1ST REVIEW

FIRE WALL IS SECURITY GUARD WHICH IS LOCATED AT THE ENTRY POINT BETWEEN PRIVATE NETWORK AND THE OUTSIDE INTERNET.FIREWALL IS USED TO EXAMINE THE INCOMING AND THE OUTGOING PACKETS.WHETHER IT CAN BE ACCEPTED OR DISCARD.PACKETS SUCH AS IP ADDRESS, TUPLE, PORT NUMBER ETC.

TO ACHIEVE CONSISTENCY, COMPLETENESS, AND COMPACTNESS, WE PROPOSE A NEW METHOD CALLED STRUCTURED FIREWALL DESIGN, WHICH CONSISTS OF TWO STEPS.

FDD REDUCTION :- IT HELP TO REDUCE THE NUMBER OF RULES FORM AN GENERATED FDD.

FDD MARKING :- MOST FIREWALLS REQUIRE SIMPLE RULES, TO MINIMIZE THE NUMBER OF SIMPLE RULES GENERATED FROM AN FDD. THE NUMBER OF SIMPLE RULES GENERATED FROM A ‘‘MARKED VERSION’’ OF AN FDD IS LESS THAN OR EQUAL TO THE NUMBER OF SIMPLE RULES GENERATED FROM THE ORIGINAL FDD.

FIREWALL COMPACTION:- REMOVING REDUNTANT RULES FROM A FIREWALL AND PRODUCES AND EQUIVALENT FIREWALL WITHING A FEWER RULES.

FIREWALL GENRATION:- FROM SEQUENECE OF RULES MARKED FDD IS CREATED.

2ND REVIVE
NETWORK CONNECTIVITY CAN USE TO SHARE FILES, EXCHANGE E-MAIL AND POOL PHYSICAL RESOURCES.IT CAN BE BOTH CURSE AND BLESSINGS.
BENEFITS OF THE FIRE WALL: -
• INCREASED ABILITY TO ENFORCE NETWORK STANDARDS AND POLICIES.
• CENTRALIZED INTERNETWORK AUDIT CAPABILITY.
LINITATIONS OF FIREWALL: -
• FIREWALLS DO NOT PROTECT TRAFFIFIC THAT IS NOT SENT THROUGH IT.
• FIREWALLS PROVIDE NO DATA INTEGRITY.
• FIREWALLS MAY NOT PROTECT ANYTHING IF THEY HAVE BEEN COMPROMISED.
• FIREWALLS CANNOT AUTHENTICATE DATAGRAMS AT THE TRANSPORT OR NETWORK LAYERS.
• FIREWALLS PROVIDE LIMITED CONFIFIDENTIALITY.

EVALUATION OF FIREWALL: -

• PERFORMANCE: - FIREWALL IMPACT THE PERFORMANCE BETWEEN LOCAL AND REMOTE NETWORK.
REQUIRMENTS SUPPORT: - A FIREWALL SUPPORTED ALL THE APPLICATION ACROSS THE TWO NETWORKS.
• ACCESS CONTROL: - ACESS CONTROL OF FIREWALL IS BASED ON IP ADDRESSES.
• AUTHENTICATION: - FIREWALL MUST SUPPORT THE AUTHENTICATION.
• AUDITING
• TRANSPARENCY.

3RD REVIVE

A FIREWALL IS SOFTWARE AND HARDWARE BASED NETWORK SECURITY SYSTEM.IT CONTROLS THE OUTGOING AND THE INCOMING OF THE DATA PACKETS WHETHER THEY SHOULD ALLOWED OR NOT.
TYPES OF FIREWALL: -
NETWORK LAYER FIREWALL: - NETWORK LAYER FIREWALLS ALSO CALLED PACKET FILTER. IN THAT FIREWALL LOW LEVEL OF TCP/IP PROTOCOL IS NOT ALLOW UNLESS THEY CANNOT MATCH RULES OF THE SET.IT REQIRE LESS MEMORY AND HAVE HAVE PROCESSING SPEED.
APPLICATION LAYER FAREWALL: - THE FIREWALL WHICH IS BASED ON THE APPLICATION LEVEL OF TCP/IP IS KNOWN AS AHE APPLICATION LAYER FIREWALL. IT USUALLY FILLTERS THE PACKETS AND ALLOWS THE MUCH GRANULAR ONE TO ENTER AND EXIT.
PROXY LAYER FIREWALL: - IT MOST SEURE TYPE OF THE FIREWALL .IT HAS THE MORE SPEED COMPARE TO THE NETWORK AND APPLICATION LEVEL FIREWALL. PACKETS DON'T PASS THROUGH A PROXY. INSTEAD THE PROXY ACTS AS AN INTERMEDIARY - COMPUTERS MAKE A CONNECTION TO THE PROXY WHICH THEN INITIATES A NEW NETWORK CONNECTION BASED ON THE REQUEST; EFFECTIVELY A MIRROR OF THE INFORMATION TRANSFER.

