NETWORK SECURITY PROBING FOR VPN

Major Project Submitted in partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering (Information and Network Security)

Submitted by

Priya Kodgyale(18MCEI03)

Guided By

Usha Patel

DEPARTMENT OF COMPUTER ENGINEERING
INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY
AHMEDABAD-382481

December 2019

Certificate

Certificate This is to certify that the major project entitled ” NETWORK SECURITY PROBING FOR VPN” submitted by Priya Kodgyale (18MCEI03), towards the partial fulfillment of the requirements for the award of degree of Master of Technology in Computer Science and Engineering (Information and Network Security) of Nirma University, Ahmedabad, is the record of work carried out by her under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project part-I, to the best of my knowledge, haven’t been submitted to any other university or institution for award of any degree or diploma.

Usha Patel
M.Tech - CSE (Information and Network Security)
CE Department Institute of Technology,
Nirma University, Ahmedabad.

Dr. Madhuri Bhavsar
Professor and Head,
CE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Rajesh N Patel
I/C Director,
Institute of Technology,
Nirma University, Ahmedabad

Statement of Originality

I, Priya Kodgyale 18MCEI03, give undertaking that the Major Project entitled ” NETWORK SECURITY PROBING FOR VPN” submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in Information and Network Security of Institute of Technology, Nirma University, Ahmedabad, contains no material that has been awarded for any degree or diploma in any university or school in any territory to the best of my knowledge. It is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. It contains no material that is previously published or written, except where reference has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Signature of Student

Date:16 May 2020

Place:

Endorsed by

Usha Patel

(Signature of Guide)

Acknowledgments

It gives me immense pleasure in expressing thanks and profound gratitude to Usha Patel, Assistant Professor, Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad for her valuable guidance and continual encouragement throughout this work. The appreciation and continual support she has imparted has been a great motivation to me in reaching a higher goal. Her guidance has triggered and nourished my intellectual maturity that I will benefit from, for a long time to come. It gives me an immense pleasure to thank Dr. Madhuri Bhavsar, Hon'ble Head of Computer Engineering Department, Institute of Technology, Nirma University, Ahmedabad for her kind support and providing basic infrastructure and healthy research environment. A special thank you is expressed wholeheartedly to Dr. Alka Mahajan, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation he has extended throughout course of this work. I would also thank the Institution, all faculty members of Computer Engineering Department, Nirma University, Ahmedabad for their special attention and suggestions towards the project work.

- Priya Kodgyale

18MCEI03

Abstract

Considering the consistent networks expansion in exponential manner, network security became key requirements of today's generation. Network Security probing for VPN (Virtual Private Network) provides proactive analysis of user VPN connectivity problems, which may cause in future. As most of the organization's employee needs to work outside the organizations network environment , user needs to be provided a secure tunnel from outside network to inside organization network. Due to any reason like certificate issue or improper software updating, user may lose the VPN connectivity or it may cause impact on organization as per critical role of user and may lead to big problem or loss. To avoid these kind of futures unconvinced problems, this solution providing a Dashboard with continuous logs monitoring and filtered information to reduce incidence handling efforts and less impact on future work due to VPN connectivity loss.

Abbreviations

CND	Cyber Network Defense
VPN	Virtual Private Network
SSL	Secured Socket Layer
DTLS	Datagram Transport Layer Security
TPM	Trusted Platform Module
DART	Diagnostic and Reporting Tool
LAN	Local Area Network
ISP	Internet Service Provider
SPI	Security Parameter Index

Contents

1. Introduction

1.1 General

As each association giving adaptability of work from remote place because of various time zone customers or any other(outsourcing) necessities VPN (virtual private network) with secure gateway tunnel is key requirement to provide remote access organizations resources, with consistency to not effect on work. It gives restricted access based on application, URL/IP address and employee role which provides primary level of security with two level authentication and authorization. Remote access can be provided with help of VPN application installed in system with trusted certificate, profile (user) using VPN connection.TPM(trusted platform module) based certificate to increase stability and security.

Definition: As the created world turns out to be progressively associated through digital channels, new vulnerabilities are revealed and misused at already inconspicuous rates. Day by day in every field network come in to picture, as networks grows more complications and vulnerabilities are increasing. To protect our network from security threads we need cyber network defense probing.

1.2 VPN Client Support

Level	Support
L1	Incident support with basic and some advance troubleshooting like, password reset, certificate installer or user account issue
L2	Advanced troubleshooting with application on bug, certificate life cycle management, security hardening.
Document	Performative data provided for some common problem like user profile mismatch.
Self	Password reset, application update.
External User	With limited access

Table 1.1: VPN client support at different level

VPN client application blocks connections to untrusted servers which are not listed in the application profile will be blocked with warning.

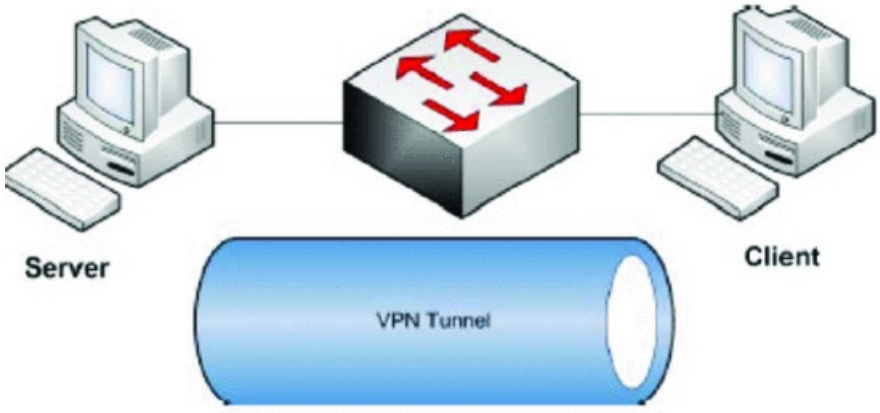

Figure 1.1: Basic VPN connectivity

[3]

Objectives:

- Automation of log collection

• Report generation to identify problem

• Alert generation for on time service

• Proactive Monitoring

Technical Requirements:

1. Splunk

2. XML

4. 4 GB RAM

1.3 Scope of work

Collecting DART(Diagnostic and Reporting tool)logs related to VPN application and analyzing the machine data logs to know user behavior or any issue regarding the VPN connection. Sorting data logs with index and forwarders to get proper information for easily understand the problem or future problem and for improve performance precautions can be done with updating software or password reset before expiring.

