), "à chaud" (en charge) ou l'équilibrage de charge. Certains procédure de commutation automatique, et dans d'autres cas nécessitent une intervention de l'administrateur.

Mise Internet-fournisseur et l'association de la bande passante. La possibilité de travailler avec plusieurs fournisseurs Internet - La condition la plus importante de toute organisation qui dépend de la connexion à l'Internet. Firewalls avec le changement de prestataires Internet peuvent passer à une ligne disponible si la communication avec un ou plusieurs fournisseurs est interrompue. La combinaison de bande passante se connecte plusieurs lignes de communication dans la vitesse d'accès canal ressources Internet.

Personnaliser. La plupart des Firewalls offrent des connexions Web SSL dans certaines ou toutes les configurations. Certains logiciels de Firewalls prend en charge une interface de ligne de commande dans une session de terminal et les Firewalls basé sur ISA Server fournit des connexions chiffrées RDP, conforme traitement FIPS (Federal Information Processing Standard).

Processeur. Cette fonctionnalité ne nécessite aucune explication supplémentaire. Elle indique le type et la vitesse du Firewalls du processeur principal.

Web-cache et proxy-serveur. Certains Firewalls ont intégré dans le cache du serveur Web. Web-cache accélère l'accès à Internet pour l'utilisateur final et peut réduire considérablement la charge sur le canal de communication avec l'Internet et ses coûts associés. Composant proxy Web augmente considérablement la sécurité, la décomposition pleinement en ses parties constituantes, puis vérifier et réparer les messages transitant par HTTP.

Les faibles niveaux de sécurité et comme mentionné plus haut dans cet article, les Firewalls sont considérés en conformité avec le niveau de sécurité de l'entreprise nécessaire. Les Firewalls sont le premier type sont conçus pour les petites et moyennes entreprises avec un faible niveau de sécurité. Dans un environnement faiblement protégé les données sensibles ne sont pas stockées dans le réseau ou le propriétaire des informations confidentielles ne peuvent pas ou ne veulent pas payer pour le Firewalls de réseau avec la numérisation puissantes de l'accès entrant et sortant, paquet et la couche application, l'exploitation complète des actions de l'utilisateur et des applications.

En règle générale, les réseaux mal protégés appartiennent à de petites entreprises avec un budget limité. LAN peut être connecté à Internet via un modem câble haut débit ou connexion ADSL avec le soi-disant «routeur à large bande" au lieu de lignes louées et des niveaux plus élevés de T, plus fréquente dans les grandes organisations. Techniquement routeurs à large bande ne s'appliquent pas aux routeurs et périphériques sont simples NAT. La plupart de ces appareils vous permet de définir quelques connexions VPN en utilisant le logiciel propriétaire client VPN.

La limite supérieure de la fourchette de prix de Firewalls pour une protection avec un faible niveau de protection - autour de 500 dollars si sur le net avec un faible niveau de sécurité n'est pas soumis aux rigueurs de la supervision de l'application de la loi, et la société dispose d'un budget très limité, vous devez faire attention aux produits de Cisco, SonicWall et Symantec, Caractéristiques comparées sont donnés dans le tableau 2.1.

Trois Firewalls ont des fonctionnalités similaires, les capacités et les niveaux de protection contre les menaces extérieures. Chaque paquet fournit un contrôle sur le respect des conditions spécifiées dans les connexions entrantes à l'Internet. Cela appareils de faible puissance, il ya des limites importantes sur le nombre d'utilisateurs. Le nombre de connexions est déterminé par le régime d'autorisation et de la capacité de chaque fournisseur de matériel.

Plus important encore, ces Firewalls n'ont pas les moyens de contrôler l'accès entrant et sortant pour les utilisateurs et les groupes. La fonction d'enregistrement de tous les appareils sont primitives. Il n'ya pas de contrôle sur le respect des conditions spécifiques au niveau de l'application. Ces restrictions sont typiques des Firewalls matériels à faible coût.

Du trio est recommandé d'utiliser un dispositif simple à configurer SonicWall 170, qui fonctionne presque automatiquement. SonicWall 170 offre une interface moderne, à travers laquelle vous pouvez passer à une connexion modem analogique si le lien à haut débit primaire. De plus, 170 SonicWall une voie locale est plus grande que les deux autres appareils.

Sécurité réseau - une composante essentielle de la stratégie globale de l'entreprise de défense en profondeur. Firewalls de réseau - les éléments clés de la protection des données et du système pour une variété de périmètres de réseau. Les entreprises ayant de faibles exigences en matière de sécurité peuvent choisir l'un des Firewalls d'une table ou d'autres produits de ce niveau, mais pour les dispositifs de protection fiables sont nécessaires pour être considéré comme ci-dessous.

Firewalls matériel pour l'environnement de réseau avec une faible fiabilité.

Tableau 2.1

	SonicWall 170	Cisco PIX 501	Symantec Firewall/VPN
Prix en US	410	495	499
Contrôle au niveau de la demande, selon l'état	Non	Non	Non
Control Protocol application	Oui (limité)	Oui (limité)	Oui (limité)
Packet Inspection du respect des conditions spécifiées	Oui	Oui	Oui
L'authentification Windows Transparent	Non	Non	Non
Enregistrement de tous les noms d'utilisateur et des applications Web et Winsock	Non	Non	Non
Contrôle au niveau de l'application à travers des tunnels SSL	Non	Non	Non
le support pour Exchange	Non	Non	Non
La passerelle de commande et de trafic client VPN au niveau de l'application	Non	Non	Non
Détection et la prévention de l'accès non autorisé	Oui	Oui	Oui
Serveur distant VPN d'accès et une passerelle VPN	Oui	Oui	Non
VPN-client	Non	Non	Non
Ports LAN 10/100-Mbps	5	4	4
Ports WAN	1	1	1
Load Balancing	Non	Non	Non
nombre d'utilisateurs	10	10	15-25
Les fonctions de transfert du dispositif de coupe-feu défaillant fonctionne correctement	Le cadran analogique avec un modem externe	Non	Le cadran analogique avec un modem externe
Internet fournisseur de commutation et de combiner la bande passante	Non	Non	Non
Définition	Interface basée sur le Web	La ligne de commande et sur le Web	Interface basée sur le Web
processeur	Processeur de sécurité SonicWALL	AMD SC520	ARM7
Web-cache et proxy-serveur	Non	Non	Non

Options pour les petites et moyennes entreprises ayant des exigences de sécurité élevées dans les organisations où la protection doivent payer beaucoup d'attention aux Firewalls imposé des exigences beaucoup plus élevées. Amélioration de la sécurité peut être causée par les conditions de la loi, la nature de l'entreprise (par exemple, dans les secteurs où la concurrence est intense est nécessaire pour protéger les secrets commerciaux) ou de la volonté du propriétaire pour obtenir une protection convenable à un prix raisonnable. Dans les petites et moyennes entreprises de haute sécurité pour le Firewalls sont traités comme l'assurance automobile. Ces organisations sont prêtes à payer à l'avance pour éviter une catastrophe potentielle.

