Analysis and research of situation awareness based on private network endogenous security

Wei Zhu[1] Hanyi Dai[2] Zhangqi Zhu[1] Peng Ye[1]

1.China Mobile Zijin (Jiangsu) Innovation Research Institute, Nanjing, Jiangsu, 210000

2.China Mobile Communications Group Jiangsu Co., Ltd., Nanjing, Jiangsu, 210000

Abstract: in 2022, in order to adapt to the rapid development of Tob customers' businesses in the industry private network, 5g MEC, cloud network, dedicated line, IDC and dict, and meet the urgent needs of government and enterprise customers for products and services such as traffic control, traffic security and anomaly detection, network security situational awareness, network operation and maintenance, business performance assurance, service inspection and SLA evaluation in the park, edge cloud, government affairs and other scenarios, Combined with the strategic deployment of "digital computing in the East and digital computing in the west", the construction planning of edge cloud, the promotion of new technologies and business application scenarios of computing network, enterprise customers have more clear and strong requirements for cloud SLA service guarantee and security level guarantee based on computing network.

Therefore, it is necessary to establish an endogenous security protection mechanism, strengthen the new security protection capability based on traffic and the security scheduling capability that moves with the computing network, and ensure that the network infrastructure is safe and controllable.

Key words: 5g private network; Safety; Situational awareness; Anomaly monitoring

1 introduction

In the 5g private network, after the operators sink the UPF to the park, they may face security risks such as worm virus /ddos attacks, the increase of new malware and malicious tools, attacks using professional industrial protocols, and attacks using vulnerabilities in industrial cloud, industrial app, and industrial edge computing.

Zijin Research Institute upgraded the computing edge awareness and security service capabilities of the minimalist intelligent control private network steward to meet the situation awareness needs of the government and enterprise business side, especially in the edge cloud, parks and other scenarios. It deployed the computing edge situation awareness products on the customer side to cover the network traffic control and anomaly detection, security situation awareness, business supportNetwork management, operation and maintenance and other requirements, as well as customized service capabilities, as well as customer collection requirements at different levels.

2 Technical solutions

2.1 Build a secure platform architecture[2]

Based on 5g private network security situational awareness platform, through massive heterogeneous data collection and analysis, in-depth detection and intelligent analysis, so as to achieve situational awareness and safe operation. The overall architecture of the platform is as follows:

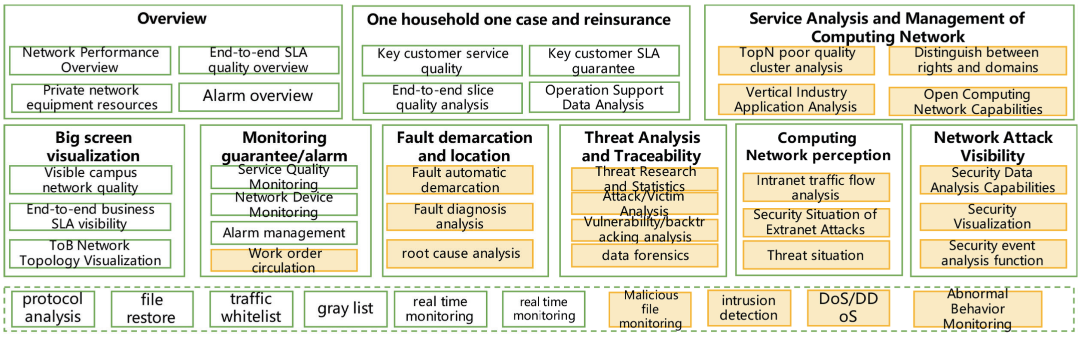

Overview
Network Performance Overview
End-to-end SLA quality overview
Private network equipment resources
Alarm overview
One household one case and reinsurance
Key customer service quality
Key customer SLA guarantee
End-to-end slice quality analysis
Operation Support Data Analysis
Service Analysis and Management of Computing Network
TopN poor quality cluster analysis
Distinguish between rights and domains
Vertical Industry Application Analysis
Open Computing Network Capabilities
Big screen visualization
Visible campus network quality
End-to-end business SLA visibility
ToB Network Topology Visualization
Monitoring guarantee/alarm
Service Quality Monitoring
Network Device Monitoring
Alarm management
Work order circulation
Fault demarcation and location
Fault automatic demarcation
Fault diagnosis analysis
root cause analysis
Threat Analysis and Traceability
Threat Research and Statistics
Attack/Victim Analysis
Vulnerability/backtracking analysis
data forensics
Computing Network perception
Intranet traffic flow analysis
Security Situation of Extranet Attacks
Threat situation
Network Attack Visibility
Security Data Analysis Capabilities
Security Visualization
Security event analysis function
protocol analysis
file restore
traffic whitelist
gray list
real time monitoring
real time monitoring
Malicious file monitoring
intrusion detection
DoS/DDoS
Abnormal Behavior Monitoring