DART logs: It is a tool that you can use to gather information helpful for investigating VPN client establishment and association issues.

• DART supports Windows, MAC and Linux.

• DART is at present accessible as an independent establishment, or the director can drive this application to the customer PC as a component of the VPN client

dynamic framework.

Splunk: It is a product innovation which is utilized for observing, looking, dissecting and envisioning the machine created information continuously. It can screen and peruse diverse sort of log documents and stores information as occasions in indexers. This device enables you to picture information in different types of dashboards.

• Quicken Development and Testing

• Enables you to construct Real-time Data Applications

• Create ROI quicker

• Deft measurements and detailing with Real-time design

• Offers search, investigation and perception abilities to engage clients of numerous types

2. Literature Survey

2.1 General VPN requirement and working

VPN is one of best source of cyber network defense which gives proactive role for security in networks. It provides two level security one is SSL(Secured Socket Layer) and another DTLS(Datagram transport Layer Security). Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment, which enforce password complexity, in part, controls what users can and cannot do on a computer system. For example: To enforce a password complexity policy that prevents users from choosing an overly simple password, To allow or prevent unidentified users from remote computers to connect to a network share, To block access to the Windows Task Manager or to restrict access to certain folders.

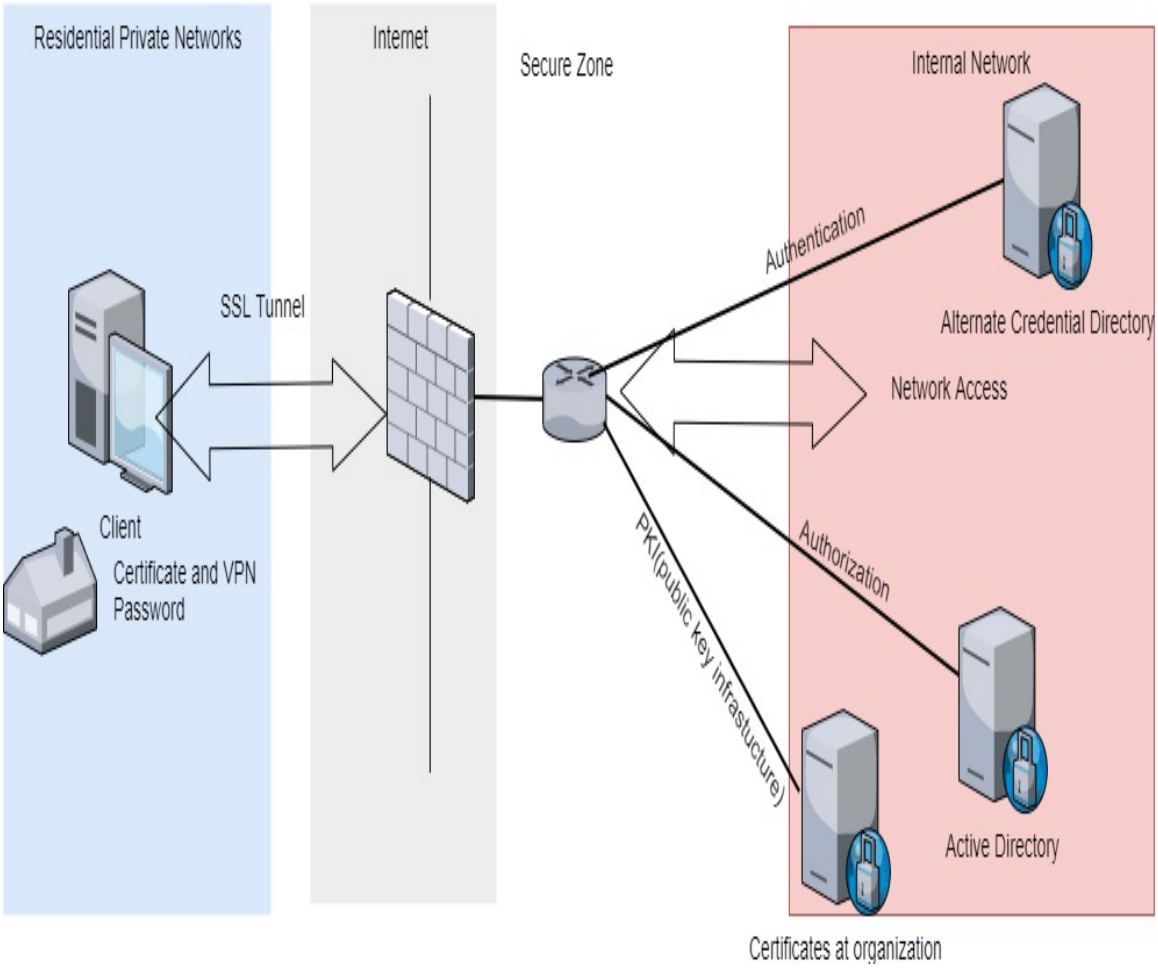

Figure 2.1: Working Flow of VPN

- SSL(Secured Socket Layer):

A SSL VPN association utilizes start to finish encryption (E2EE) to ensure information transmitted between the endpoint gadget customer programming and the SSL VPN server through which the customer interfaces safely to the web. Undertakings use SSL VPNs to empower remote clients to safely get to authoritative assets, just as to verify the web sessions of clients who are getting to the web from

outside the venture. A SSL burrow VPN empowers clients to safely get to various system administrations by means of standard internet browsers, just as different conventions and applications that are not online. The VPN burrow is a circuit built up between the remote client and the VPN server; the server can associate with at least one remote sites.

• DTLS(Datagram transport Layer Security):

TLS and SSL are the standard conventions utilized for verifying stream-based TCP Internet traffic. DTLS is a convention dependent on TLS that is fit for verifying the datagram transport. DTLS is appropriate for verifying applications and administrations that are delay-touchy (and henceforth use datagram transport), burrowing applications, for example: VPNs and applications that will in general come up short on document descriptors or attachment cradles. DTLS strengthen VPN that gives security to remote associations and quickens execution for different applications and administrations. Joining secure access control and streamlining for numerous conventions and application types onto a solitary stage limits chance and merges foundation while guaranteeing Quality of Service.

