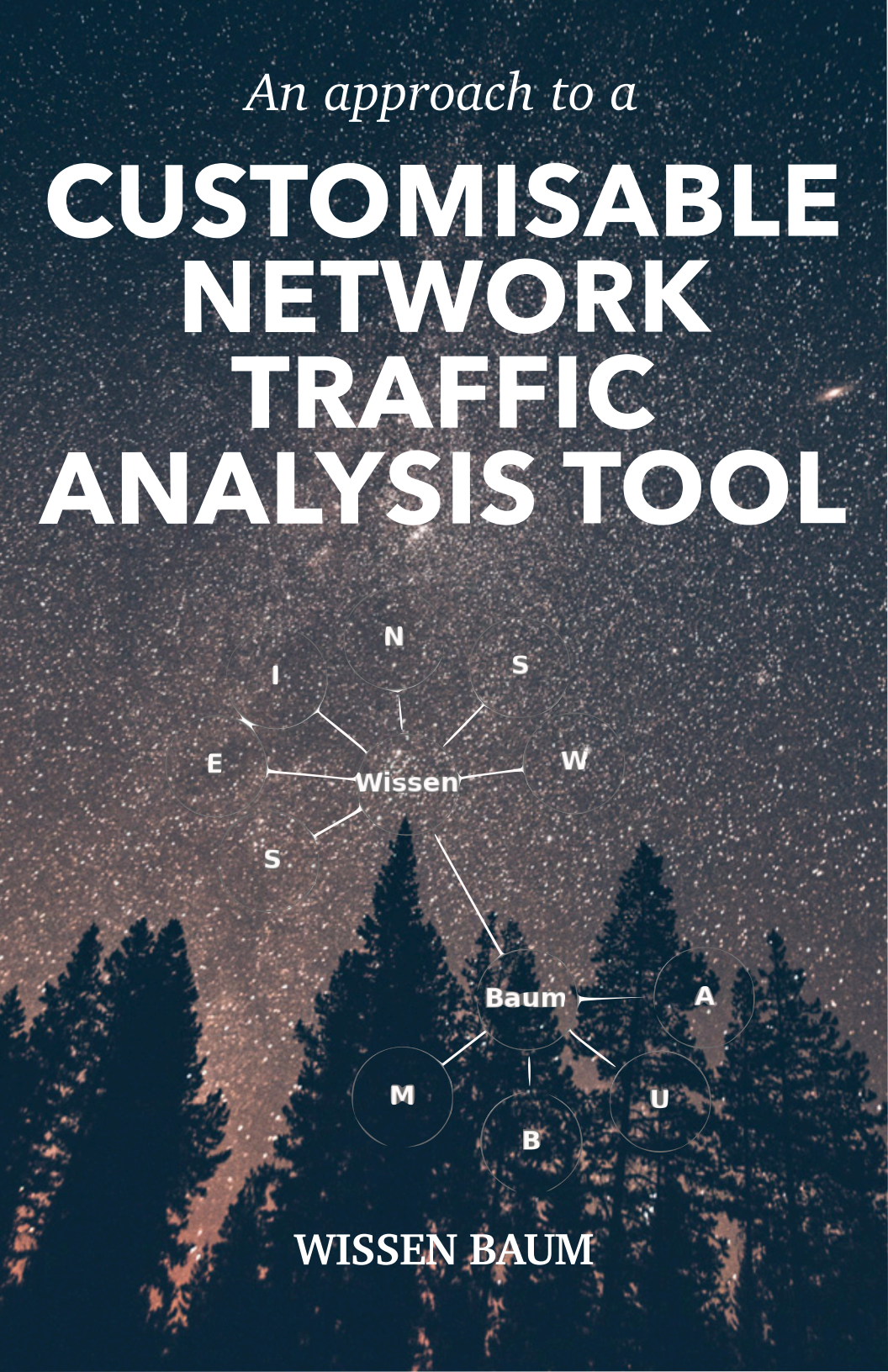
An approach to a

CUSTOMISABLE NETWORK TRAFFIC ANALYSIS TOOL



WISSEN BAUM

An approach to a

CUSTOMISABLE NETWORK TRAFFIC ANALYSIS TOOL

WISSEN BAUM

We are ISO 9001-2015 certified knowledge driven Digital Engineering, IT Services and Product Development company with global presence in Pune, Delhi (India) , Wolfsburg (Germany), Troy (USA). Our teams consist of experts from IIT, IIM, FH-Germany with expertise with Digital Engineering consultancies, engineering innovations and IT solutions to assist our customers to realise their goals such as Value transformation, increase Market share, minimising Risks, Assets management and capitalization on new opportunities. We work in the area of **Digital Engineering** with expertise towards *Product Design, Engineering Design & Support, Reverse engineering, Value engineering, Advance Engineering, Engineering prototypes, Tooling and Documentation*. We support our clients with **IT Solutions** in the area of *Digital Services, Digital Transformation, Network Security, Application Development, Data to Analytics to Machine Learning to AI, IIoT, AR and VR* solutions.