Figure 2.1: Security Platform Architecture

2.2 Probe safety function

Collect 5g traffic based on 5g traffic probe (and virtualization probe), and realize 5g traffic based extraction, correlation and output. 5g private network security through traffic and interactive log data:

Considering the application environment of vertical industry users, support scada/plc industrial Internet of things flow safety detection

Support traffic security analysis and threat detection under 5g high traffic

Tap the advantages and highlights of pipeline flow collection of operators, focusing on attack traceability analysis and evidence retention

Consider the security capability output for industry users, support flexible customization and function integration, and support multiple identity authentication:

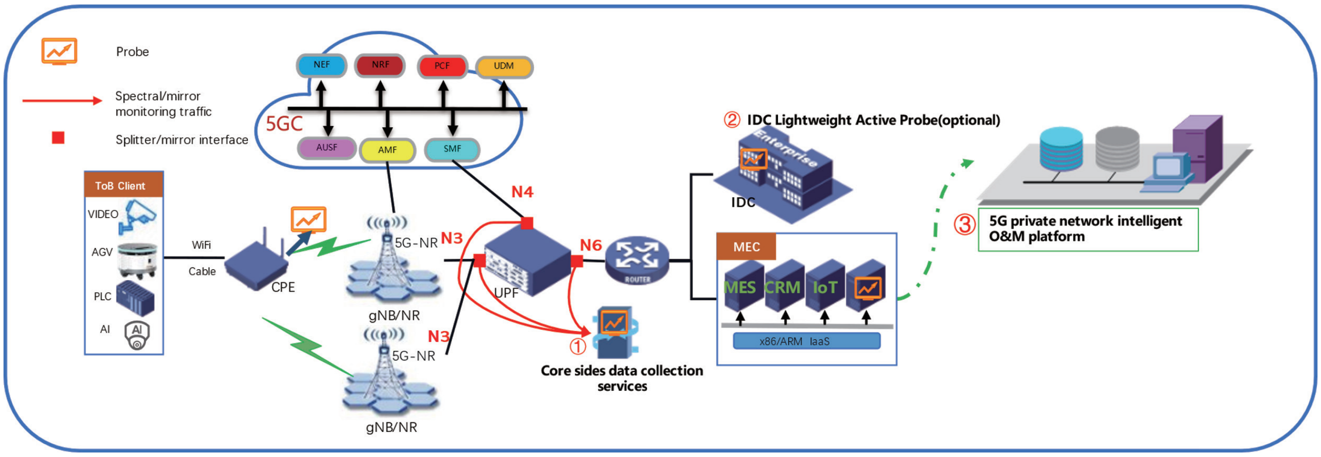

Probe
Spectral/mirror monitoring traffic
Splitter/mirror interface
5GC
NEF
NRF
PCF
UDM
AUSF
AMF
SMF
ToB Client
VIDEO
AGV
PLC
AI
WiFi
Cable
CPE
5G-NR
N3
gNB/NR
5G-NR
N3
gNB/NR
N4
UPF
N6
ROUTER
① Core sides data collection services
② IDC Lightweight Active Probe(optional)
Enterprise
IDC
MEC
MES
CRM
IoT
x86/ARM IaaS
③ 5G private network intelligent O&M platform

Figure 2.2:5g private network monitoring probe deployment

2.2.1Flow analysis and restore

Before determining, it is necessary to specify the optimization area and the optimization cell, mainly through the following steps:

(1) Support in-depth parsing and service restoration of HTTP, FTP, SMTP, POP3, IMAP, TCP, UDP protocols;

(2) Support the restoration and storage of malicious files detected in the traffic for association analysis and forensics.