4TH REVIEW

FIREWALL IS A SECURITY DEFENCE TOOL IN THE FIELD OF THE COMPUTER NETWORK SECURITY. ITS IS USED BETWEEN THE INCOMING AND OUTGOING OF THE PACKETS.FIREWALL CONSIST OF THE HARDWARE AND THE SOFTWARE. THE INFORMATION FLOW THOROUGH THE FIRE WALL HENCE THE ACTIVITES LIKE PERMISSION, REJECTION, MONITORING CARRIED OUT BY FIREWALL.
FIREWALL WORKS ON PRE-DEFINED CONFIGURATION AND THE RULES. IT ALLOWS THE PACKTES BY LOOKING THE RULES THAT DEFINE.
GOOD FIRE WALL HAS TWO ATTRIBUTES: -

- ONE IS THAT ALL INFORMATION MUST PASS THROUGH THE FIREWALL.
- SECURITY POLICY OF THE PROTECTED NETWORK IS IT ALLOWED TO PASS THROUGH THE FIREWALL.
- RECORD THE INFORMATION CONTENT AND ACTIVITIES THROUGH THE FIREWALL.
- FOURTH IS TO DETECT AND ALARM NETWORK ATTACKS.

FIREWALL IS THE PACKET FILTERING TECHNOLOGY WHETER IT STATIC OR DYNAMIC.DATA PASS THROUGH THE PACKET FIREWALL PASS THROUGH EACH PACKET AND IT ALLOWS THE PACKET TO ENTER IF THE PACKET FULFILL THE RULES AND CONFIGURATION.

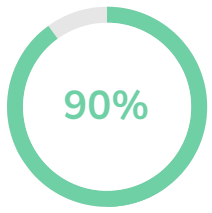
5TH REVIEW

CLOUD IS BECOMING A DOMINANT COMPUTING PLATFORM. CLOUD IS USUALLY HOSTS MANY DIFFERENT PLATFORMS. IN THAT RESEARCH PAPER THEY INTRODUCED ABOUT THE CLOUD COMPUTING FIREWALLS E.G. CLOUD DATA CENTRE.
THE LARGE NUMBER OF SERVICES SUCH AS E-BUSINESS, SOCIAL NETWORKS ETC GOES UNDER THE NUMEROUS TYPES OF MALICIOUS ATTACK, DDoS ETC TO PROTECT THE HOST SERVICE THE CLOUD COMPUTING FIREWALL IS USED.ITS IS THE FAFTEST GROWING SECTOR IN IT INDUSTRY.
FRAMEWORK OF CLOUD FIREWALL, AND ESTABLISH A MATHEMATICAL MODEL FOR THE DETECTION CHAIN MECHANISM, AND FURTHER EXTRACT A NUMBER OF PERFORMANCE METRICS.

# Plagiarism Scan Report

Report Generated on: Jan 04,2023


Plagiarised




Unique

| | |
|---|---|
| Total Words: | **728** |
| Total Characters: | **4602** |
| Plagiarized Sentences: | **3.9** |
| Unique Sentences: | **35.1 (90%)** |

## Content Checked for Plagiarism

FIRE WALL IS SECURITY GUARD WHICH IS LOCATED AT THE ENTRY POINT BETWEEN PRIVATE NETWORK AND THE OUTSIDE INTERNET.FIREWALL IS USED TO EXAMINE THE INCOMING AND THE OUTGOING PACKETS.WHETHER IT CAN BE ACCEPTED OR DISCARD.PACKETS SUCH AS IP ADDRESS, TUPLE, PORT NUMBER ETC.