Le problème de fournir un niveau élevé de sécurité lors du choix d'un Firewalls avec un niveau accru de protection est nécessaire d'examiner un certain nombre d'exigences supplémentaires.

Il faut identifier le traitement du réseau de l'entreprise à l'Internet. Au minimum, vous devez écrire le nom et applications impliqués dans les tentatives pour accéder aux ressources à travers le Firewalls. Il est également recommandé de préciser les noms des sites et le type de contenu.

Il faut un mécanisme paramètres de Firewalls pour bloquer les applications de lancement, qui constituent une menace pour l'intégrité du réseau et les données - par exemple, un pair (P2P) et les programmes de messagerie instantanée (Instant Messaging - IM).

Le Firewalls doit arrêter le trafic non autorisé à la fois entrants et sortants, l'inspection des paquets pour le respect des conditions spécifiées et le contrôle au niveau de l'application pour toutes les interfaces, y compris VPN.

Le Firewalls doit fournir l'inspection des paquets pour le respect des conditions spécifiées et le contrôle au niveau de l'application pour le trafic entrant en passant par le Firewalls de réseau de l'entreprise afin que les utilisateurs distants peuvent accéder aux données provenant de l'extérieur de l'entreprise. Vérification du respect des conditions prévues doivent être effectuées sur les données chiffrées pour la transmission sur les lignes de communication.

Bloquer ou atténuer les effets des vers, virus, logiciels espions et autres menaces à l'intégrité des données à la périphérie du réseau, le contrôle au niveau de l'application est nécessaire à toutes les étapes.

Si vous souhaitez accéder à des affaires importantes - l'information doit fournir des mécanismes de tolérance aux pannes.

Malgré les exigences de sécurité élevées à respecter par certaines petites entreprises, ces entreprises restent encore faibles et ne disposent pas d'un budget de grandes sociétés. En moyenne, une petite organisation est prête à dépenser jusqu'à 3000 $ sur la solution de sécurité, ce qui rendra la vie de 3-4 ans. Solutions du prix journalier pour dépréciation (environ 2 dollars par jour) est faible par rapport aux pertes financières qui pourraient découler de choisir une des solutions fiables.

Sélectionnez Devices

Les tableaux 2.2 et 2.3 résument les Firewalls matériels qui assurent la sécurité du réseau acceptable pour ceux qui ont besoin d'une protection sérieuse pour les petites et moyennes entreprises.

Firewalls matériel pour les petites entreprises avec des exigences de sécurité élevées. Tableau 2.2.

Caractérisation	SonicWALL Pro 3060	Cisco PIX-515E-R-DMZ	Network Engines NS6200	Symantec SGS 5420
Prix en US	2319	2699	2499	2999
Contrôle au niveau de la demande, selon l'état	Non	Oui (limité)	Oui (modérément)	Oui (limité)
Control Protocol application	Oui	Oui	Oui	Oui
Packet Inspection du respect des conditions spécifiées	Oui	Oui	Oui	Oui
L'authentification Windows Transparent	Non	Non	Oui	Non
Enregistrement de tous les noms d'utilisateur et des applications Web et Winsock	Non	Non	Oui	Non
Contrôle au niveau de l'application à travers des tunnels SSL	Non	Non	Oui	Non
le support pour Exchange	Non	Non	Oui	Non

La passerelle de commande et de trafic client VPN au niveau de l'application	Non	Non	Oui	Non
Détection et la prévention de l'accès non autorisé	Oui	Oui	Oui	Oui
Serveur distant VPN d'accès et une passerelle VPN	Oui	Oui	Oui	Oui
VPN-client	Non	Oui	Oui	Non
Ports LAN 10/100-Mbps	5	2	3	5
Ports WAN	1	1	1	1
Load Balancing	Non	Non	Oui	Non
Nombre d'utilisateurs	Unlimited.	Unlimited.	Unlimited.	50
Les fonctions de transfert du dispositif de coupe-feu défaillant fonctionne correctement	Non	Non	Non	Non
Mise Internet-fournisseur et la bande passante	Non	Non	Non	
Définition	Interface basée sur le Web	La ligne de commande et sur le Web	Narrow Web et compatible FIPS RDP	Interface basée sur le Web
Processeur	2 GHz Intel	1 GHz Intel	2 GHz Intel	Intel
Web-cache et de proxy	Non	Non	Oui	Non

Firewalls matériel pour les grandes entreprises avec des exigences de sécurité élevées. Tableau 2.3.

Caractérisation	SonicWALL Pro 4060	Cisco PIX-515E UR-FE-BUN	RimApp RoadBLOCK F302PLUS
Prix en US	4995	5145	5580
Contrôle au niveau de la demande, selon l'état	Non	Oui (limité)	Oui
Control Protocol application	Oui	Oui	Oui
Packet Inspection du respect des conditions spécifiées	Oui	Oui	Oui
L'authentification Windows Transparent	Non	Non	Oui
Enregistrement de tous les noms d'utilisateur et des applications Web et Winsock	Non	Non	Oui
Contrôle au niveau de l'application à travers des tunnels SSL	Non	Non	Oui
le support pour Exchange	Non	Non	Oui
La passerelle de commande et de trafic client VPN au niveau de l'application	Non	Non	Oui
Détection et la prévention de l'accès non autorisé	Oui	Oui	Oui