We are working with global OEM and Tier 1 suppliers around the globe. Our few of our esteemed customers are Altair, Ansys, Faurecia, IAC, Plastic Omnium, Tata, Mahindra, Mercedes Benz, PepsiCo, Varroc, Unilever and many more. We are closely associated with our associates such as ARAI, Klatt Dynamics, Hawener Technologies to provide global expertise.

Office 1,Prime 12,H-1, Sector No. 26
Business District Pradhikaran, Nigdi,
Pune, India 411044
http://www.wissenbaumllp.com

Breslauer Straße 16,
38440 Wolfsburg,
Germany
http://www.wissenbaumllp.com

The purpose of this white paper is to illustrate the current situation in the industry related to Network assets and a basic approach to handle the enormous amount of available network data into a useful and valuable information by performing Network Traffic Analysis.

Further the scope of the document is limited to What is Network Traffic Analysis, Why it should be done, an approach on how it is done and various other solutions which could help Business to improve the overall manner in which the network assets are managed.

NETWORK TRAFFIC ANALYSIS

Network Traffic Analysis in short “NTA” is a name coined by GARTNER. In this Technology driven world the industries have grown enormously to meet the market demand however still haven’t completely deciphered on how to organise the Network Infrastructure securely which in turn is a key attribute to meet their goal.

One of the key IT industrial problem is that How to maintain and optimise the Network Assets. Network Traffic Analysis help us to overcome this problem and additionally reap tremendous value to the Business in terms of improved security and network utilisation.

1. WHAT

WHAT DOES NETWORK TRAFFIC ANALYSIS MEAN?

"Network Traffic Analysis is the process of recording, reviewing and analysing network traffic for the purpose of performance, security and/or general network operations and management."

It is the process of using manual and automated techniques to review granular-level detail and statistics within network traffic.

Techopedia explains that Network traffic analysis is primarily done to get in-depth insight into what type of network packets or data is flowing through a network. Typically, network traffic analysis is done through a network monitoring or network bandwidth monitoring software/ application. The traffic statistics from network traffic analysis helps in:

- Understanding and evaluating the network utilization
- Download/upload speeds
- Type, size, origin and destination and content/data of packets

Network security staff uses network traffic analysis to identify any malicious or suspicious packets within the traffic. Similarly, network administrations seek to monitor

download/upload speeds, throughput, content, etc. to understand network operations.
Network traffic analysis is also used by attackers/intruders to analyze network traffic patterns and identify any vulnerabilities or means to break in or retrieve sensitive data.

Gartner's Neil MacDonald identified Network Traffic Analysis as one of the Top Technologies for Security in 2017. Now, in their inaugural Market Guide for Network Traffic Analysis, Gartner states that:

- To improve the detection of suspicious network traffic, security and risk management leaders should:
- Implement behavioural-based network traffic analysis tools to complement signature-based detection solutions.
- Include NTA-as-a-feature solutions in their evaluations, if they are available from security information and event, firewall, or other security products.
- Focus on scalability (can the solution analyze the volume of traffic in the network?)

Reference: Gartner, "Market Guide for Network Traffic Analysis," by Lawrence Orans, Jeremy D'Hoinne, and Sanjit Ganguli. February 28, 2019.

Traffic Analysis in simple term is about understanding *what are all the assets connected in the network, what are all the assets do in a network infrastructure and finally are they secure and performing business relevant transactions.In order to achieve the above all in an efficient way a tool is must to have..*

Network Traffic Analysis Tool should be considered keeping in mind that it enhances security, it is scalable, customisable and help in keeping the network assets compliant for IT Security audits.

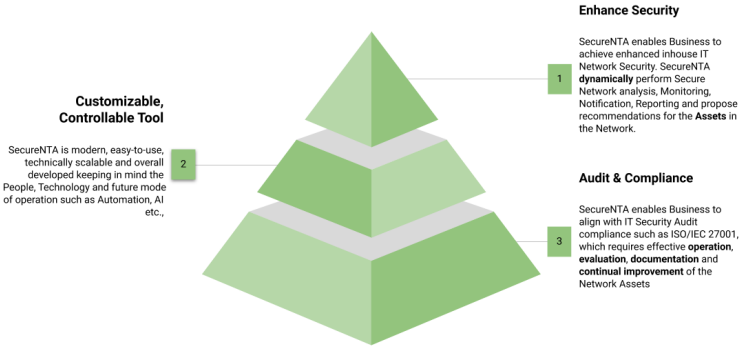


Illustration of key things to consider in the Network Traffic Analysis tool

Hence the tool should fulfil the demand for a High End Network Analysis Tool and additionally cover further areas of Network, IIoT, Data Engineering, Preventive & Predictive maintenance.

2. HOW

HOW THE NETWORK TRAFFIC LOOKS LIKE?

"An unorganised network environment as shown in the illustration shows that all network assets in the network are connected to one another to perform various production activity.