2.2 Requirement of Dashboard

As every day security vulnerabilities increasing it is must to focus on prevention with handling incidents, which can be done with collection of logs and other VPN related data in advance to analyze and provide solution before incident happens.

Collection of large amounts of data and raw data analyzing is biggest and complicated task which can be easily done with sorted and labeled data with splunk dashboard.

• Previous Incident handling

Separate team for collecting logs and basic level of analysis to identify the problem with help of documentation and gathering other relevant data from user.

•Improvements required

-Automate system to gather data and logs: to save time and man power.

-Proactive mechanism: To improve performance.

-Automation in finding solutions: To reduce redundant work for similar problems with highlighted tabs.

-Monitoring new problems, Deep analysis: To ease in understanding logs via segregation in logs, if unknown problem comes.

-Error tracking: To track errors and Finding root cause with monitoring tabs and small log file.

3. Implementation

3.1 Existing System

A separate team to handle large number of VPN client issue requires lots of time. collection of DART logs to be done with every client thus analyzing and resolving problem manually leads to redundant work for similar problems. Engineer can not see broader view of incidents so, increased time with different levels of working.

3.2 Proposed system

All clients data together will give broader view to look at problem and become easy to handle similar problems in proper manner. Saves time and efforts with minimum interaction with user gives more customer satisfaction due to handling incident in small time duration.

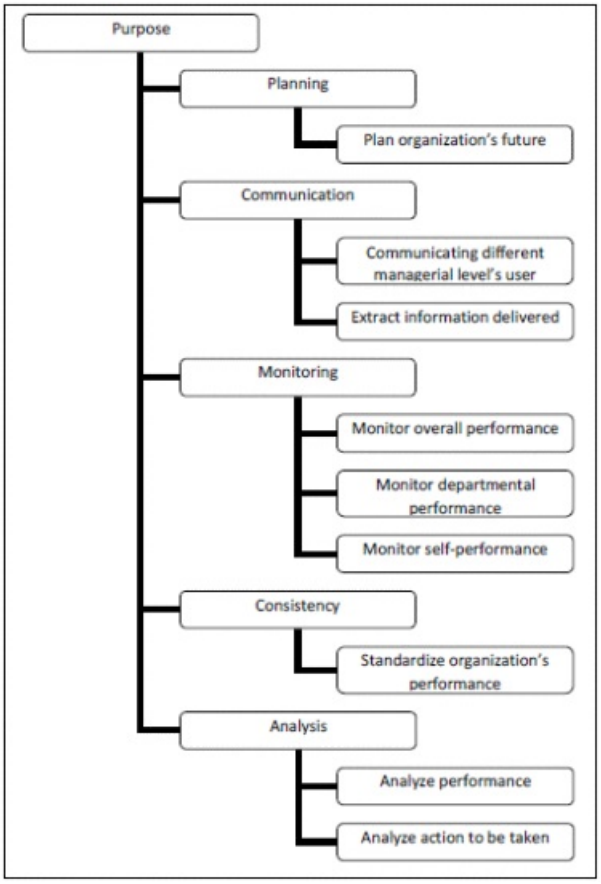

Figure 3.1: Purpose of Dashboard[11]

3.3 Dashboard

Platform to represent data in graphical and sorted manner. Mainly two dashboards

1. General Dashboard: Provides counts of different users having issues or fine to identify impact on number of users.

2.Troubleshooting Dashboard: Provides analyzing and troubleshooting problem facility.