Serveur distant VPN d'accès et une passerelle VPN	Oui	Oui	Oui
VPN-client	Non	Oui	Oui
Ports LAN 10/100-Mbps	5	6	2-5
Ports WAN	1	1-4	1-5
Load Balancing	Non	Non	Oui
nombre d'utilisateurs	illimité	illimité	illimité
Les fonctions de transfert du dispositif de coupe-feu défaillant fonctionne correctement	Oui	Oui	Oui
Internet fournisseur de commutation et de combiner la bande passante	Oui	Non	Oui
Configuration de l'interface basée sur le Web	La ligne de commande et sur le Web	Un site complet et compatible FIPS RDP	
processeur	2 GHz Intel	433-MHz Celeron	2.8-GHz Intel
Web - la mise en cache et de proxy	Non	Non	Oui

SonicWALL Pro 3060 et Cisco PIX 515E--RDMZ de Firewalls matériels systèmes traditionnels Cisco. Network Engines NS6200 entreprise basée sur Microsoft ISA Server 2004 et SGS 5420 de Symantec sont des produits qui sont communément appelés Firewalls "logiciel" - ils fonctionnent sur la base d'un système d'exploitation d'usage général ou avoir des disques durs (parfois il ya deux composantes). NS6200 est le Firewalls "de troisième génération", dans lequel la stabilité et la fiabilité du Firewalls matériel, combinée à la flexibilité, de facilité de mise à niveau et la volonté de refléter le dernier produit de menaces. Caractéristiques SGS 5420 - intermédiaires: il ne fonctionne pas avec un système d'exploitation d'usage général, mais il a un disque dur.

Dispositifs de sécurité réseau recommandé Network Engines et Symantec, qui dépassent matériel modèle packet inspection traditionnelle pour le respect des conditions spécifiées. La principale différence réside dans la profondeur de contrôle au niveau de l'application, s'assurer que les deux appareils, par rapport aux Firewalls SonicWALL et Cisco.

Pour contrôler les Firewalls au niveau des applications de sa catégorie, vous pouvez utiliser intégré et les modules d'extension externes (par exemple, anti-virus, filtrage des fichiers téléchargés, filtrage du courrier, le blocage de pop-up

publicitaires, analyse du contenu Web). Dans ce cas, en raison du prix élevé de l'appareil peut être hors de portée pour les petites et moyennes entreprises.

Il a finalement été donné au Firewalls réseau moteurs préférence à l'appareil grâce à ses mérites Symantec, décidant de créer un environnement de réseau avec un niveau de sécurité élevé.

Authentification transparente pour toutes les connexions sortantes via le Firewalls. Dans un environnement avec un niveau élevé de sécurité pour l'enregistrement d'un domaine nécessite une authentification à deux facteurs. Merci à l'authentification transparente, les utilisateurs ne peuvent pas partager les informations d'identification pour l'accès à l'Internet, parce que le système n'affiche jamais l'écran de connexion. Il en résulte une amélioration de la précision des informations contenues dans le magazine et l'efficacité d'une nouvelle enquête sur la base de ces informations.

Journalisation complète de toutes les connexions entrantes et sortantes via le Firewalls. Ces informations, y compris les noms des utilisateurs et les applications concernées à accéder aux ressources sur le Firewalls, sont essentiels à l'audit de performance pour le respect de la loi et dans les enquêtes administratives, pénales et civiles.

Contrôle au niveau de l'application tunnels SSL (Secure Sockets Layer - secure sockets layer). NS6200 dispositif basé sur ISA Server 2004 effectue un contrôle des connexions SSL entrantes application de la couche à travers le Firewalls. Ces composés peuvent être utilisés pour des références à des données privées sur le serveur Microsoft Outlook Web Access (OWA) ou Microsoft SharePoint Portal Server. Contrairement à d'autres Firewalls dans le tableau 2.3, NS6200 peuvent décrypter connexion SSL à travers le Firewalls, en-têtes et le mécanisme de transfert de données est appliquée à la gestion du Firewalls, puis re-crypter les données pour la livraison via la connexion cryptée sécuritaire.

Packet Inspection du respect des conditions prévues et le contrôle au niveau de l'application sur tous les VPN-interfaces. Ce test porte sur les liens de la passerelle d'accès à distance VPN entre sites. Canaux VPN sont souvent le maillon

faible dans de nombreux Firewalls ainsi que connecté à la machine VPN, généralement considéré comme «de confiance» et ne sont pas soumis à un contrôle au niveau de l'application. Cette approche a été la principale cause de l'attaque du ver Blaster sur le réseau, autrement protégés contre les menaces extérieures. Dangers Blaster similaires, existent encore, et connexions VPN peuvent encore servir comme moyen de distribution. NS6200 ouvre des canaux VPN pour contrôler au niveau des applications et bloque les attaques sur le Firewalls.

Même avec les modules d'extension coûteuses à contrôler au niveau de l'application, aucun autre Firewalls n'a pas les caractéristiques de sécurité mis en œuvre dans le NS6200.

Plus de réseaux à grande échelle avec un niveau élevé de protection et moyennes et grandes entreprises, ainsi que leurs sociétés affiliées caractéristiques des exigences de sécurité similaires. Comme les petites entreprises avec robustes, ils nécessitent une inspection des paquets complets pour le respect des conditions spécifiées et le contrôle au niveau de l'application, l'exploitation complète et des fonctionnalités de contrôle d'accès des utilisateurs / groupes à travers le Firewalls. La principale différence entre une sécurité grande entreprise et une petite entreprise n'est sociétés d'énergie beaucoup plus financiers qui répondent aux exigences de sécurité de l'information.

Ces entreprises n'ont pas besoin de les firewalls les plus technologiquement avancés et de haute performance coûtent 35 mille dollars, ils ont probablement besoin d'une protection de l'information fiable. La seule attaque au niveau de l'application peut conduire à des pertes de plusieurs millions de dollars.

Calculez combien d'argent l'organisation de ce type sont prêts à dépenser pour une protection de Firewalls, n'est pas facile. Certaines entreprises donnent la sécurité sont extrêmement importantes et sont prêts à payer plus de 10 mille dollars pour l'excellent Firewalls avec inspection des paquets avec état et de contrôle au niveau de l'application. D'autre part, beaucoup de moyennes et grandes entreprises qui ont besoin d'une sécurité robuste, sont réticents à payer plus de 2500 $ pour

cette composante essentielle de l'infrastructure de sécurité réseau. En général, la plupart des organisations de cette taille consacre volontiers de 5000 à 6000 $ pour un bon Firewalls.