Now this situation raises the following questions:

- *What connects to what at any given time.*
- *Why they connect*

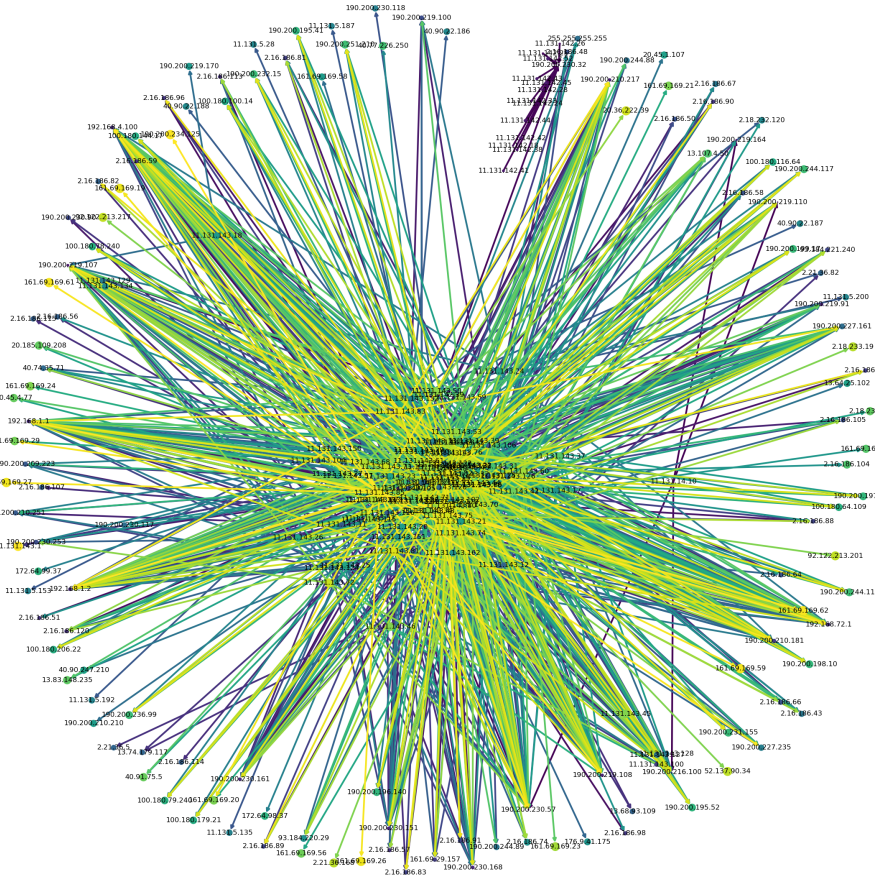


Illustration of an unorganised Network traffic

• *Are they meant to connect?*

All these network traffic connections or network traffic data is written into a file named SYSLOG. SYSLOGs in general consumes lot of storage space varying from few Gigabytes for small networks and few Terabytes in case of huge networks. These logs keep accumulating over the period of time and as a result the logs are deleted periodically either 90 or 180 days depending the size and need.

This means it is impossible to know

- How was the network behaviour in the past?
- Have the security measures improved?
- What Network Infrastructure changes were done?

Additionally the huge log size creates a special challenge. It is cumbersome to analyse the SYSLOG data completely with a normal data editing tool to come up with a meaningful information.Moreover the data need to be analysed with some logical approach so that the outcome derives value to the business.

Hence it is evident that, there is a need for a Network Traffic Analysis, additionally a need for a tool and moreover it has to be customisable to meet the Business requirements in order to achieve the complete value.

3. ANALYZE

KEY ASPECTS THAT THE NETWORK TRAFFIC ANALYSIS TOOL SHOULD DO?

Visualise a shop floor with numerous devices on multiple line assembly and they all are connected in a network (VLANS) to manufacture a part. Let us consider the four Shop floor devices (SFD in short) SFD0, SFD1, SFD2 and SFD3 respectively as shown in the illustration.

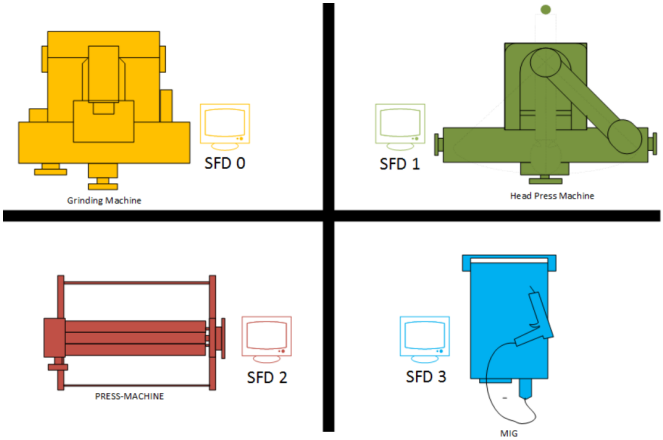


Illustration for network devices or assets in a Shop Floor

3A. NETWORK MATRIX

“IDENTIFY THE NETWORK COMMUNICATION MATRIX”

Network Communication Matrix helps understand What device IP connects to What other device IPs in the network. This is the first step towards organising the network. Here organisation could benefit knowing what is the relevant and irrelevant traffic for their Business operations, hence Network Analysis tool

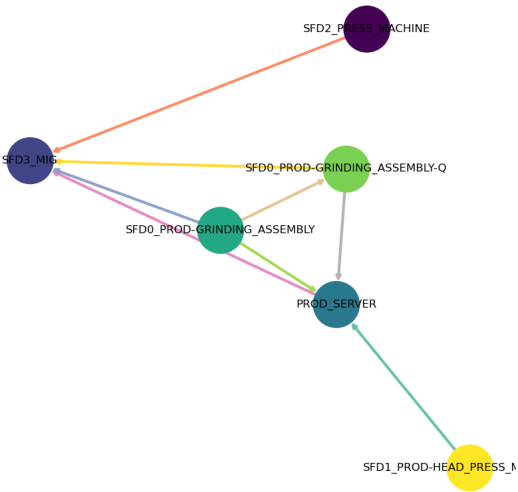


Illustration of Network Communication Matrix

should therefore pocess this key feature to visualise the Network Communication Matrix as shown in the illustration.