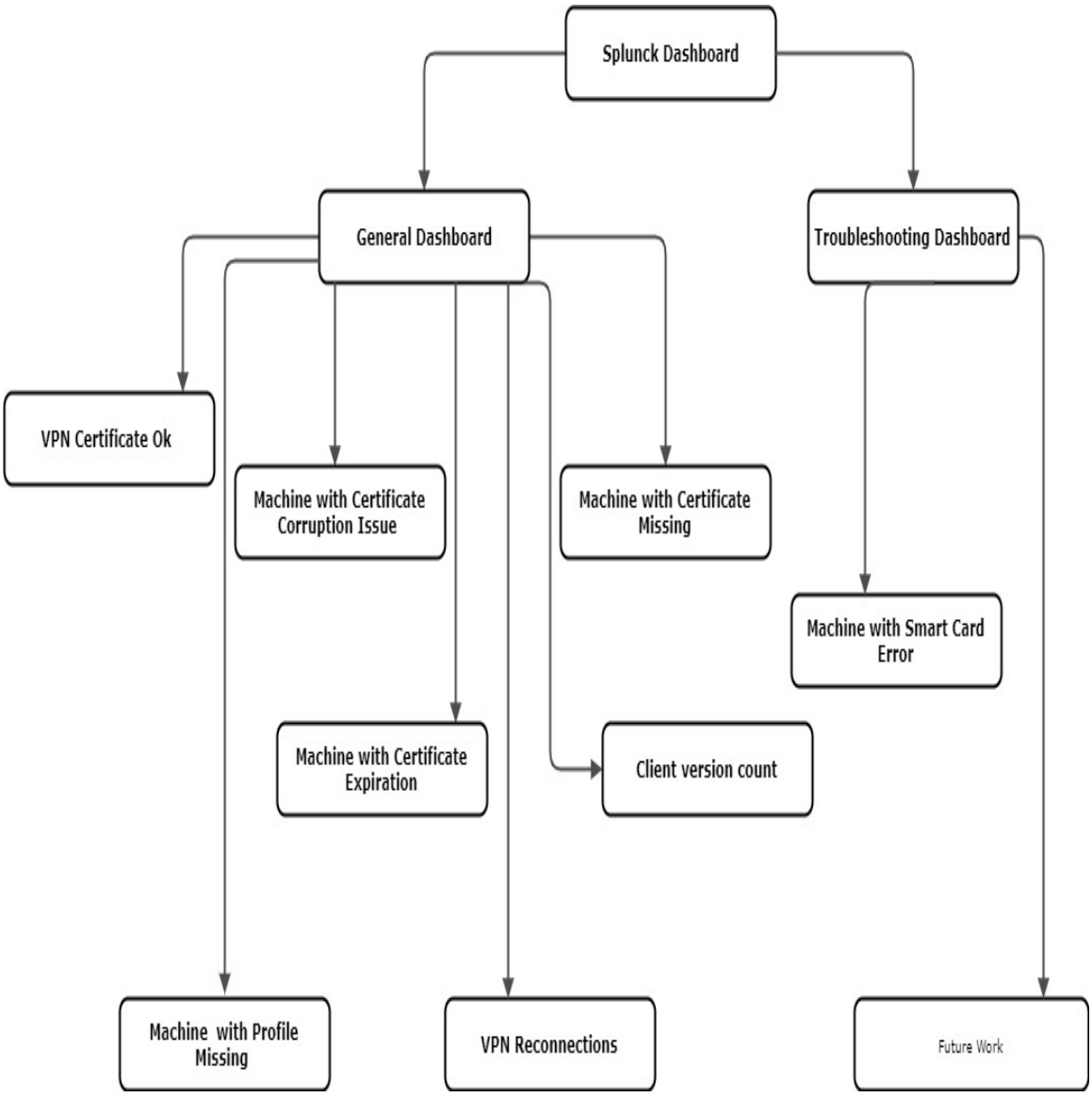

Figure 3.2: Architecture of Dashboard

1. VPN Certificate OK: A computerized declaration is an electronic archive and is given by a trustworthy Certification Authority (CA), who oversees such endorsements. VeriSign is a case of a Certification Authority. In the event that two

friends acknowledge each other's advanced authentications, they trust every others character, however they believe that the contrary companion is who they state they are.

• At the point when a CA gives an authentication to a VPN gadget then it is ensuring the VPN gadget is who it professes to be, and it does this by marking the testament it distribute and gives to the VPN gadget.
• Installs in system with application and user details from machine.
• Used for verifying user while connecting to VPN gateway tunnel.
• This tab gives count of users having correct certificate which matches user profile, not expired or not damaged.

2. Machine with Profile Missing: Users system may contain many certificates from that VPN client certificate should be picked is informed by users profile, which contains users details and VPN gateway details.

3. SSL loopback error: After SSL connection routing is failed due loop back IP (127.0.0.0) address and it wont go the actual gateway address and gives error.
• This tab gives the count of machines which have loop-back address.

4. Machine with Certificate corruption issue: certificate may be corrupted or tampered by virus or improper installation, which may cause problem while connecting VPN.

• Authentication fails due to wrong (misplaced) information from certificate.

5. Machine with Certificate Expiration: Every certificate is provided by some trusted Certification Authority (CA) with limited access duration after that Certificate is not valid as it is expired.

• Even after renewing alert messages few users don't renew it and certificate expires.

6. Machine with Certificate missing: Due to any reason certificate of VPN may be deleted or misplaced from user's system and without certificate user can't login to VPN connection.

• This tab gives information about these users having certificate missing.

7. VPN Reconnection: There are different reasons, which may lead to VPN disconnection. In some cases switch firewalls cause the detachment issues since Wi-Fi switches typically pound the VPN to a stop following a couple of moments of utilization, doubtlessly on the grounds that they can't stay aware of SPI(Security Parameter Index)/Firewall turned on or it may happen due to some reasons like software driver crash.

• Having this problem users details and count is specified by this tab of dashboard.

8. Client version count: few users having outdated software(VPN client) version installed in there systems.

• Miss of latest version push in their system due to ignorance of inactive system.

• User might not be aware of advantage of latest version.

• There are too many older versions.

• User should be on minimum required version to work VPN fine.

• There are still users who works on older version of VPN client software.

• It gives count of different users with different versions.

• Which helps to get performance improvement by updating users to latest or minimum required version.

9. Machine with login issue: Automated tool which try to fix the certificate related issue and resolve it without knowing to user like certificate missing, corrupted or expired.

• If it is beyond scope of the tool it gives login error or issue.

• Which helps resolver about basic test and gives user details with login issue.

10. Graveyard Machines: User systems having old (less than specified) or lesser version counted as graveyard machines.

• Gives count of all older version (< 4.33xxx), which may cause issue due to bugs in older version.

• Saves to cause security issue and connectivity issues with user details.

3.4 Design Flow

It gives designing flow of VPN client Dashboard to Cyber Network Defense probing for VPN.