Généralement déployé dans les grandes entreprises avec un haut niveau de sécurité. SonicWALL PRO 4060 et Cisco PIX 515E-UR-FE-BUN sont basées sur Firewalls matériel traditionnel et assurent le niveau de sécurité du réseau. Packet Inspection du respect des conditions spécifiées - la base de produits de sécurité pour sa mise en œuvre ne nécessite pas de modules d'extension coûteux. Les deux modèles sont dotés de hautes performances, mais il manque l'équilibrage de charge des capacités et des fonctions de transmission de l'appareil défaillant fonctionne correctement, si elles sont essentielles pour un accès ininterrompu aux données critiques.

En revanche, les F302PLUS de barrage de périphériques basés sur ISA Server 2004 fournit une RimApp complet de contrôle au niveau de l'application, à un prix abordable. Dans la configuration standard, les filtres sont mis en œuvre des sites Web, vérifier les fichiers téléchargés à partir d'Internet pour les virus et les filtres anti-spam. En outre, des modules et Rainwall RainConnect du dispositif de barrage de Rainfinity fournit l'équilibrage de charge et les fonctions de transfert du périphérique défaillant fonctionne correctement pour le matériel Firewalls barrage et des canaux de communication sur Internet des fournisseurs. dispositif de RoadBLOCK prend en charge toutes les fonctions et les rapports de haut niveau mentionnés ci-dessus, l'exploitation forestière, et dispose de fonctionnalités puissantes pour la commande d'un utilisateur et l'accès du groupe de connexions entrantes et sortantes via le Firewalls.

Le choix optimal du réseau et les Firewalls de haut niveau, dans cette section, fournir un excellent niveau de sécurité et de haute performance pour les moyennes et grandes entreprises.

3. SECURITE DES PERSONNES

3.1. Types et les conditions de droit du travail

Les facteurs les plus importants en termes de performance humaine psycho-physiologique liée à la sécurité, sont le type de travail, de sa gravité et de l'intensité, ainsi que les conditions dans lesquelles l'd'activités de travail.

Le travail physique est caractérisé par une augmentation de la charge de muscle sur le système musculo-squelettique, le système cardiovasculaire, neuromusculaire, respiratoires, etc Il développe un système de muscles, stimule les processus métaboliques dans le corps, mais en même temps peut avoir des conséquences négatives, par exemple, provoquer des maladies de l'appareil locomoteur dans la mauvaise organisation et la sur-intensification du flux de travail. Aujourd'hui, le travail purement physique est rare.

Classification moderne de travail sur les formes de travail suivantes.

Travail mécanisé - nécessite moins d'énergie et la sollicitation musculaire, mais se caractérise par la grande vitesse et la monotonie du mouvement humain.

Après la fin de la restauration des fonctions normales de l'organisme à se produire rapidement. Lorsque l'organisme de la maladie ou, en l'absence de compétences dans le travail de cette reprise ralentit.

Le travail sur la bande transporteuse se caractérise par une plus grande vitesse et l'uniformité de mouvement, le temps de l'opération est strictement réglementée. En conjonction avec une tension nerveuse considérable, à grande vitesse et la monotonie des travaux sur la ligne d'assemblage conduit à un épuisement nerveux rapide et la fatigue.

Les travaux sur semi-automatique et automatique pro ¬ duction sont les mécanismes d'entretien périodique des opérations simples. Il nécessite moins d'énergie et de tension par rapport aux travaux sur la ligne d'assemblage.

Le travail mental est associé à l'acquisition et au traitement de l'information, il nécessite une tension de l'attention, la mémoire et améliorer les processus de la pensée, caractérisées par une augmentation du stress émotionnel et

une diminution de l'activité physique. Charge mentale prolongée a un impact négatif sur l'activité mentale - pire mémoire, l'attention, la perception fonction ca ¬ tection de l'environnement.

Formes de travail intellectuel: l'exploitation, la gestion ciel ¬, créatif, le travail des enseignants, des médecins, des étudiants.

Le travail d'enseignement se caractérise par une contrainte ¬ schihsya fonctions de base mentaux ¬ tions - mémoire, l'attention, la présence des examens liés au stress, tests, des documents de test.

Le travail créatif (le travail des scientifiques, des écrivains, des artistes, construction-teurs, compositeurs) - la forme la plus complexe de l'activité mentale, il nécessite un effort de neuro-émotionnelle importante. Solution des problèmes de sécurité est impossible sans prendre en compte les capacités physiques des travailleurs, son efficacité, la capacité de travailler sans blessures et d'accidents.

La performance humaine dépend de nombreux facteurs: le niveau de son développement, son humeur, l'état émotionnel, la volonté, les milieux de travail, la motivation, sur l'organisation et les conditions de travail.

Réduction du rendement résultant de l'été effectuée par un travail particulier, et les sentiments complexes qui lui sont associés, est appelé fatigue.

État de fatigue et physiologique du corps, caractérisé rizuyuscheesya un certain nombre de critères objectifs: ¬ tion augmente la pression artérielle, une diminution de la glycémie, la perte de productivité, la détérioration des sensations subjectives (refus de continuer à travailler, fatigue, etc.)

Si, après le jeu de temps pour se reposer après le travail, capacité à travailler n'est pas entièrement récupéré, vient d'épuisement. Les plus rapides fatigue s'installe lorsque le travail monotone.

Réduire les effets du travail répétitif sur une personne peut être, si elle est faite chaque transaction plus significative, de fusionner les opérations en plus complexe et diversifié. La durée de l'opération ne doit pas être inférieure à 30 secondes, la charge sur les différents organes des sens et les parties du corps doivent alterner. Il est conseillé d'utiliser une ceinture de fréquence libre, de

transférer les travailleurs d'une étape du processus à une autre, régler le rythme variable de la chaîne de montage au cours de la journée de travail (shift). Quand ¬ Menen des conditions optimales de travail et de repos au cours de la journée de travail (shift), la nomination de courtes pauses supplémentaires, l'esthétique de la conformité de production et de mise en œuvre du cadre musical fonctionnelle du processus de production permettront de réduire la monotonie du travail et de la fatigue.

Avec le reste passive pour éviter la fatigue pendant le travail est utilisé loisirs et de gymnastique de fabrication, pause gymnastique.

L'apparition de la fatigue nerveuse (mental) par opposition à la physique (musculaire) n'entraîne pas la résiliation automatique de travail, mais ne provoque l'excitation, changements névrotiques, troubles du sommeil. Les activités à forte prévalence du travail manuel requis courte, mais séjours plus fréquents.