2.2.2Threat detection

(1) Cover a variety of attack features:

Including detection of edge cloud, network viruses, worms, spyware, Trojan backdoors, scanning detection, brute force cracking and malicious traffic;

It supports e-mail exception detection, and supports exception detection for e-mail accounts, e-mail keywords, etc;

It supports remote control anomaly detection, detection and alarm of remote control protocols, and supports msrdp, vnc, TeamViewer, PcAnyWhere, and telnet protocols;

(2) Covers a variety of detection engines:

Including support for DDoS detection and alarm in network layer and application layer;

Support custom TCP and UDP port scanning detection model, built-in web application machine learning detection model, built-in malicious file detection engine;

(3) Support the detection of malicious IP, malicious URL, malicious domain name and malicious email; It supports importing and exporting customized Threat Intelligence in Excel.

2.2.3Threat analysis

(1) It supports the statistics of threats in the network, including the top view of attackers, the top view of victims, the top view of malicious files, the distribution of threat events, the top view of rule hits, the view of asset identification proportion, and the demonstration screen recording and screenshot proof;

(2) Support fast retrieval and presentation of stored data logs;

(3) It supports a more flexible analysis method for massive data full field retrieval, and can retrieve or display based on any field in the log.

2.2.4Flow analysis and restore

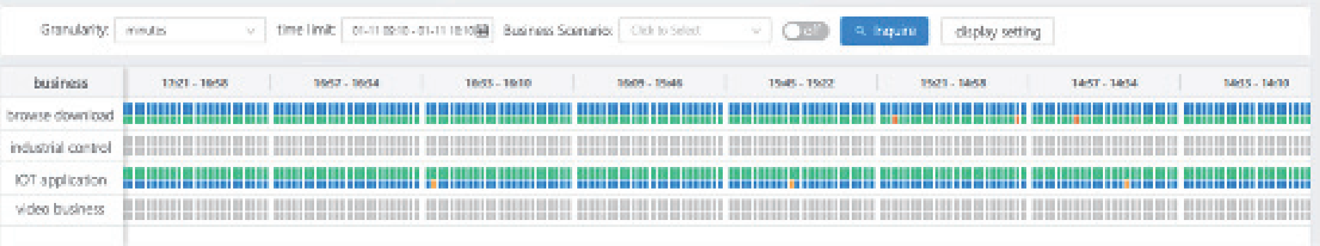
It supports the detection and alarm of illegal websites, and supports the customization of illegal websites.

2.3 service quality monitoring of 5g private network

5g private network service quality monitoring. This function module realizes the statistics and visual display of relevant indicators of the health quality of business applications.

It supports statistical analysis and display of health quality of different business applications in different time granularity. The threshold can be customized

And the quality of each particle size can be visually displayed through different colors


Granularity: minutes

time limit: 01-11 09:10 - 01-11 18:10

Business Scenarios: Click to Select

Figure 2.3: overview of business quality monitoring

2.3.1Industrial interconnection service quality

Realize the visual analysis and presentation of relevant performance indicators of industrial interconnection (Modbus) services in the park, such as transaction delay, transaction success rate, transaction number, transaction non response rate, etc.

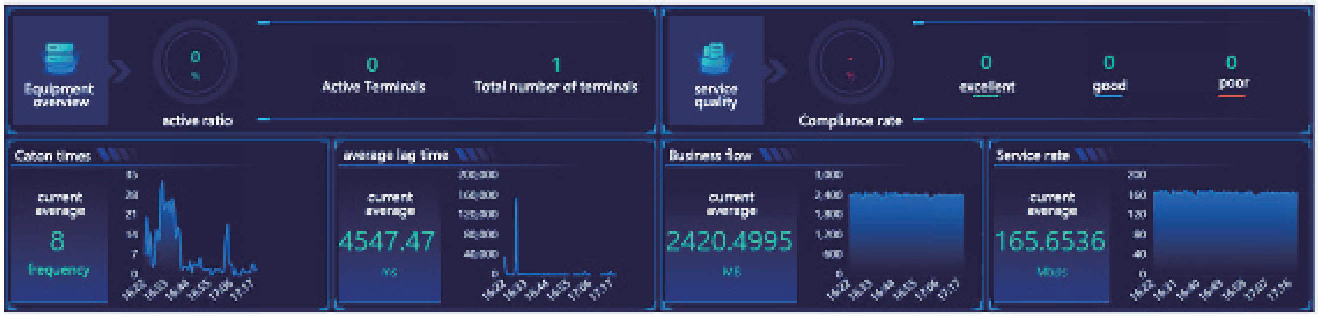


Figure 2.4: Industrial interconnection service quality monitoring indicators

2.3.2 IOT service quality

It can visually analyze and present the relevant performance indicators of IOT Internet of things (mqtt/soap) services in the park, such as service flow, service rate, mqtt link success rate, mqtt link delay, subscription request success rate, ocap response delay, COAP success rate, etc.