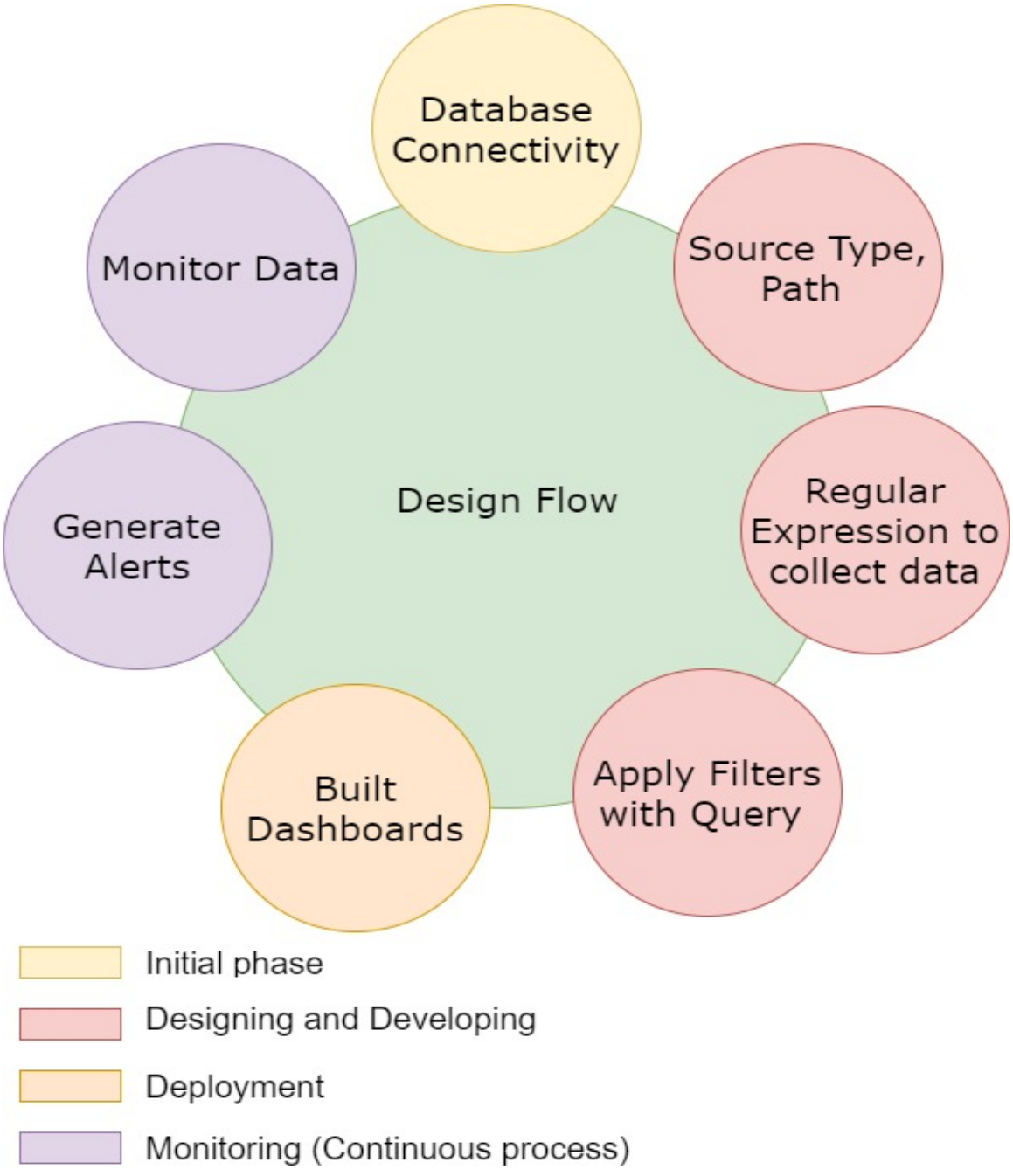

Figure 3.3: Design flow of Dashboard

Outcomes:

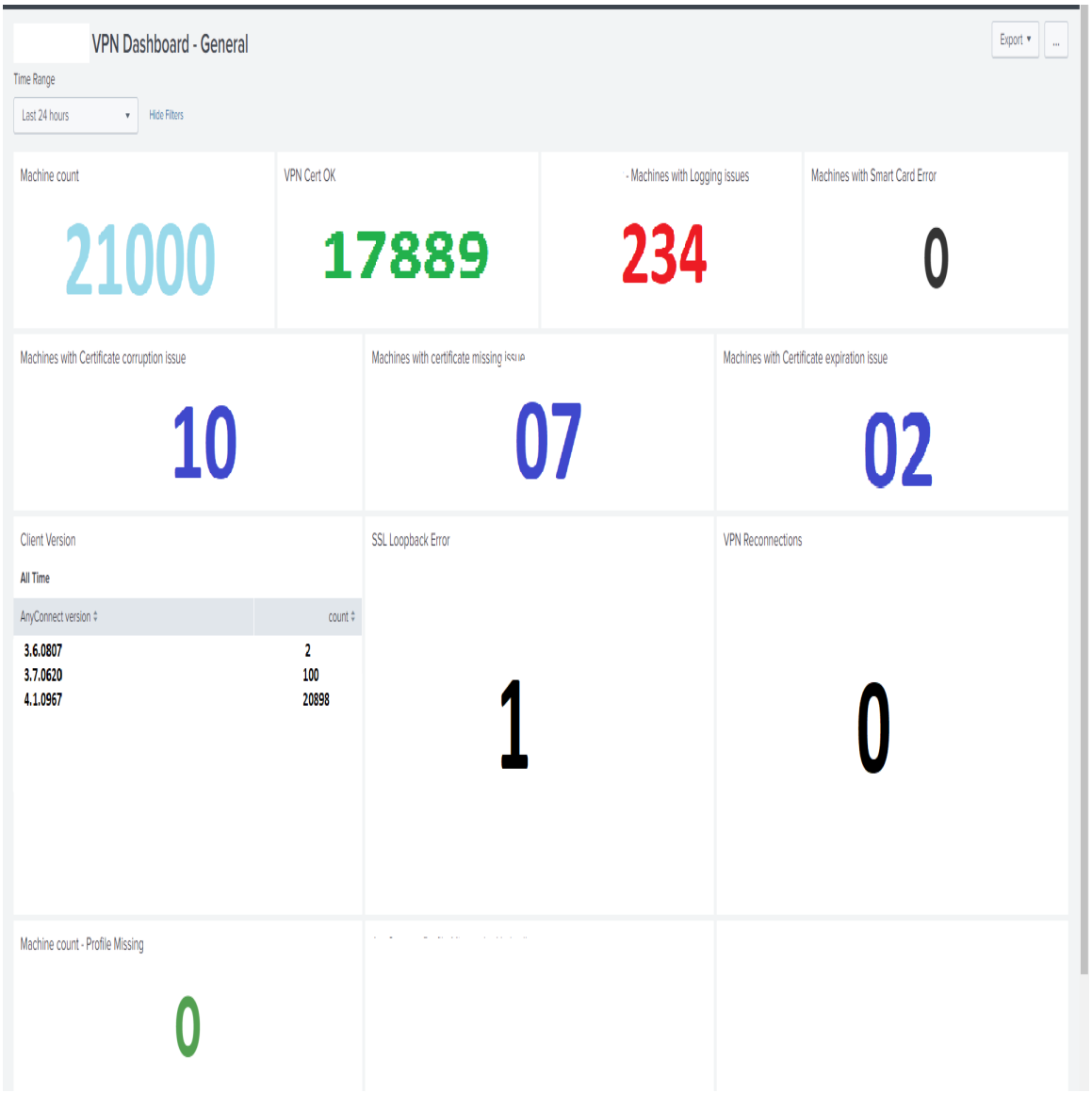

Figure 3.4: General Dashboard

Sample query: source="XmlWinEventLog: VPN Client software name " Name="Tool name " message="There was an issue with logging"

• Data visualization in terms of graph: Easy to recognize the data and we can generate reports accordingly with number of users and user details with id, which helps to reach user easy and fast manner with exact information related to problem.