La période de récupération après une activité physique est plus intense, et se termine dans un temps relativement court.

La fatigue nerveuse découle principalement en raison de la ruée vers l', surtension attention, l'ouïe et la vision, de la mémoire et l'activité mentale. Dans le même temps, le travail mental, de façon surprenante, s'écoule très peu, avec un relativement faible consommation d'énergie. En soi, il est peu fastidieux.

Cela implique que le travail UMST-veineuse modérée (pas très occupé) peut être effectuée pendant une longue période sans interruption pour se reposer. Toutefois, les personnes qui oeuvrent principalement dans le travail intellectuel, doit périodiquement un séjour plus long.

Droits en milieu de travail à prédominance travail mental devraient être à l'aise à tous les égards. Microclimat, éclairage ¬ tion, la couleur de la chambre doit remplir les conditions optimales. Cependant, il faut éliminer ces facteurs négatifs comme la monotonie du travail, le bruit, les vibrations, etc

3.2 Base ergonomique pour la protection du travail

Pour créer un cadre confortable et en toute sécurité des conditions de travail à une étude approfondie de l'environnement homme-machine au travail, qui sont étroitement liés et affectent la sécurité, la performance et la santé.

Ergonomie - la discipline scientifique qui étudie les conditions humaines complexes spécifiques de travail dans le secteur manufacturier moderne.

Par personne dans le cadre du travail sont beaucoup de facteurs: le type de travail, de sa gravité et l'intensité, les conditions dans lesquelles elle exerce ses activités (substances nocives, le rayonnement, le climat, l'éclairage, etc), les capacités physiologiques humaines (en particulier les caractéristiques anthropométriques d'une personne , la vitesse de réaction à différents stimuli, les caractéristiques de perception de couleurs humaines, etc.) Afin de système homme-machine de fonctionner efficacement et de ne pas porter préjudice à la santé humaine, il est nécessaire tout d'abord d'assurer la compatibilité des caractéristiques de l'homme et la machine. Compatibilité entre l'homme et la machine est déterminée par la anthropométrique, sensori-motrice, l'énergie (bio-mécanique) et la compatibilité psycho-physiologique.

Compatibilité anthropométrique prend en considération la taille du corps humain, la possibilité de revoir l'espace extérieur, les dispositions de (postures) de l'opérateur pendant le fonctionnement.

Sensori-compatibilité implique la prise en compte de la vitesse du moteur (moteur) homme des opérations et ses réactions sensorielles ¬ tions pour différents types de stimuli (lumière, son, etc) lorsque la vitesse de la machine et de signalisation.

Compatibilité Energy (biomécanique) a pris le pouvoir ¬ Gaeta compte des capacités humaines pour déterminer les efforts déployés par les gouvernements.

Compatibilité Psychophysiological devrait envisager de re ¬ homme d'action sur la couleur, les couleurs, la gamme de fréquences du foyer ¬ signaux Vai, de la forme et d'autres paramètres esthétiques de la machine.

3.3 En milieu de travail

Organisation du travail, de la conception du contrôle et de la gestion doit tenir compte des caractéristiques anthropométriques et sensori-moteur, biomécaniques et physiologiques d'une personne. Importants ergonomiques postures de travail de personne importante. Travailler posture «debout» nécessite une grande dépense d'énergie et d'inculquer ¬ mène à la fatigue rapide. Posture de travail "assis" moins fastidieux, et il est plus préférable. La projection du centre de gravité du corps humain en position de travail doit être situé dans la zone de son palier.

L'espace de travail, qui a mené le processus de travail devrait être divisé en zones de travail. Zonage du lieu de travail dans les plans horizontal et vertical. Région, confortable pour l'action des deux mains de travail, il est nécessaire de combiner avec la zone d'angle visuel. Emplois minimum d'espace nécessaire pour effectuer des travaux à différentes positions du corps.

Sinon, la position du corps est instable Mal ¬, et nécessite un effort musculaire considérable. Cela pourrait conduire ¬ té à la maladie de l'appareil locomoteur (par exemple, l'utilisation ¬ krivlenie colonne vertébrale), fatigue rapide, une blessure. Une partie intégrante du milieu de travail dans la «séance» est un opérateur de chaise de travail. Le siège doit respecter les droits anthropométriques et, si nécessaire, pour tenir compte des modifications apportées au matériel et les vêtements. Les principaux paramètres géométriques de chaises de bureau sont normalisées. Il est conseillé d'utiliser des chaises avec des paramètres réglables (hauteur, inclinaison du dossier) pour régler les sous les caractéristiques anthropométriques de l'individu.

Pieds et des mains contrôles doivent être conformes aux efforts déployés par les caractéristiques biochimiques de la personne et en fonction de la fréquence d'utilisation situé dans les domaines respectifs de portée. Les efforts déployés par les gouvernements ne devraient pas être trop petit pour un homme à surveiller ¬ Vat effectué son mouvement. Dans le même temps, trop d'effort conduit à une

fatigue rapide et la tension sur les muscles. Pour le gouvernement, il existe différents types de recommandations pour les forces jointes optimales.

Les appareils de l'information visuelle de l'opérateur en fonction de leur fréquence d'utilisation, doivent également résider dans les zones respectives de champ visuel humain. Si vous utilisez fréquemment les appareils doivent être situés à l'angle de vision optimal, avec un rare - dans les angles de vision maximal.

Coloriage en couleur, contrôles de taille doit correspondre aux caractéristiques psycho-physiologiques et anthropométriques d'un éclairage de personne en milieu de travail et d'autres caractéristiques de l'environnement lumineux.

3.4 Prodiguer les premiers soins

Premiers secours aux blessés dans un accident prouve ¬ vayut immédiatement sur les lieux avant l'arrivée du médecin ou de transport de la victime à l'hôpital. Chaque employé devrait être en mesure de prodiguer les premiers soins à la victime et l'auto-assistance («self-help»). Lorsque les premiers secours doivent:

1) Supprimer le facteur traumatique;
2) Enlever le patient de la scène;
3) Pour traiter les zones endommagées du corps et arrêter l'hémorragie;
4) Ne pas perturber le site de fracture pour éviter un choc traumatique;
5) Pour livrer la victime à l'hôpital.

