```
================================================================================
FIREWALL LOG ANALYSIS REPORT
================================================================================
Report Generated: 2024-11-16 11:45:19
================================================================================

PART 1: STANDARD ANALYSIS
--------------------------------------------------------------------------------
================================================================================
FIREWALL LOG ANALYSIS REPORT
================================================================================
Report Generated: 2024-11-16 11:45:18
Analysis Period: 2024-11-07 12:55:49 to 2024-11-07 11:56:21
================================================================================

1. EXECUTIVE SUMMARY
--------------------------------------------------------------------------------
Total Records Analyzed: 39,980
Unique Source IPs: 112
Unique Destination IPs: 2,376
Total Data Transferred: 68.97 GB

2. SECURITY ANALYSIS
--------------------------------------------------------------------------------
2.1 Traffic Actions:
        accept: 25,411 (63.6%)
        close: 6,952 (17.4%)
        client-rst: 3,433 (8.6%)
        server-rst: 2,697 (6.7%)
        timeout: 856 (2.1%)
        dns: 413 (1.0%)
        ip-conn: 218 (0.5%)

2.2 Application Risk Distribution:
        elevated: 20,111 (50.3%)
        medium: 7,591 (19.0%)
        low: 1,427 (3.6%)
        high: 579 (1.4%)
        critical: 2 (0.0%)

2.3 High Risk Applications Detected:
        - DNS: 10,694 instances
        - Microsoft.Portal: 1,994 instances
        - Google.Services: 1,899 instances
        - Microsoft.365.Portal: 1,006 instances
```

- Microsoft.Teams: 505 instances
- Windows.Push.Notification: 497 instances
- Slack: 434 instances
- Microsoft.Authentication: 392 instances
- Google.Ads: 259 instances
- WhatsApp_File.Transfer: 245 instances

2.4 DENIED TRAFFIC ANALYSIS

No denied traffic found in the logs.

3. TRAFFIC ANALYSIS

3.1 Top Source IPs by Traffic Volume:
- 172.16.201.2: 23.92 GB
- 172.16.2.27: 4.02 GB
- 172.16.2.2: 3.19 GB
- 172.16.2.17: 1.91 GB
- 172.16.3.94: 1004.86 MB
- 172.16.3.88: 733.27 MB
- 172.16.3.185: 632.06 MB
- 172.16.2.11: 470.57 MB
- 172.16.3.67: 430.84 MB
- 192.168.110.134: 313.12 MB

3.2 Top Destination IPs by Traffic Volume:
- 122.184.73.135: 19.28 GB
- 163.116.219.35: 6.57 GB
- 8.37.110.90: 2.34 GB
- 8.37.109.130: 490.72 MB
- 8.8.8.8: 285.76 MB
- 173.243.132.34: 260.39 MB
- 152.195.38.76: 156.29 MB
- 108.158.251.107: 149.14 MB
- 104.114.99.48: 126.27 MB
- 108.159.15.119: 122.41 MB

3.3 Top Services:
- HTTPS: 18,100 connections
- DNS: 16,208 connections
- udp/443: 1,505 connections
- HTTP: 754 connections
- tcp/5719: 740 connections
- PING: 567 connections
- tcp/853: 326 connections

tcp/5228: 217 connections
tcp/5091: 145 connections
udp/6000: 128 connections

4. GEOGRAPHIC ANALYSIS

4.1 Top Destination Countries:
United States: 30,916 connections
India: 5,250 connections
Singapore: 1,030 connections
France: 548 connections
Korea, Republic of: 284 connections
Russian Federation: 274 connections
Ireland: 241 connections
Japan: 239 connections
Netherlands: 209 connections
Germany: 201 connections