TO ACHIEVE CONSISTENCY, COMPLETENESS, AND COMPACTNESS, WE PROPOSE A NEW METHOD CALLED STRUCTURED FIREWALL DESIGN, WHICH CONSISTS OF TWO STEPS. FIRST, ONE DESIGNS A FIREWALL USING A FIREWALL DECISION DIAGRAM (FDD).

FDD REDUCTION :- IT HELP TO REDUCE THE NUMBER OF RULES FORM AN GENERATED FDD.

FDD MARKING :- MOST FIREWALLS REQUIRE SIMPLE RULES, TO MINIMIZE THE NUMBER OF SIMPLE RULES GENERATED FROM AN FDD. THE NUMBER OF SIMPLE RULES GENERATED FROM A ‘‘MARKED VERSION’’ OF AN FDD IS LESS THAN OR EQUAL TO THE NUMBER OF SIMPLE RULES GENERATED FROM THE ORIGINAL FDD.

FIREWALL COMPACTION:- REMOVING REDUNTANT RULES FROM A FIREWALL AND PRODUCES AND EQUIVALENT FIREWALL WITHING A FEWER RULES.

FIREWALL GENRATION:- FROM SEQUENECE OF RULES MARKED FDD IS CREATED.

2ND REVIVE

NETWORK CONNECTIVITY CAN USE TO SHARE FILES, EXCHANGE E-MAIL AND POOL PHYSICAL RESOURCES.IT CAN BE BOTH CURSE AND BLESSINGS.

BENEFITS OF THE FIRE WALL: -

- INCREASED ABILITY TO ENFORCE NETWORK STANDARDS AND POLICIES.
- CENTRALIZED INTERNETWORK AUDIT CAPABILITY.

LINITATIONS OF FIREWALL: -

- FIREWALLS DO NOT PROTECT TRAFFIFIC THAT IS NOT SENT THROUGH IT.
- FIREWALLS PROVIDE NO DATA INTEGRITY.
- FIREWALLS MAY NOT PROTECT ANYTHING IF THEY HAVE BEEN COMPROMISED.
- FIREWALLS CANNOT AUTHENTICATE DATAGRAMS AT THE TRANSPORT OR NETWORK LAYERS.
- FIREWALLS PROVIDE LIMITED CONFIFIDENTIALITY.

EVALUATION OF FIREWALL: -

- PERFORMANCE: - FIREWALL IMPACT THE PERFORMANCE BETWEEN LOCAL AND REMOTE NETWORK.

REQUIRMENTS SUPPORT: - A FIREWALL SUPPORTED ALL THE APPLICATION ACROSS THE TWO NETWORKS.

- ACCESS CONTROL: - ACESS CONTROL OF FIREWALL IS BASED ON IP ADDRESSES.
- AUTHENTICATION: - FIREWALL MUST SUPPORT THE AUTHENTICATION.
- AUDITING
- TRANSPARENCY.

3RD REVIVE

A FIREWALL IS SOFTWARE AND HARDWARE BASED NETWORK SECURITY SYSTEM.IT CONTROLS THE OUTGOING AND THE INCOMING OF THE DATA PACKETS WHETHER THEY SHOULD ALLOWED OR NOT.
TYPES OF FIREWALL: -
NETWORK LAYER FIREWALL: - NETWORK LAYER FIREWALLS ALSO CALLED PACKET FILTER. IN THAT FIREWALL LOW LEVEL OF TCP/IP PROTOCOL IS NOT ALLOW UNLESS THEY CANNOT MATCH RULES OF THE SET.IT REQIRE LESS MEMORY AND HAVE HAVE PROCESSING SPEED.
APPLICATION LAYER FAREWALL: - THE FIREWALL WHICH IS BASED ON THE APPLICATION LEVEL OF TCP/IP IS KNOWN AS AHE APPLICATION LAYER FIREWALL. IT USUALLY FILLTERS THE PACKETS AND ALLOWS THE MUCH GRANULAR ONE TO ENTER AND EXIT.
PROXY LAYER FIREWALL: - IT MOST SEURE TYPE OF THE FIREWALL .IT HAS THE MORE SPEED COMPARE TO THE NETWORK AND APPLICATION LEVEL FIREWALL. PACKETS DON'T PASS THROUGH A PROXY. INSTEAD THE PROXY ACTS AS AN INTERMEDIARY - COMPUTERS MAKE A CONNECTION TO THE PROXY WHICH THEN INITIATES A NEW NETWORK CONNECTION BASED ON THE REQUEST; EFFECTIVELY A MIRROR OF THE INFORMATION TRANSFER.