Les premiers soins doit être familier avec les blessés. Ceci est particulièrement important dans les fractures, hémorragies graves, perte de conscience, les brûlures thermiques et chimiques. Soulever et transporter les blessés à la prudence, en gardant ci-dessous. PREMIERS SECOURS chaque site de production, chaque chantier doit être équipé du secourisme.

Trousse de premiers soins. Dans une trousse de premiers soins comprend pansements (bandages, coton, forfaits individuels, sparadrap, lingettes stériles,

garrot), l'ammoniac (utilisé pour l'excitation de souffle, traitement de la peau pour les brûlures à l'acide, piqûres d'insectes), une solution alcoolique de 5% de l'iode (pour traitement des plaies), le permanganate de potassium (permanganate de potassium) - pour un lavage d'estomac font solution légèrement rose est également utilisé pour le traitement des plaies, de bicarbonate de soude (pour laver l'estomac, traitement de la peau pour les brûlures), borique Vaseline (pour lubrifier le tissu à la fermeture des plaies pénétrantes, la lubrification peau), du charbon actif (5 ... 10 comprimés se désintègrent et boivent à divers empoisonnement), de l'acide borique (lavage des yeux, le traitement du cuir), de la nitroglycérine (pour la douleur dans le cœur); analgine, aminopyrine (analgésiques), la papavérine (utilisée douleur dans le cœur, une crise hypertensive), des ciseaux, un couteau, un verre de médicaments, le bout des doigts, l'approvisionnement en eau potable.

3.5 Comment soigner les plaies et contusions

Fournir de l'aide doit se laver les mains avec de l'eau et du savon, essuyez-les avec de l'alcool ou de l'iode lubrifier vos doigts. Vous ne pouvez pas laver la plaie avec de l'eau, le purifier, le toucher, même les mains propres. Si la plaie est sale, il vous suffit de frotter la peau autour des bords de la plaie à la périphérie du coton ou de la gaze stérile. Abrasions, des injections, des blessures mineures qui ne saignent pas, lubrifier 5% de teinture d'iode ou de vert brillant, et d'appliquer un bandage.

Les petites blessures peuvent coller une bande de plâtre, avec BF-6, collodion, qui désinfecter la plaie et de protéger contre la contamination ¬ tion. En l'absence de pansement sur le terrain, vous pouvez utiliser un mouchoir propre après humidification avec l'iode.

Les blessures incluent des dommages aux vaisseaux sanguins et saignements, qui peuvent être internes (les plus dangereux) et l'extérieur. Hémorragie interne se produit lors de la pénétration des blessures à la cavité

abdominale ou thoracique, briser les organes internes à la suite d'un choc violent, chute, écrasement, etc Le sang s'accumule avec les cavités internes du corps.

Les symptômes d'une hémorragie interne, une pâleur, une faiblesse, un pouls rapide, l'essoufflement, des étourdissements, de la soif, perte de connaissance. Méthodes à arrêter le saignement interne de premiers secours ne peuvent pas. La victime doit assurer le repos et appeler un médecin. Sur le dommage doit mettre froid (glace, neige, etc.) Hémorragie externe peut être:

1) Capillaires sanguins gouttes agit sur toute la surface de la plaie;
2) Veineuse - sombre couleur rouge sang suit un cours d'eau douce;
3) Le sang - l'oxygène riche en couleur écarlate du sang, coule sous la forme d'un jet pulsé.

Arrêter le saignement veineux peut être imposant un bandage serré sous la zone endommagée ou appliquer un garrot, échouage.

L'hémorragie artérielle plus dangereux. Arrêter le saignement artériel peut être imposant un bandage serré au-dessus de la zone endommagée ou appliquer un garrot, échouage.

Pour une touche, vous pouvez utiliser un foulard, ceinture, ceinture, tuyau en caoutchouc, etc Avant d'appliquer le harnais blessé membre soulevé, la gravure, la torsion appliqués sur les vêtements ou placés en lui un morceau de tissu (Figure 4.1.).

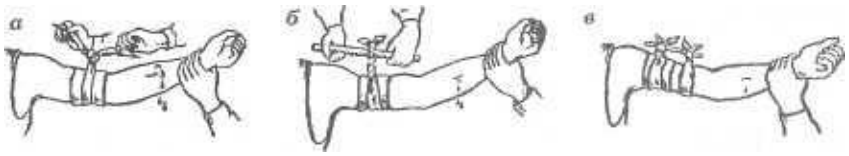


Fig. 4.1. Hémostase torsion: a - le nœud b-torsion avec un bâton, en - curling baguette

Serrez le cordon seulement besoin d'arrêter le saignement. Le câblage ne doit pas être laissé à l'état serré pendant plus de 2 heures, ou une nécrose des extrémités peut se produire, pour cette occasion doit être remise au centre médical le plus proche.

Chocs solaire et thermique.

Signes: Le premier, maux de tête, faiblesse, flux sévère de sang à la tête, acouphènes, nausées, vertiges, soif, cyanose de la face, de l'essoufflement, un rythme cardiaque de 120 ... 140 battements par minute, la température du corps monte à 40 ° C. La peau des touchés chaud et rincé, ses pupilles dilatées. La victime ¬ Sheha apparaissent des convulsions, des hallucinations, des délires. Condition rapidement détérioré et il peut mourir en quelques heures du Pas ¬ ralicha respiratoire et un arrêt cardiaque.

Premiers secours: déplacer la victime dans un endroit frais et à l'ombre, enlever ses vêtements et se coucha quelques leva la tête pour tête et du cœur appliquer des compresses froides ou de la douche à l'eau froide. Si la conscience est perdue, il faut boire abondamment des boissons froides. Pour l'excitation de la victime pour donner renifler un coton imbibé avec de l'ammoniaque. En cas de violation de la respiration ou une insuffisance cardiaque - procéder immédiatement à la respiration artificielle et le massage cardiaque.

3.6 Electrocution

Changements dans les tissus locaux dans un accident électrique sont les brûlures thermiques de gravité variable. Modifications courantes sont principalement développées à la suite de dommages au système nerveux. Ces changements dans le système nerveux et l'op ¬ image extraite de la lésion et de sa gravité.

Des lésions bénignes caractérisées accablé, la fatigue, la peur, et parfois des évanouissements.