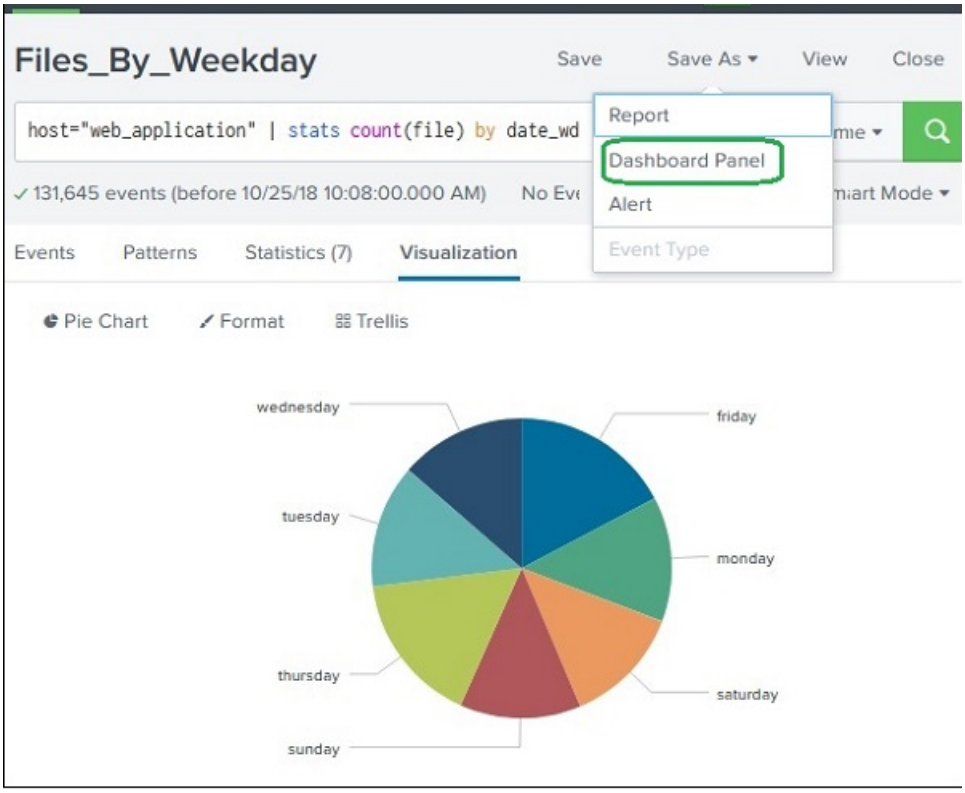

Figure 3.5: Graphical representation of data

4. Monitoring Dashboard

4.1 Existing System

Troubleshooting meetings with user to understand the problem and focus on DART log file analysis depends on users defined problems, which might not be the actual problem.

Requires deep analyzing of DART logs to find root cause and test unless it resolved.

Figure 4.1: Traditional Troubleshooting

4.2 Proposed system

Required clients data will be segregated depends on common problems with highlighting tab and range specified, which saves troubleshooting time as well as analysing logs thoroughly.

4.3 Troubleshooting Dashboard

Troubleshooting Dashboard: The Dashboard, which will give segregated data in tabular or graphical form to reduce the troubleshooting time and find root cause of VPN client problem. • Ease of Analysing logs.

• Time saving .

• Understanding way of representation.

• User friendly.

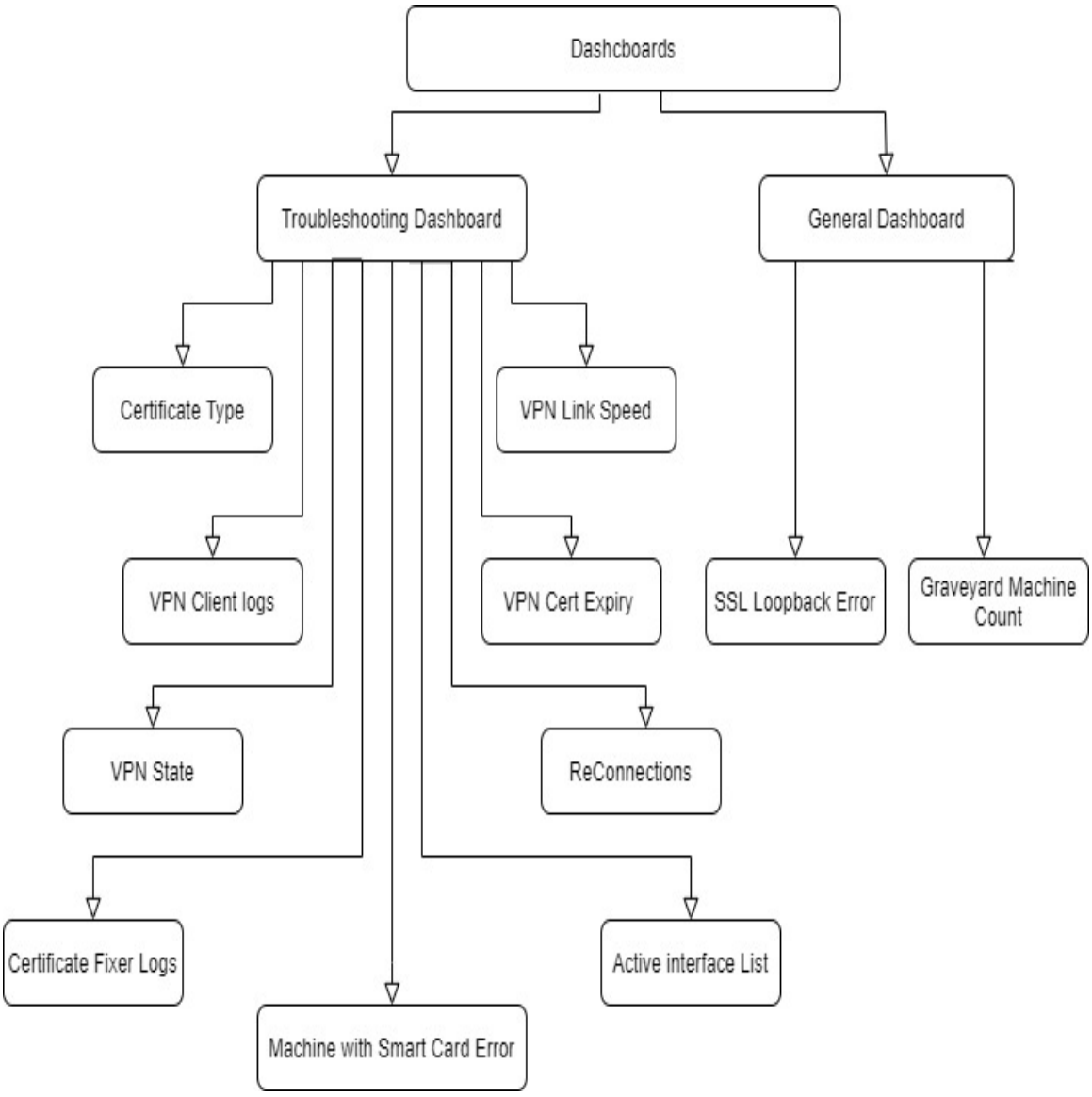

Figure 4.2: Architecture of Troubleshooting Dashboard

1. Certificate type: Certificates provides authentication to ensure the access to right person on VPN client. There are various types of certificates categorized based on which, version of operating system on users' machine-like old windows

machines, current versions of windows or Linux based operating machines. This tab showing, which type TPM (trusted platform module) of certificate user having. It will be useful to recognize the version compatibility of VPN client with user machine and easy to identify the problem.