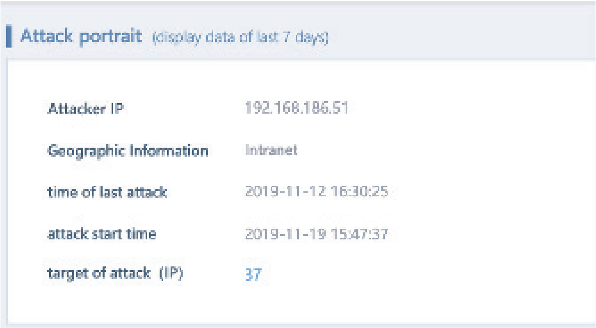
3 Current network practice

3.1 User traffic ranking and traffic analysis

Users are composed of multiple IP addresses or IP address segments. Users can be customized. User behavior analysis is based on users in the network. Analyze users' online behavior from the dimensions of user visit area distribution, user traffic ranking, user activity ranking, network high-risk behavior warning, and bad behavior warning. It supports the top ranking of user traffic access values and the traffic trend chart over time.

3.2 User ID traceability

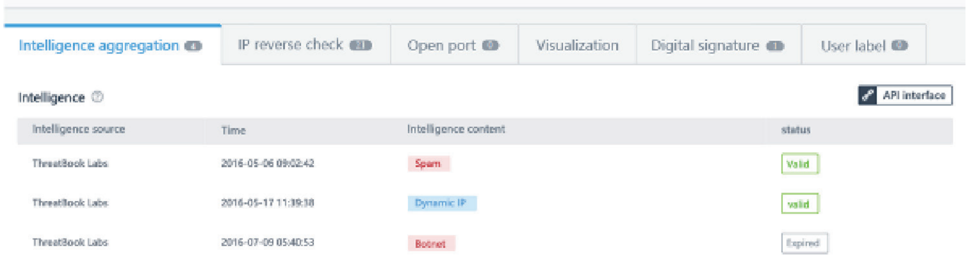
Draw a portrait of the attacker through multiple dimensional information, explore the common means and tools of the attacker, and provide ideas for security protection.


Attack portrait (display data of last 7 days)

Attacker IP	192.168.186.51
Geographic Information	Intranet
time of last attack	2019-11-12 16:30:25
attack start time	2019-11-19 15:47:37
target of attack (IP)	37

Figure 3.1 attack portrait

The effectiveness of the portrait description of the attacker is that it is convenient for security analysts to analyze it from the perspective of entities, including the active time of the attacker, the preferred attack target / website, common attack tools, and the classification of attack types.



Intelligence

Intelligence source	Time	Intelligence content	status
ThreatBook Labs	2016-05-06 09:02:42	Spam	Valid
ThreatBook Labs	2016-05-17 11:39:18	Dynamic IP	valid
ThreatBook Labs	2016-07-09 05:40:53	Botnet	Expired

Figure 3.2 Detailed analysis and conclusion

Judge whether it belongs to a script kid who uses automated tools to attack, or an attacker who has been planning for a long time. It is convenient to grade the risk of personnel and the priority of disposal, such as whether to determine and take effective blocking measures.

3.3 Cloud monitoring of industrial Internet on cloud

By monitoring MEC cloud security resource pool, the following capabilities are realized:

Intensive deployment and reduction of comprehensive cost:

Integration of multiple security capabilities and one hardware device

Independent deployment and cluster deployment

Adapt to elastic expansion on cloud:

On demand, dynamic and flexible deployment of secure network elements

Security service chain arrangement

Adapt to different business security requirements on the cloud

Simple and easy to use, reducing the difficulty of operation and maintenance

Automatic configuration of security policy template

Standardized security cloud service capability

Unified management and multi-dimensional visualization

4 Promotion value

4.1 Product safety value promotion

Based on the self intelligent network capability of the minimal intelligent control private network Butler platform, the network security situation awareness capability is improved. Meet the requirements of network traffic control and anomaly detection, security situational awareness, network management and operation and maintenance in the park side and edge cloud scenarios, and provide customized service capabilities.