Gravité moyenne des lésions caractérise par une perte de conscience de durée variable, pâleur ou cyanose de la peau, des convulsions, dépression respiratoire et la perturbation du cœur. Apprendre à respirer, superficielle, un pouls faible et rapide. Souvent, la paralysie des membres.

Dans les lésions graves - choc, souvent un état de mort clinique. Effet traumatique totale (choc électrique) survient lorsque le flux de quantités nocives de courant à travers le corps humain et se caractérise par l'excitation des tissus vivants du corps, contraction involontaire des différents muscles du corps, le cœur, les poumons et d'autres organes et systèmes, il ya donc une violation de leur travail ou un arrêt complet.

Avec la défaite de choc électrique est nécessaire tout d'abord de le libérer de l'action d'un courant électrique. Ceci peut être réalisé ou l'autre branche de la victime des parties sous tension, ou hors tension. La séparation d'avec les pièces sous tension est effectuée en utilisant des bâtons secs, les conseils, la coupe bêches, etc La victime peut être retardée pour des vêtements secs. S'il est difficile de verser ¬ séparée des parties actives par la victime, il faut couper le fil avec un manche de hache sec ou un objet avec une poignée isolante. Avec ses mains nues ne peut pas toucher la victime.

La principale condition pour le succès de la première aide - une action rapide, puisque après 5 min après la paralysie du cœur de l'homme ne peut être sauvé. Si la victime est à une hauteur, avant de débrancher la chute de tension devrait être de protéger la victime.

Après l'élimination de l'action en cours devrait être de déterminer l'état de la victime. Si la victime est consciente, il est nécessaire de fixer ou de s'asseoir dans une position confortable, et avant l'arrivée d'un médecin de fournir un repos complet, regarder certainement le souffle et le pouls.

Si la victime est inconsciente mais respire normalement et son pouls palpable, il devrait être facile à poser, ouvrir col et la ceinture, mettre le nez de laine de coton imbibé d'ammoniaque, saupoudrer avec de l'eau et assurer un repos complet.

Arrêt respiratoire et l'activité cardiaque - la pire du courant électrique. S'il n'y a pas de respiration, mais le patient a impulsion détectable, vous avez besoin pour commencer la respiration artificielle. S'il n'ya pas de battement de coeur, puis, avec la respiration artificielle devrait être externe (indirect) massage cardiaque.

Lorsque la victime se réveille, et quand il est temps de lumière ¬ zheniyah, il doit donner analgine ou aminopyrine, de boire beaucoup de liquide pour mettre un pansement sur la zone brûlée et a été transporté à l'hôpital.

3.7 Brûlures

Premiers secours: faire la victime hors de portée de la chaleur. Enflammer les vêtements sur le corps ou substance brûler rapidement éteint, pour arrêter l'accès de l'air à la zone de combustion (près avec un tissu épais, recouvert de terre, sable), qui couve vêtements remplis d'eau. Sur le touché avec des brûlures étendues du vêtement doit être coupé et laissé en place. Cloques et arracher des morceaux de vêtements collés à la brûlure ne peuvent pas l'être! Il a brûlé des zones à ne pas toucher les mains. Endroits brûlés en ¬ couvrent gaze propre ou mis à sec bandage de gaze de coton. En brûlures vaste victime enveloppé dans un drap propre. Les dommages peuvent être désinfectés par l'hydratation de leur eau de cologne.

La victime est d'envelopper dans une couverture, boire beaucoup de liquides, donner ou Analgin amidopirin et immédiatement transporté à l'hôpital.

Brûlures proviennent d'une exposition à la peau une température élevée (thermique), et également contre les effets des acides et alcalis (chi ¬ skie) contre courant électrique (puissance).

Sur la gravité existe quatre degrés de brûlures:

I. rougeur et gonflement de la peau;
II. bulles remplies de plasma sanguin;
III. cordes, une nécrose des tissus;
IV. carbonisation du tissu.

Quand je degré des brûlures brûlé zone de peau lavé avec de l'alcool, eau de Cologne, vodka, ou une solution faible de potassium manganèse acide.

Pour les brûlures II et III degrés sur la zone affectée de la peau après avoir fait sauter ¬ appliquer un pansement stérile. Vous ne pouvez pas ouvrir les bulles formées et séparées adhérant morceaux de vêtements. Une attention particulière est

nécessaire lorsque les vêtements brûlés libérant les parties du corps. Il est recommandé dans ce cas, enlever les vêtements et les chaussures afin de ne pas déchirer la peau et ne pas contaminer la plaie.

Avec des brûlures oculaires causées par une exposition à un arc électrique, appliquer des lotions solution d'acide borique ggogo de 2%.

La peau, l'acide calcinée ou alcalin lavé à l'eau courante froide pendant 12 . 20 min. Ensuite, appliquez un cataplasme de soude pour l'acide brûlures et brûlures caustiques - d'une faible solution de vinaigre ou de l'acide borique (1 cuillère à café pour 1 tasse).

3.8 Empoisonnement par des produits chimiques

Lorsque l'intoxication apparaissent des maux de tête, étourdissements, nausées, essoufflement, dans les cas graves - des convulsions et perte de conscience. Si des signes d'intoxication à la victime doivent être portées à l'air frais, mettre une compresse froide sur la tête et donner l'ammoniac de l'odorat. Lorsque les vomissures de la victime doit être mis sur le côté. Si elle est inconsciente, appeler un médecin immédiatement, et avant qu'il est venu faire la respiration artificielle.

Premiers secours pour l'empoisonnement chimique est réduite principalement par le fait que, jusqu'à l'arrivée du médecin, ou jusqu'à la livraison de la victime dans l'agence de gauche chebnoe pour retirer le poison de l'organisme ou de le neutraliser. Si le poison est entré dans le corps à travers le tractus gastro-intestinal, il est nécessaire de donner à la victime quelques verres d'eau tiède ou une solution faible de potassium de l'acide, du manganèse, et puis vomir. Vomissements provoquent une irritation de la paroi postérieure du pharynx ou avec une solution de sel de cuisine (2 cuillères à soupe par tasse teployvody). Après des vomissements pour la liaison à la victime devrait être accordée poison à boire un verre d'eau avec deux à trois cuillères à soupe de charbon actif ¬ tré, puis laxatif salin.

Solution de lavage gastrique cas d'intoxication par les sels et les acides de métaux lourds est recommandé d'oxyde de magnésium (20 ... 30 g pour 1 litre d'eau). L'oxyde de magnésium forme des composés insolubles de métaux lourds et neutralise l'acide.