4TH REVIEW

FIREWALL IS A SECURITY DEFENCE TOOL IN THE FIELD OF THE COMPUTER NETWORK SECURITY. ITS IS USED BETWEEN THE INCOMING AND OUTGOING OF THE PACKETS.FIREWALL CONSIST OF THE HARDWARE AND THE SOFTWARE. THE INFORMATION FLOW THOROUGH THE FIRE WALL HENCE THE ACTIVITES LIKE PERMISSION, REJECTION, MONITORING CARRIED OUT BY FIREWALL. FIREWALL WORKS ON PRE-DEFINED CONFIGURATION AND THE RULES. IT ALLOWS THE PACKTES BY LOOKING THE RULES THAT DEFINE.
GOOD FIRE WALL HAS TWO ATTRIBUTES: -
• ONE IS THAT ALL INFORMATION MUST PASS THROUGH THE FIREWALL.
• SECURITY POLICY OF THE PROTECTED NETWORK IS IT ALLOWED TO PASS THROUGH THE FIREWALL.
• RECORD THE INFORMATION CONTENT AND ACTIVITIES THROUGH THE FIREWALL.
• FOURTH IS TO DETECT AND ALARM NETWORK ATTACKS.
FIREWALL IS THE PACKET FILTERING TECHNOLOGY WHETER IT STATIC OR DYNAMIC.DATA PASS THROUGH THE PACKET FIREWALL PASS THROUGH EACH PACKET AND IT ALLOWS THE PACKET TO ENTER IF THE PACKET FULFILL THE RULES AND CONFIGURATION.

5TH REVIEW

CLOUD IS BECOMING A DOMINANT COMPUTING PLATFORM. CLOUD IS USUALLY HOSTS MANY DIFFERENT PLATFORMS. IN THAT RESEARCH PAPER THEY INTRODUCED ABOUT THE CLOUD COMPUTING FIREWALLS E.G. CLOUD DATA CENTRE.
THE LARGE NUMBER OF SERVICES SUCH AS E-BUSINESS, SOCIAL NETWORKS ETC GOES UNDER THE NUMEROUS TYPES OF MALICIOUS ATTACK, DDoS ETC TO PROTECT THE HOST SERVICE THE CLOUD COMPUTING FIREWALL IS USED.ITS IS THE FAFTEST GROWING SECTOR IN IT INDUSTRY. FRAMEWORK OF CLOUD FIREWALL, AND ESTABLISH A MATHEMATICAL MODEL FOR THE DETECTION CHAIN MECHANISM, AND FURTHER EXTRACT A NUMBER OF PERFORMANCE METRICS.

**Firewall Design Methods - Computer Science and Engineering**
FIRST, ONE DESIGNS A FIREWALL USING A FIREWALL DECISION DIAGRAM (FDD).
https://www.cse.msu.edu/Students/Current_Grad/LectureSeries/2005/liu.html

100%

**Local Area Network Handbook, Sixth Edition - Google Books Result**
• FIREWALLS DO NOT PROTECT TRAFFIFIC THAT IS NOT SENT THROUGH IT.
https://books.google.com/books?id=LWsHEAAAQBAJ

100%

**Research on Computer Network Security Based on Firewall ...**

• FOURTH IS TO DETECT AND ALARM NETWORK ATTACKS.

https://iopscience.iop.org/article/10.1088/1742-6596/1744/4/042037/pdf

100%

**Research on Computer Network Security Based on Firewall ...**

• RECORD THE INFORMATION CONTENT AND ACTIVITIES THROUGH THE FIREWALL.

https://www.researchgate.net/publication/349387266_Research_on_Computer_Network_Security_Based_on_Firewall_Technology

100%