3B. NETWORK TRAFFIC

“UNDERSTANDING THE TRAFFIC”

Tool should further provide insight on the overall traffic distribution across time. The traffic should be further categorised in to Connections, Bytes and Duration against average hourly, daily, weekly, monthly network utilization as illustrated in the image

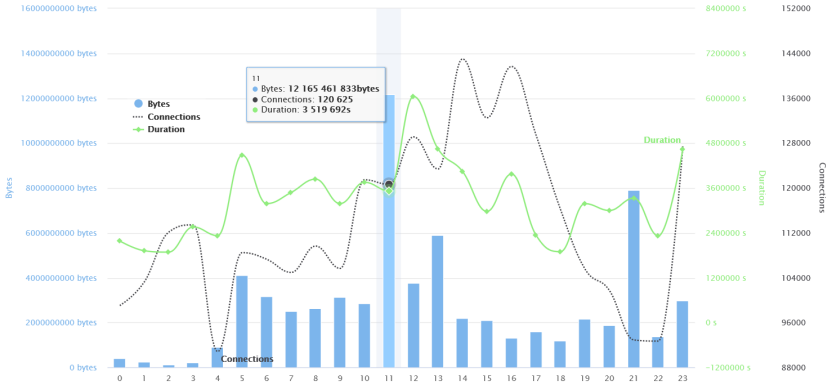


Illustration of Traffic Distribution across 24 Hours

The traffic distribution information helps to understand the peak Production, Network utilization, high Data Transfer

and additionally support to plan for Maintenance, Software Updates etc.,

Traffic utilization feature would be very valuable for business to proactively schedule various production activities.

Additionally if the data is integrated with Network assets performance information such as CPU, Processor Speed, Memory, Storage etc., this could further give insight for the management about the overall performance vs utilization. This way Business could compare cost savings for their existing physical infrastructure to a cloud based infrastructure.

This tool feature on the long run could provide valuable information to the Business to arrive at a decision on How their Future mode of operation should be?.

3C. IP

“ANALYSING THE IP”

IP based analysis enables us to identify which specific IP or a device or a network asset is responsible for more connections, high data transfer etc., As IPs are very sensitive data they have to be handled efficiently since they could open doors for IT Security breaches.

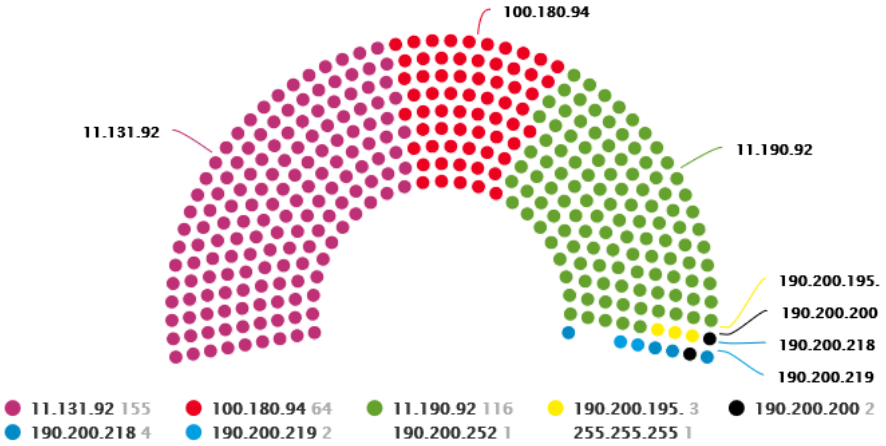


Illustration of Source and Destination IP Ranges of involved Network Assets

Best practice would be to use a Bar-code or QR Code or Hostnames near the devices or network assets instead of leaving the IP address on the device. This reduce the chance of a security event. The IPs shown in the image are only for illustration purpose.