4.2 Operation, maintenance and promotion of enabling 5gtob Park

At present, the platform has been launched in Suzhou, Nanjing, Wuxi and Nantong

After the deployment in other cities and regions, the results achieved active end-to-end quality diagnosis, rapid fault demarcation, 7*24 service availability and network quality monitoring in the park, which saved a lot of manpower and material resources, ensured the stability of the customer network, and improved customer satisfaction.

5 summary

This paper establishes an endogenous security protection mechanism to strengthen the new security protection capability based on traffic and the security scheduling capability that moves with the computing network, so as to ensure the security and controllability of the network infrastructure.

Realize the integration and collaboration of cloud, network, edge and end, and provide high-quality edge side network access and self-service, self operation and maintenance, and self-management capabilities;

Realize on-demand drainage and traffic mirroring, and provide network traffic security detection, DDoS, attack detection, security situational awareness and other value-added services for enterprise side edge cloud, private network and other scenarios.

5.1 Main innovations

(1) Traffic collection and signaling surface backfilling: the collected business traffic of enterprise private network user surface is divided into: N3 interface traffic (gtp-u) between GNB and UPF and n6/n9 interface traffic at UPF outlet; Control surface: N4 interface flow of UPF and SMF; The final n3/n4/n6 traffic analysis can realize the backfilling of user data and the binding and association of signaling and user probes.

(2) MEC edge cloud tenant Traffic Association: build the operation and operation and maintenance analysis capability of traffic visualization based on 5g MEC, covering: 1) MEC operation Perception Analysis: SDN network traffic, bandwidth utilization, five tuple analysis and business performance visualization in the tenant level cloud; 2) Open flow visualization and self-service value-added capabilities for 5g MEC Tenants: Tenant owned business and application performance analysis, fault demarcation, etc.

References:

[1] Jun Shen,Guorong Liu, Ming He, 5G private network security requirements analysis and strategy discussion [j]Mobile communications, 2021 (3): 35-39

[2] Shu Zheng’s network security deployment scheme for 5G customized private network [j] Telecom express, 2022 (7): 23-27

[3] Huanyi Mai,Xiaodi Huang , security analysis and Strategy Research of 5g smart steel private network [j]Telecom express, 2022 (1): 18-20

[4] Development and security analysis of chenbaomin 5g private network [j]Electronic technology and software engineering, 2022 (6): 22-25

[5] Chaoyang Li,Pengfei Hu ,HuiFu Zhou , 5G customized private network deployment scheme and security strategy research for data not leaving the park [j] Jiangxi communication technology 2021 (2): 4-7

[6] Jun Wang, Yongchun Tian design of a wide area 5g secure private network for key industry applications [j]Journal of China Academy of Electronic Sciences, 2021 (10): 964-972

[7] Shan Wang, Yong Wang,Yuming Ding, research on the application scheme of in-depth analysis of 5g private network data [j]Post and Telecommunications design technology, 2022 (6): 77-81

[8] Discussion on zhuzhihong 5g enterprise private network UPF construction scheme [j]Communication and information technology, 2022 (1): 81-83

[9] Huamin Fan the development of industry private network in 5g era [j]Post and Telecommunications design technology, 2022 (2): 77-80

[10] Application and Simulation of Zhang Xin and Cheng Min 5g private network in industrial scenes [j]Mobile communications, 2022 (8): 81-85

[11] Application and Simulation of 5g private network in industrial scenes by Zhou Xin, Songyang, liukunyao [j]China new communications, 2021 (7): 117-118

[12] Li Shuang, Guo Zhongzhi, Wang Shuai, 5g network edge cloud solution for industrial Internet demand [j]Post and Telecommunications design technology, 2022 (2): 81-87

[13] Mai Huanyi, Huang Xiaodi, et al. Research on safety protection of 5g+ industrial control system under Bao 2.0 [j]Telecom express, 2022 (4): 14-17

[14] Liguole on the opportunities and challenges of 5g private network development [j]Communication world, 2021 (5): 37-39

[15] Sun Xi, Tian Lin, Li Dawei research status of 5g based private network security [j]Journal of command and control, 2020 (4): 299-309