Si la respiration s'est arrêtée en raison de la toxicité (par exemple, la vapeur d'éther, de l'ammoniac) pour transporter la victime à l'air frais et pratiquer la respiration artificielle.

L'intoxication peut acides et alcalis. Ainsi, l'acide et à l'alcali, corrodant la muqueuse de la bouche, de l'œsophage et de l'estomac, peut provoquer leur rupture.

Lorsque la victime d'un empoisonnement acide donner à boire une solution de bicarbonate de soude (1-2 cuillères à soupe par tasse d'eau), le lait, l'eau. En cas d'intoxication alcali affecté arrosé avec de l'eau et de l'acide acétique, le jus de citron, le lait. Si vous soupçonnez une perforation (douleur dans la poitrine et l'estomac) ne donne pas la victime à boire, et il était urgent transporté à l'hôpital.

L'empoisonnement peut également de l'alcool, de l'alcool méthylique et de substituts d'alcool. Premiers secours à la victime dans cette affaire - laver le ventre, lui donnant à boire 2-3 verres d'eau tiède, puis, en appuyant sur la racine de la langue, faire vomir.

Avec l'affaiblissement de la respiration ou de l'arrêter - immédiatement de ¬ lat respiration artificielle.

Dans tous les cas de suspicion de substitution d'empoisonnement à l'alcool, liquides techniques, des parfums et des produits cosmétiques touchées ont besoin d'une livraison à l'hôpital.

En cas de contact poison de la formulation de la peau doit être soigneusement laver au jet d'eau, de préférence avec du savon ou sans bavures ou frotter la peau, de l'enlever avec un morceau de gaze (tissus, coton), puis laver à l'eau froide ou une solution faiblement alcalin (1 cuillère à café potable soude dans un verre d'eau). Si le poison pénètre dans les yeux doit être rincé avec de l'eau ou une solution à 2% de bicarbonate de soude.

Pour protéger vos mains contre les produits chimiques utilisés en caoutchouc, et dans certains cas, de la laine ou des gants synthétiques, et pâte spéciale (pommades).

Galvanotipisty, photographes, photocopieurs, imprimantes, travilschiki, les accepteurs sur les presses offset et d'autres travailleurs qui entrent en contact avec des solutions chimiques doivent travailler dans de l'acide et des gants de caoutchouc sans soudure résistant aux alcalis ou des gants de coton acide de protection avec un revêtement spécial. Pour maintenir les propriétés protectrices de gants et mitaines ne pas les frapper sur les mains contaminées, empêcher la pénétration de l'huile, acide, etc

Dans les ateliers, qui utilise de grandes quantités d'acides et aux alcalis (placage, gravure département) doivent porter des bottes en caoutchouc.

La protection respiratoire contre les gaz dangereux, des vapeurs et de la poussière, à l'aide de dispositifs de filtrage et d'isoler spéciales.

Dispositifs de filtrage sont divisés en masques à gaz, pré-affecté à la protection contre les gaz et vapeurs toxiques et respiratoire ¬ Torah pour protéger le système respiratoire de la poussière et de la fumée.

Respirateurs peuvent être avec ou sans Vannes. Les vannes sont utilisées pour la séparation de l'air inspiré et expiré. Les respirateurs sont conçus pour protéger non seulement le système respiratoire, mais aussi la tête, le cou, le visage de substances irritant pour la peau sont de la forme ¬ kapyu Shona ou un casque, qui est attaché aux filtres de compagnon différent ¬ riaux, feutre, laine, carton spécial, papier, etc .

Visage, le cou et les mains lorsque vous travaillez avec des substances corrosives protéger les onguents spéciaux, des pâtes, qui sont appliqués sur la peau avant de commencer, puis rincez. Les pâtes et pommades sont divisés en hydrophile et hydrophobe. Hydrophile - se dissolvent facilement dans l'eau. Ils protègent la peau contre les graisses, huiles, produits pétroliers.

CONCLUSION

Après avoir examiné les problèmes décrits, on peut conclure que les firewalls protéger les réseaux informatiques de l'organisation de toute intervention non autorisée. Les Firewalls sont un moyen nécessaire pour assurer la sécurité de l'information. Ils constituent la première ligne de défense. Lors de la sélection et l'achat de Firewalls doit être réfléchir sur et à analyser. Sélectionnez l'architecture et les composants du Firewalls souhaité. Bien configurer le logiciel et tester la configuration du Firewalls.

Au cours de l'analyse, il a été constaté que le Firewalls réseau Engines NS6200 est plus sûr, plus facile à utiliser, et est disponible pour les petites entreprises avec des exigences de sécurité élevées.

Pour les grandes entreprises souhaitables l'achat Firewalls RimApp F302PLUS de barrage, car il est sûr, facile à utiliser et accessible pour les grandes entreprises avec des exigences de sécurité élevées.

LISTE DES SOURCES UTILISEES

1. "Постановление Президента Республики Узбекистан от 23.10. 2012 № ПП-1836"
2. "Постановление Президента Республики Узбекистан №13 (513) от 02.04.2012 О мерах по дальнейшему внедрению и развитию современных информационно - коммуникационных технологий"
3. "Приложение 2 к Постановлению Президента Республики Узбекистан №167 от 05.09.2005"
4. OU Laponina. Firewall. "INTUIT", Moscou, 2009;
5. TV Ogltri. Les Firewalls. Utilisation pratique des firewalls. "DMK", Moscou, 2008;
6. David Chapman, Andy Fox. Les Firewalls Cisco Secure PIX. "Williams", Moscou, 2009;
7. TA Biyachuev. La sécurité des réseaux d'entreprise. Spb 2008.;
8. AY Chardonnerets. Protection des réseaux informatiques contre les accès non autorisés. "S & T", Saint-Pétersbourg, 2009.;
9. R. Ziegler. Firewalls sous Linux. "Williams", Moscou, 2009;
10. Magazine «Chip», Juillet 2007;
11. "Les problèmes de sécurité de l'information», Journal, Avril 2008;
12. Yakovlev. Conférence «Firewalls» pour 2009;
13. http://cisco.com
14. http://zonealarm.com
15. http://hub.ru
16. http://opennet.ru
17. http://infosecurity.ru
18. http://www.security-teams.net
19. http://www.oszone.ru