The tool should pocess the below listed features:

- Identifies the Source, Destination IP Ranges of all involved network assets.
- Categorises the TOP IP based on Connections, Bytes, & Duration
  - *In this illustration top 4 ips contributes to 80% of connections*
- Identify the legitimate and illegitimate traffic connections
    - Internal IPs connecting to external Network in the internet
- Identifies the various type of traffic performed by the IPs

Performing a detailed analysis on IP is very imperative and the below listed criteria's should be considered

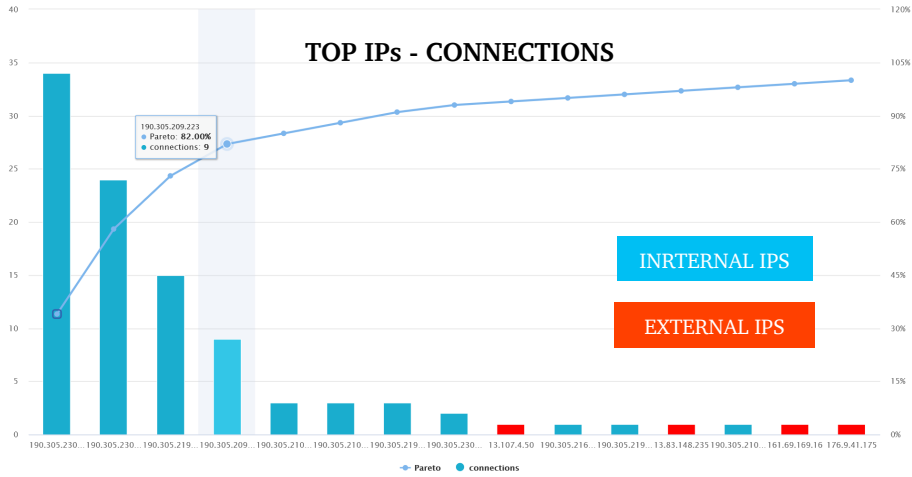


Illustration of Traffic Distribution across 24 Hours

- IP belongs to which VLAN
- IP belongs to which Range
- IP belongs to which location
- IP belongs to which Value Streams or Assembly lines
- IP belongs to which kind of Operating System
    - (Windows or Legacy. This is feasible based on device naming convention or AD or other ways to map IP with Operating System.
- IP belongs to any third party applications
- IP belongs to critical assets
- IP belongs to VPN etc.,

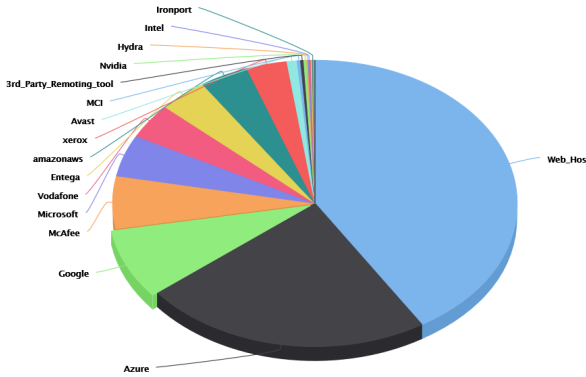


Illustration of External IP

- IP belongs to External Internet - which are the main source of security attacks.

Hence all the above listed features should be a must have feature in the analysis tool. Additionally the analysis on IP should support in creation of appropriate Firewall Rules.

3D. PORTS

"ANALYSING THE PORTS"

Ports like IPs are a very important network data. The network ports 0-65535 TCP/UDP are fixed and known to all those who work in the network environment. As a result this creates a high level security challenge. Ports are highly vulnerable and need to be monitored regularly otherwise it could trigger security event.

The analysis tool should process the below listed features

- Identifies various ports and categorise them as Source and Destination ports

- analyze the data dynamically to identify the anomalies by Ports based on bytes, connections, port type etc..,

- Categorises the ports further by port names, purpose of connection etc., to deploy appropriate security measures

In the illustration above Destination Port 445 contributes to high bytes transfer. In this case Port 445 TCP Microsoft-ds

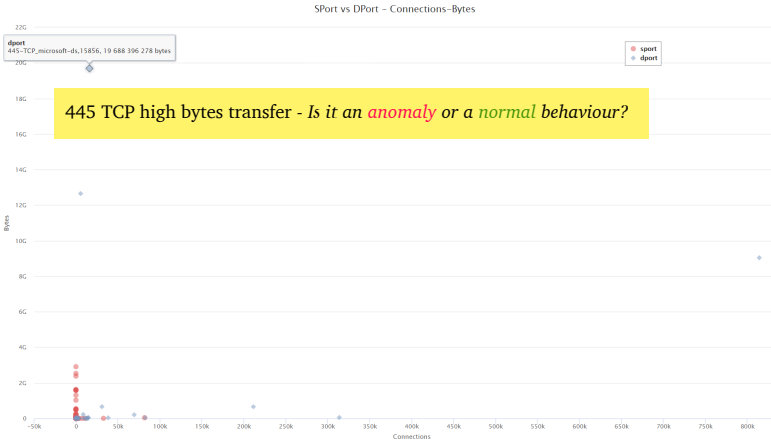


Illustration of Source and Destination Ports - Connections vs Bytes

is a renowned port for File Transfer at the same time need to be always mindful that this port was exploited by the attackers in the past.

The vulnerability that the attackers are exploiting is in the SMB component in Windows. Server Message Block (SMB) is a network protocol that provides file and printer sharing services in Windows systems (139 Netbios, 445 TCP). SMB may be allowed within the internal network for sharing files and printers; however, it should be restricted from connecting to the external network.