5. APPLICATION ANALYSIS

5.1 Application Categories:
Network.Service: 12,151 (30.4%)
unscanned: 7,598 (19.0%)
Collaboration: 6,392 (16.0%)
Web.Client: 4,312 (10.8%)
General.Interest: 3,553 (8.9%)
unknown: 2,041 (5.1%)
Social.Media: 789 (2.0%)
P2P: 577 (1.4%)
Video/Audio: 484 (1.2%)
Email: 429 (1.1%)
Business: 381 (1.0%)
Update: 319 (0.8%)
Storage.Backup: 222 (0.6%)
Cloud.IT: 95 (0.2%)
Proxy: 2 (0.0%)
Remote.Access: 2 (0.0%)
Game: 2 (0.0%)

5.2 Top Applications:
DNS: 10,694 connections
HTTPS.BROWSER: 3,997 connections
Microsoft.Portal: 1,994 connections
Google.Services: 1,899 connections
Zoom: 1,048 connections

Microsoft.365.Portal: 1,006 connections
QUIC: 681 connections
Facebook: 617 connections
BitTorrent: 577 connections
Microsoft.Teams: 505 connections

5.3 Detailed Application Analysis:

Application: DNS
Total Traffic: 5.44 MB
Top Source IPs:
- 172.16.2.11: 303.0 connections (26.83 KB)
- 172.16.2.17: 1.0 connections (84.00 B)
- 172.16.3.127: 43.0 connections (2.93 KB)
- 172.16.3.185: 575.0 connections (41.60 KB)
- 172.16.3.190: 3.0 connections (212.00 B)
Top Destination IPs:
- 1.1.1.1: 10.0 connections (1.26 KB)
- 117.96.122.70: 2.0 connections (0.00 B)
- 122.175.1.5: 3.0 connections (0.00 B)
- 192.168.29.1: 10.0 connections (0.00 B)
- 208.67.222.222: 5.0 connections (638.00 B)

Application: HTTPS.BROWSER
Total Traffic: 2.14 GB
Top Source IPs:
- 172.16.2.10: 2.0 connections (11.37 KB)
- 172.16.2.11: 82.0 connections (1.29 MB)
- 172.16.2.14: 6.0 connections (383.31 KB)
- 172.16.2.16: 4.0 connections (68.20 KB)
- 172.16.2.17: 48.0 connections (3.51 MB)
Top Destination IPs:
- 100.20.76.137: 1.0 connections (16.12 KB)
- 100.29.154.62: 2.0 connections (28.20 KB)
- 103.103.196.92: 26.0 connections (349.73 KB)
- 103.103.196.94: 2.0 connections (32.29 KB)
- 103.166.216.43: 30.0 connections (8.32 MB)

Application: Microsoft.Portal
Total Traffic: 292.78 MB
Top Source IPs:
- 172.16.2.11: 81.0 connections (1.73 MB)

- 172.16.2.27: 4.0 connections (4.63 KB)
- 172.16.3.185: 104.0 connections (3.43 MB)
- 172.16.3.190: 1.0 connections (10.39 KB)
- 172.16.3.25: 29.0 connections (623.69 KB)

Top Destination IPs:

- 104.114.110.196: 7.0 connections (124.46 KB)
- 104.114.85.198: 30.0 connections (9.61 MB)
- 104.114.94.26: 28.0 connections (271.17 KB)
- 104.114.99.48: 2.0 connections (126.27 MB)
- 104.208.16.88: 14.0 connections (207.66 KB)

Application: Google.Services
Total Traffic: 85.92 MB
Top Source IPs:

- 172.16.3.185: 3.0 connections (4.41 KB)
- 172.16.3.67: 6.0 connections (13.94 KB)
- 172.16.3.87: 19.0 connections (54.09 KB)
- 172.16.3.88: 167.0 connections (1.39 MB)
- 192.168.110.105: 202.0 connections (2.47 MB)

Top Destination IPs:

- 142.250.113.94: 13.0 connections (174.64 KB)
- 142.250.114.94: 3.0 connections (50.42 KB)
- 142.250.115.94: 2.0 connections (33.85 KB)
- 142.250.138.94: 18.0 connections (296.31 KB)
- 142.250.181.10: 13.0 connections (1.11 MB)