2.VPN link speed: As VPN is secure tunnel between user and organization resources. User may not get full bandwidth of internet access as provided by users ISP(internet service provider) even though user has full VPN access. VPN link speed depends on multiple factor like ISP provider, compatibility of VPN client to the modem or router used by user for internet access , sometimes it depends on wifi or direct LAN connection and dominating factor might be number of users using same VPN gateway at same time (load balancing). VPN link speed also depends on applications used by users, which requires various bandwidth to different types of application resources. Low speed on VPN link as compare to ISP bandwidth may cause re-connection or slowness issue. This tab provides user's internet access speed when user connected via VPN and highlight, if it is very low than required, which may cause disconnections in future. It provides current speed of VPN link in MBPS(megabits per second)by which, it can be easily identified slowness issue.

3.VPN Cert Expiry: It will check the data from certificate and trace the valid from and valid to dates . After comparing current date with valid to date it will show that how long, it will be valid from current date. It shows, after how many number of days from today it will expire. From given number of days, it will be

easy to understand user requires immediate updates or not. If certificate is already expired and could not be updated by Cert fixer then, it will give result expired with red highlights. It will be easy to identify the Certificate fixer failure .

4.VPN state: What is current state of user's VPN connection is specified by this tab

• Connecting: VPN connection is not established yet (Above to establish).

• Connected: User is connected via VPN client right now.

• Reconnecting: user was connected previously but now reconnecting to VPN due some reason.

• Reconnected: re connection happened due to some hurdles in connection state.

• Disconnecting: on users request or due to some reason VPN is disconnecting now.

• Disconnected: User's VPN connection is disconnected state now due to session expire or users request.

5.Reconnections: Re-connections may happen due to several reasons • Power cut or internet supply breaks and resumes due to slowness issue or low speed of ISP provider.

• VPN re connections may happen, when user has both IPV6 and IPV4 protocol address and it is trying to connect VPN may get confused between IPV6 address and IPV4 which can leads to re connections.

• Number of times VPN re connections happening in users machine will help to

understand root cause of re connections

• This tab shows how many re connections happened in users machine in specified duration.

6.Machine with Smart card error: Smart card and VPN both are used to protest data and provide security with authentication. this tab shows highlights if user having smart card error issue. When user using smart card and trying to connect via VPN, it does not allow and through error as it does not allow authentication or entering username and password.

7.Active interface list: User can connect via different interfaces to the ISP internet like LAN(local area network) cable , Wifi(Wireless Fidelity). What all are actively present interfaces are there on user's machine listed with this tab and along with id(identity) number. This can be useful to identify the re connections issue sometimes. More than one active interface may lead to switching connections in between and causes re connection. It also provides information about interfaces to understand the other problems of VPN connection according to which, interface user using right now for VPN connection.

8.Certificate fixer logs: It will provide logs related to certificate fixer which are separated from VPN client logs. It contains all logs related to certificate like Renewed date: last renewal date of certificate, which is renewed by Certificate fixer automatically, when certificate is above to expire or corrupted or missing due to

some reasons (deleted, profile update). Certificate corrupted or missing and cannot be fixed by the Certificate fixer and other certificate related logs with details of time and date to analyze.

9. VPN client logs: Actual log file contains all above date with time basis but serration of log file in required tab will ease to analyze data. Remaining data, which are not present in above tabs and not in Certificate fixer logs are given in this logs like VPN connection, re connection times : When user connected to reconnected to VPN connection. Re-connections happened due to user request or automatic re-connections. User connected via, which active interface. Each information related to VPN connection along with time or date will be provide in this logs to analyze them deeply, when new or unknown problem occurs to find root cause.

Outcomes:

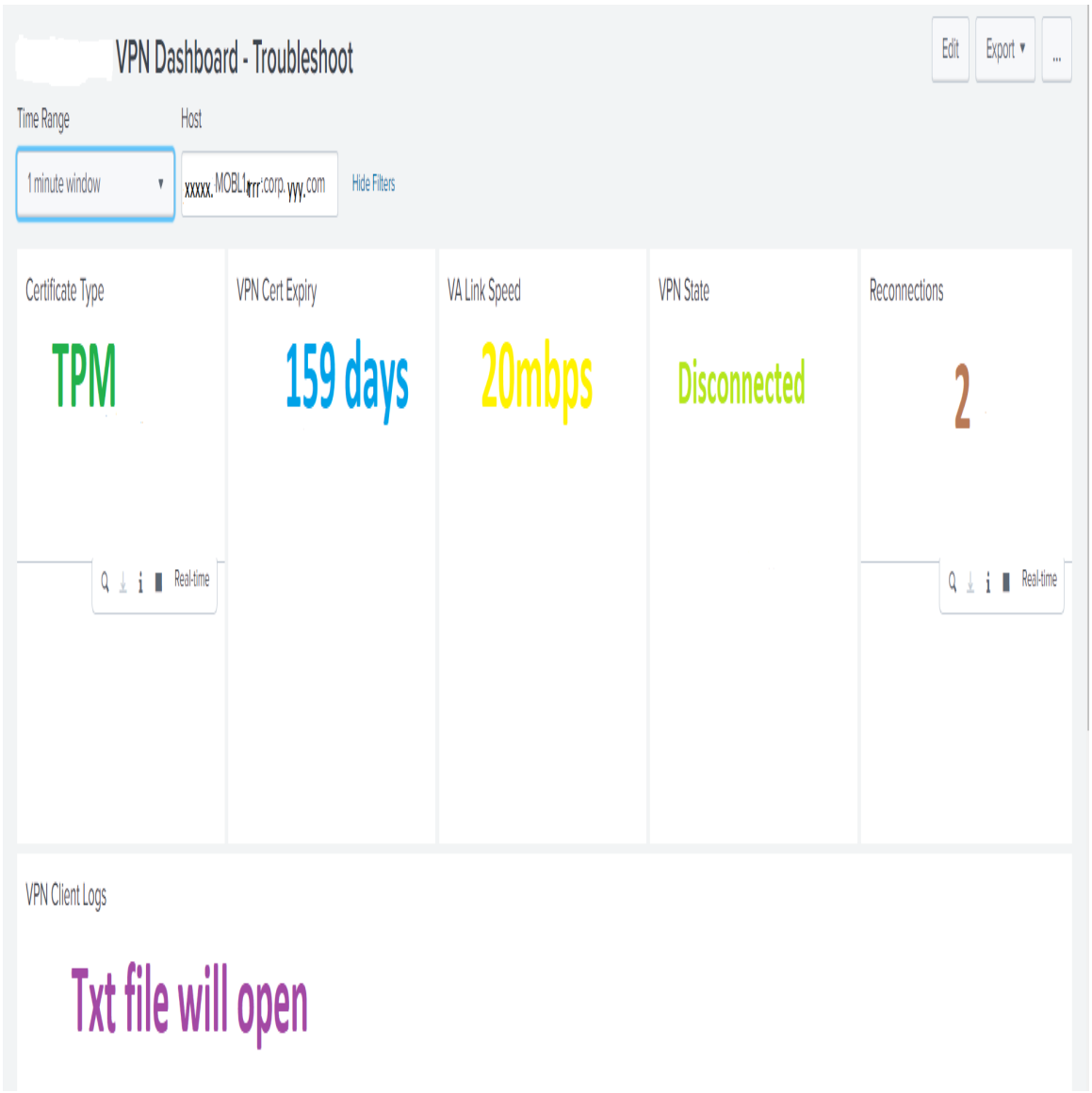

Figure 4.3: Troubleshooting Dashboard 1.1

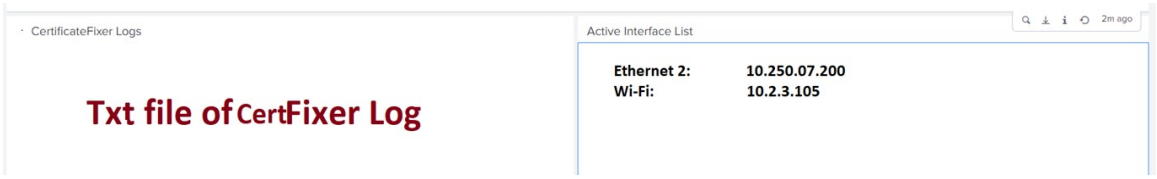

Figure 4.4: Troubleshooting Dashboard 1.2

Sample query: index=windows-client sourcetype=xml* source="XmlWinEventLog:VPN Client software name Client" host="*" VPN-state="Reconnecting" | stats count by host | sort -count

5. Summary and Conclusion

5.1 Summary

Studied and compared VPN connection with different level of security and Different VPN connectivity issues. Collection of logs and analyzing them to find root cause of VPN disconnection. Dashboard will help in summarizing common re-connectivity reasons and provide information in advance to take proactive decisions. Dashboard also helps in troubleshooting problems and find root cause to individual users and provide easy way of analysing the issues with segregation of data .

5.2 Conclusion and Future work

5.2.1 Conclusion

As Dashboard gives prier information about users with different VPN connectivity issue may cause in future, so it reduces the loss and efforts of handling incidents related to VPN client. It is preventive mechanism for VPN connectivity loss and gives sorted and required data of users. Saves times and manual efforts along with

user friendly and understanding Dashboard view.

5.2.2 Future work

Combining dashboards to ease resolving incidents with advance mechanism and alert generation.

Bibliography

[1] Chen Fei; Wu Kehe; Chen Wei; Zhang Qianyuan, IEEE. The Research and Implementation of the VPN Gateway Based on SSL. International Conference on Computational and Information Sciences 2013.

[2] Jinhai Zhang.Research on Key Technology of VPN Protocol Recognition. IEEE International Conference of Safety Produce Informatization (IICSPI) 2018

[3] Lin Shaofeng; Guo Chaoping; Sun WeifengPublisher. Design and Implementation of an Enhanced VPN Isolation Gateway. International Conference on Robots and Intelligent System (ICRIS), 2017

[4] Siddharth Mahajan; Mitesh Parekh; Hardik Patel; Sharvari . BRB dashboard: A web-based statistical dashboard IEEE International Conference on Innovations in Information, 2017

[5] Toasa; Marisa Maximiano; Catarina Reis; David Guevara,. Data visualization techniques for real-time information — A custom and dynamic dashboard for analyzing surveys' results IEEE 13th Iberian Conference on Information Systems and Technologies (CISTI), 2018

[6] Te-Jen Su; Shih-Ming Wang; Yi-Feng Chen; Chao-Liang Liu. Attack detection of distributed denial of service based on Splunk. IEEE International Conference on Advanced Materials for Science and Engineering (ICAMSE), 2016

[7] K. Karuna Jyothi*, Dr. B. Indira Reddy IT Department, Sreenidhi Institute of Science and Technology, Ghatkesar, Telangana, India. Study on Virtual Private Network (VPN), VPN's Protocols And Security. IJSRCSEIT International Journal of Scientific Research in Computer Science, Engineering and Information Technology 2018

[8] A. A. Rahman, Y. B. Adamu and P. Harun, Review on dashboard application from managerial perspective, International Conference on Research and Innovation in Information Systems (ICRIIS), Langkawi 2017

[9] R. Toasa, M. Maximiano, C. Reis and D. Guevara, "Data visualization techniques for real-time information — A custom and dynamic dashboard for analyzing surveys' results," 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres 2018

[10] W. Noonpakdee, T. Khunkornsiri, A. Phothichai and K. Danaisawat, "A framework for analyzing and developing dashboard templates for small and medium enterprises," 2018 5th International Conference on Industrial Engineering and Applications (ICIEA), Singapore 2018

[11] R. Magdalena, Y. Ruldeviyani, D. I. Sensuse and C. Bernando, "Methods to Enhance the Utilization of Business Intelligence Dashboard by Integration of Evaluation and User Testing," 2019 3rd International Conference on Informatics and Computational Sciences (ICICoS), Semarang, Indonesia 2019