It is strongly recommended that *blocking "all versions of Server Message Block (SMB) at the network Firewall* ***by blocking TCP port 445*** *with related protocols on* ***UDP ports 137-138 and TCP port 139,*** *for all network devices." This* ***measure prevents the WannaCry attack*** *and should be implemented on business and internal firewalls.*

The Port traffic analysis need to be performed efficiently on every individual network asset. Hence the analysis tool should support with identifying the devices that require to use these vulnerable ports. This information could be used by

the Network personnel to define appropriate firewall rules to prevent security breaches such as Ransomware, WannaCry etc.,

Additionally the tool should enable in anomalies detection based on port traffic behaviour.

3E. FIREWALL

"DEFINING FIREWALL RULES"

Firewall Rules definition is a cumbersome process and it is impossible to do it at a large scale accurately without analysing the network logs efficiently. If the traffic is not analysed properly it could result in a security event or a network availability failure or production downtime.

Firewall Rules are like Security Guards with guidelines and the network IPs, Ports are like the key traffic identifiers or Identity card for the Firewall to accept or allow the traffic entering into the network boundary.

The tool should thus pocess the below listed features:

- **Identify Firewall rules** for the **100% traffic**
- Categorise the rules based on the traffic pattern
- Propose Business to Allow/Deny Rule permission based on IPs or Ports or Device Mac Address
- Exportable as a report for review and carry out further Business actions.

Rule Permission	Source IP	Destination IP	Source Port	Destination Port	Review Comments
Domain Joining Rule					
☑ Allow ☐ Deny	"sip":["100.180.143.124","100.180.143.43","100.180.143.170","100.180.143.160","100.180.143.63","100.180.143.130","100.180.143.59","100.180.143.33","100.180.143.73","100.180.143.162","100.180.143.20","100.180.143.116","100.180.143.151","100.180.143.75","100.180.143.72","100.180.143.39","100.180.143.24","100.180.143.25","100.180.143.123","100.180.143.50","100.180.143.11","100.180.143.26","100.180.143.30","100.180.143.12","100.180.143.49"]	"dip": ["190.200.219.108","190.200.219.110","190.200.230.57","190.200.230.58","190.200.240.59","190.200.230.67","190.200.230.78","190.200.240.79"]	"source_port":["4149-TCP","63558-UDP","50191-UDP","1027-UDP","65201-UDP","4850-TCP","58286-UDP","50838-TCP","4150-TCP","59208-UDP","55419-UDP","49981-UDP","61477-UDP","61567-UDP","63460-UDP","59538-UDP","59190-UDP","50907-UDP","56421-UDP","50836-TCP","56913-UDP","51432-UDP","64729-UDP","63273-UDP","56506-UDP","50837-TCP","53494-UDP","55868-UDP","54728-UDP","53234-UDP","51031-UDP","4851-TCP","49174-UDP","55038-UDP"]	"destination_port":["88-TCP","53-UDP"]	Name: Enter review comments

Illustration of Firewall Rule

- This should be repeatable in the event of retiring or adding a new asset to the Network.

The above illustration is an example of Domain joining Firewall Rule in a html table format. It is important that the network assets (Source IP) are allowed to connect to other device on the network (Destination IP) through the allowed Source and Destination Ports respectively.

This approach has to be performed for every single network asset or device part of that network boundary. If it is meticulously done then the network asset permission would be limited only to business relevant traffic.

Overall by analysing and applying all the required Rules or permissions the overall Network traffic bandwidth to and fro within the network boundary would be reduced. Therefore directly reflects in cost savings in terms of network bandwidth, reduced non business relevant activities etc., and provides input towards planning *what is the bandwidth consumed and what is the optimal network bandwidth and what would be required future network bandwidth etc.,* Hence it is mandatory that this feature is a must to have feature in the Network Traffic Analysis tool.

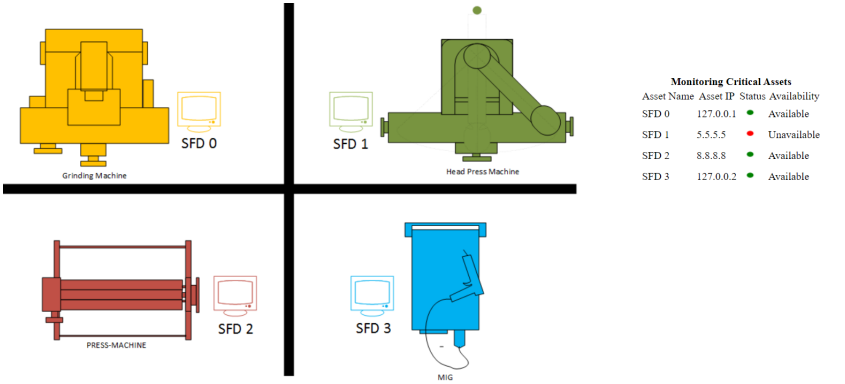


Illustration of Network Asset Availability Monitoring

3F. MONITOR

“TRAFFIC MONITORING & ALERTING”

Monitoring and alerting are a must have feature for any tool or a web application, in this case it is even more important as the analysis is done on Network assets. The network traffic analysis provides useful information such as traffic behaviour, network asset behaviour, device availability, port usage etc., These analysis should enable business to track, monitor, act and prevent security events.