Application: Zoom
Total Traffic: 88.02 MB
Top Source IPs:

- 172.16.2.11: 141.0 connections (2.13 MB)
- 172.16.2.17: 145.0 connections (11.46 MB)
- 172.16.2.2: 90.0 connections (15.45 MB)
- 172.16.3.185: 309.0 connections (3.99 MB)
- 172.16.3.67: 194.0 connections (1.89 MB)

Top Destination IPs:

- 134.224.0.55: 1.0 connections (4.60 KB)
- 162.12.233.230: 21.0 connections (2.43 MB)
- 162.12.233.244: 122.0 connections (4.67 MB)
- 162.12.235.201: 2.0 connections (51.51 KB)
- 170.114.1.180: 16.0 connections (159.30 KB)

Application: Microsoft.365.Portal

Total Traffic: 217.19 MB
Top Source IPs:
- 172.16.2.11: 29.0 connections (102.49 KB)
- 172.16.2.27: 5.0 connections (55.01 KB)
- 172.16.3.185: 74.0 connections (307.05 KB)
- 172.16.3.190: 1.0 connections (1.42 KB)
- 172.16.3.25: 3.0 connections (3.98 KB)

Top Destination IPs:
- 104.114.108.161: 2.0 connections (129.22 KB)
- 104.114.68.220: 4.0 connections (3.07 MB)
- 104.114.92.239: 2.0 connections (150.86 KB)
- 104.114.99.5: 2.0 connections (24.33 KB)
- 104.211.140.135: 1.0 connections (14.31 KB)

Application: QUIC
Total Traffic: 232.16 MB
Top Source IPs:
- 172.16.2.11: 8.0 connections (639.75 KB)
- 172.16.3.185: 4.0 connections (335.96 KB)
- 172.16.3.67: 8.0 connections (45.13 KB)
- 172.16.3.81: 2.0 connections (9.89 KB)
- 172.16.3.87: 14.0 connections (441.75 KB)

Top Destination IPs:
- 104.17.24.14: 6.0 connections (102.28 KB)
- 104.18.35.28: 1.0 connections (3.60 KB)
- 104.18.41.158: 2.0 connections (7.20 KB)
- 104.18.43.204: 1.0 connections (3.60 KB)
- 104.21.90.38: 1.0 connections (3.60 KB)

Application: Facebook
Total Traffic: 6.37 MB
Top Source IPs:
- 192.168.110.108: 3.0 connections (11.78 KB)
- 192.168.110.125: 272.0 connections (1.22 MB)
- 192.168.110.136: 342.0 connections (525.84 KB)

Top Destination IPs:
- 116.119.125.146: 16.0 connections (79.64 KB)
- 116.119.195.82: 43.0 connections (212.71 KB)
- 116.119.77.211: 16.0 connections (79.79 KB)
- 116.119.85.146: 16.0 connections (79.61 KB)
- 157.240.13.10: 7.0 connections (53.42 KB)

Application: BitTorrent
Total Traffic: 291.48 KB
Top Source IPs:
- 192.168.110.154: 577.0 connections (78.08 KB)
Top Destination IPs:
- 101.179.201.185: 1.0 connections (0.00 B)
- 101.32.244.116: 1.0 connections (0.00 B)
- 101.51.92.211: 4.0 connections (0.00 B)
- 104.21.0.111: 1.0 connections (105.40 KB)
- 105.97.149.143: 2.0 connections (0.00 B)

Application: Microsoft.Teams
Total Traffic: 44.62 MB
Top Source IPs:
- 172.16.2.11: 51.0 connections (503.97 KB)
- 172.16.3.185: 31.0 connections (533.52 KB)
- 172.16.3.25: 4.0 connections (17.46 KB)
- 172.16.3.67: 41.0 connections (603.73 KB)
- 172.16.3.88: 30.0 connections (484.63 KB)
Top Destination IPs:
- 52.112.100.52: 2.0 connections (7.57 KB)
- 52.112.120.216: 29.0 connections (5.17 MB)
- 52.112.124.220: 1.0 connections (9.12 KB)
- 52.112.127.48: 1.0 connections (18.46 KB)
- 52.112.39.36: 2.0 connections (13.95 KB)