The tool should pocess the below listed features:

- 24/7 Availability Monitoring for critical assets
- Anomalies detection
- Alert notification by Email

- History of events or Timeline information about the traffic pattern minimum for critical assets (even though this is a good to have feature for root cause detection and additionally it may consume lot of application resources, storage etc.,

In the above illustration four devices are monitored for network availability. This device availability should be checked periodically and incase a device or network asset become unavailable a security incident has to be generated and a notification should be shared to the network team and the person in charge of the assembly line.

This would enable them to take necessary action required to bring the device or asset back online. This a key feature for any network tool and in this case as we are analysing Network Traffic it becomes even more vital for the Business operations team to track and monitor it.

High Availability means high productivity and also additionally threshold could be defined for any identified traffic behaviour such as

- an abnormal spike in File transfer,
- Connections to websites with no Business relevance
- Traffic related to 3rd party Remote Desktop tools
- Traffic from outside network or locations etc.,

Hence Monitoring and Alerting should be a must to have feature of the Network Traffic Analysis tool.

3G. DASHBOARD

“DYNAMIC DASHBOARD”

Dynamic Dashboard integrated with powerful software engine on the background to analyze high volume of network data in realtime and transform them into valuable network information.

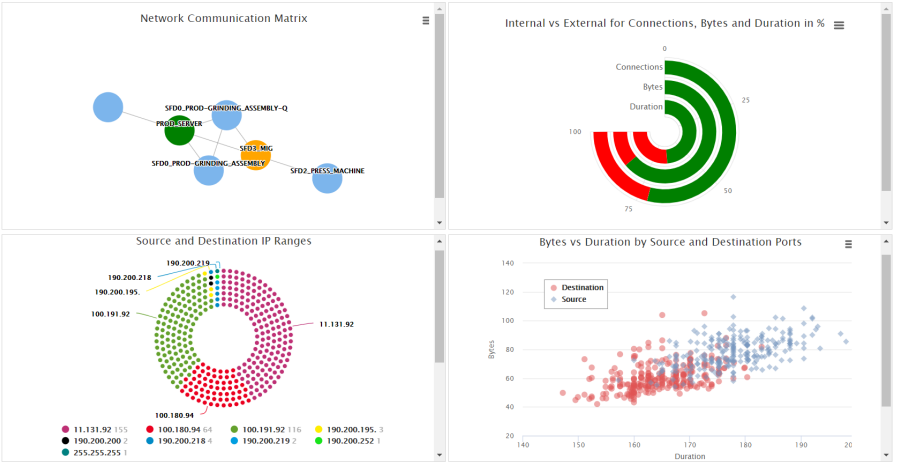


Illustration of Dynamic Dashboard

In the illustration above the Dashboard shows in a single view the *Network Communication Matrix, Traffic distribution of Internal and External Traffic w.r.t connections, bytes and duration, IP ranges distribution and Port traffic behaviour*.

Thus analysis tool dashboard should display the required information that are valuable for the business to take key production decisions such as maintenance, prevent security events, monitor changes etc., so that the Business and the operations team are mutually benefitted.

Overall the dashboard should be customisable to the requirement of the business focussing on Value in terms of *ease of Operations, Security and Availability*.

3H. ADVANCED

“ADVANCED ANALYSIS AND REPORTING”

Advanced Traffic analysis is a good to have feature since it could benefit the business in identifying anomalies or abnormal traffic behaviour. This feature could be used as a preventive analysis and appropriate security measure could be taken by defining further monitoring or alerting.

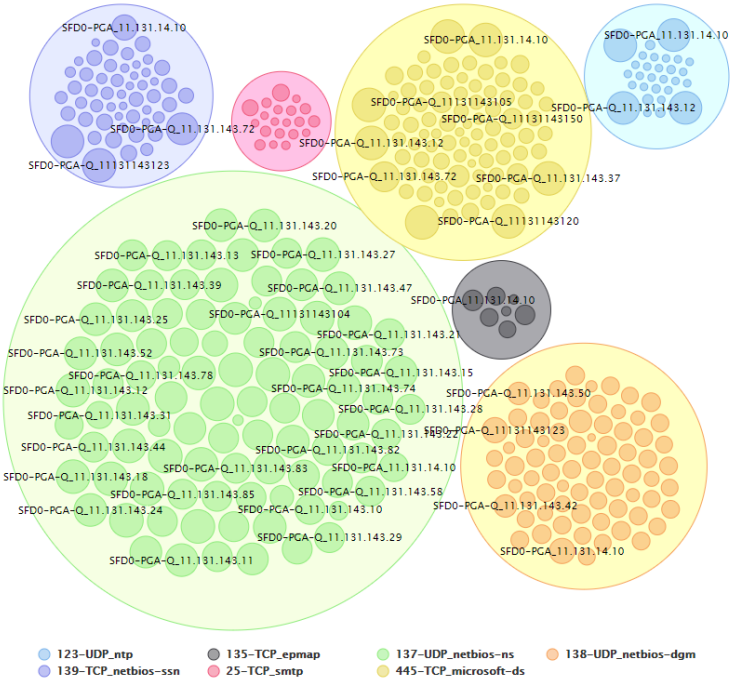


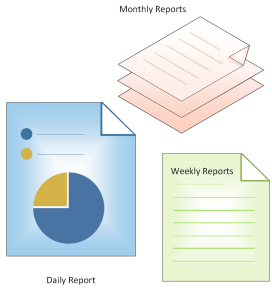
Illustration of Advanced analysis feature

Preventing or detecting a Security event before occurrence is a very difficult task, however with proper analysis and alerting in place it is possible. Hence the tool should process advanced network analysis as a feature.

In the following illustration the ports traffic behaviour are analysed. These are some of the key ports which are vulnerable and could be exploited by the attackers.

The illustration provides information about ports and associated IPs in this scenario as long as the IPs are internal the traffic behaviour is considered to be safe. These ports in general are used for internal purposes however if there are some external IPs involved then a security event should be created and further analysis should be done. The outcome could be helpful in either setting up a monitoring alert, closure of a security breach by blocking the related Port and IP traffic in the Firewall.

Last but not the least a detailed Reporting of complete Network Traffic Analysis should be generated and shared to the key stakeholders such as CISO, Business Leaders, Operations Head, Network Team etc., The tool should pocess feature to generate daily, weekly and monthly reports in the form of PDF or HTML which could be stored and utilised in the event of internal or external Security Audits.



4. NTA PROCESS

“SHOULD BE A PROCESS DRIVEN NETWORK TRAFFIC ANALYSIS TOOL”

Process driven network analysis means the security measures could be continuously followed and improved. This also provides opportunity for the Organisational members to accept some roles and responsibilities over the period of time.

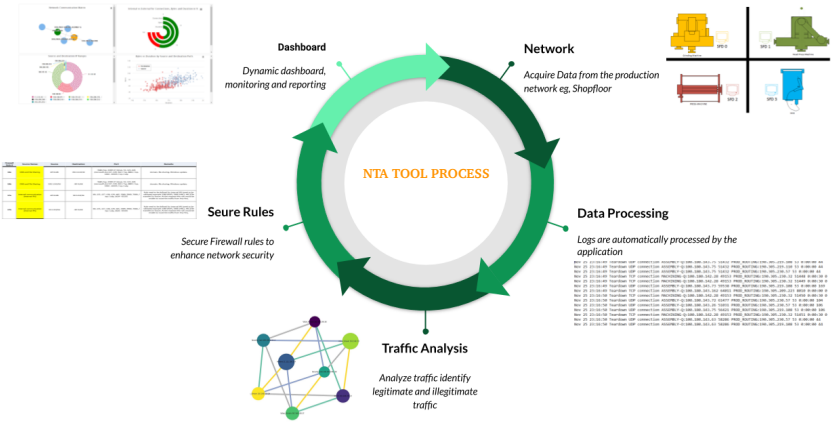


Illustration of.a Process driven Network Traffic Analysis Tool

In the event of key security findings the nature of the breach, impact, cause and measure should be shared to the

entire organisation. This should be followed as part of a security best practices since this would create security awareness across the organisation.

Additionally provides opportunity for the Business to hear from the key members about their view on the security measures. Overall the benefit of providing periodic awareness means less money spent on the awareness campaigns related to Security breaches, Trainings etc.,

The above illustration is a proposed process on how combining the process and analysis Tool would help the. Business. The idea is that the Tool based analysis should be performed periodically hence it should be easy to handle and repeatable process.

Additionally in the event of a new firewall wall the whole analysis information could be used to replicate the network setup and once the network setup is put in place the analysis could be performed once again and the results could be validated for any deviation. This would be a humungous task without a process and tool in place.

Hence the tool features should engage the appropriate organisational members for key workflows in order to achieve the desired result. This kind of process driven approach would help the organisation implement high-level of security measure and also plan for the Future mode of Operation.

5. NTA VALUE

“SHOULD BE A VALUE DRIVEN NETWORK TRAFFIC ANALYSIS TOOL”

Value driven network analysis means benefits that could be directly realised as an outcome from the Tool. The below listed key values should be must to have as part of benefits from the tool

- **Knowing** - *Tool should enable businesses understanding their own Network Better to create Security awareness and plan measures to mitigate network security Risks.*

Illustration of Network Traffic Analysis tool to be value

- **Utilization** - *Identifying non performing assets would reduce Total Cost of ownership*

- **Maintenance** - *Network Traffic peak pattern enables Business to plan for maintenance, patching etc.,*

- **Threats** - *Enables to identify Business relevant and non business relevant traffic such as External Internet IPs, Malicious IPs that could be blocked in the Firewall to prevent security threats.*

- **Compliance** - *Monitor key assets for availability and Generate periodic reports for Audit and compliance*

SUMMARY

❖

Network Traffic Analysis Tool is a must to have tool for any Organisation irrespective of how big network infrastructure they pocess. The understanding from the analysis serves the basis for how the Organisation would shift to its next level of operations and mitigate the risks, network threats etc.,

Having a customisable tool means not only the necessary security measures could be made possible it could also provides opportunity to integrate further network assets such as HMI, IIoT devices, Sensors, edge devices etc.,

When appropriate customisations are done to the tool and the dashboard the same tool could become a multipurpose tool. This in turn would provide high value in terms of security and cost savings for the Business.

WISSEN BAUM