6. POLICY ANALYSIS

6.1 Policy Usage:

- EM-EMP _ Virtual Link: 22,826 hits
- EM-GSC to Virtual Link: 7,646 hits
- Airtel_ext: 7,055 hits
- InternalLAN: 1,717 hits
- CCTV _ internet: 736 hits

6.2 Detailed Policy Analysis:

Policy: EM-EMP _ Virtual Link
Total Traffic: 2.74 GB
Most Active Source IPs:
- 192.168.110.105: 2,297.0 hits (178.74 MB)
- 192.168.110.108: 2,229.0 hits (115.52 MB)
- 192.168.110.113: 2.0 hits (5.16 KB)

- 192.168.110.114: 2,043.0 hits (261.20 MB)
- 192.168.110.125: 1,362.0 hits (8.40 MB)

Most Accessed Applications:
- DNS: 7,677 times
- HTTPS.BROWSER: 2,412 times
- Google.Services: 1,704 times
- Microsoft.Portal: 1,197 times
- Microsoft.365.Portal: 756 times

Traffic by Risk Level:
- elevated: 14,636 connections
- medium: 4,648 connections
- low: 1,179 connections
- high: 579 connections
- critical: 2 connections

Policy: EM-GSC to Virtual Link
Total Traffic: 9.88 GB
Most Active Source IPs:
- 172.16.3.10: 8.0 hits (187.02 KB)
- 172.16.3.100: 17.0 hits (906.25 KB)
- 172.16.3.101: 20.0 hits (862.23 KB)
- 172.16.3.103: 5.0 hits (330.03 KB)
- 172.16.3.104: 6.0 hits (38.25 KB)

Most Accessed Applications:
- DNS: 2,713 times
- HTTPS.BROWSER: 1,294 times
- Microsoft.Portal: 712 times
- Zoom: 672 times
- Microsoft.365.Portal: 216 times

Traffic by Risk Level:
- elevated: 4,776 connections
- medium: 2,132 connections
- low: 207 connections

Policy: Airtel_ext
Total Traffic: 24.55 GB
Most Active Source IPs:
- 172.16.201.2: 7,055.0 hits (23.92 GB)

Most Accessed Applications:
Traffic by Risk Level:

Policy: InternalLAN

Total Traffic: 31.64 GB
Most Active Source IPs:
- 172.16.2.10: 2.0 hits (11.37 KB)
- 172.16.2.11: 935.0 hits (470.57 MB)
- 172.16.2.14: 6.0 hits (383.31 KB)
- 172.16.2.16: 4.0 hits (68.20 KB)
- 172.16.2.17: 369.0 hits (1.91 GB)

Most Accessed Applications:
- Zoom: 376 times
- DNS: 304 times
- HTTPS.BROWSER: 291 times
- Windows.Push.Notification: 96 times
- Microsoft.Portal: 85 times

Traffic by Risk Level:
- medium: 811 connections
- elevated: 699 connections
- low: 41 connections

Policy: CCTV _ internet
Total Traffic: 170.80 MB
Most Active Source IPs:
- 192.168.20.100: 130.0 hits (5.46 MB)
- 192.168.20.49: 504.0 hits (52.70 MB)
- 192.168.20.50: 102.0 hits (55.19 MB)

Most Accessed Applications:
Traffic by Risk Level:

7. SECURITY RECOMMENDATIONS

---

1. Review and potentially restrict high-risk applications: DNS, Microsoft.Authentication, Microsoft.365.Portal
2. Review traffic on unusual ports: 10033, 1024, 10240, 10769, 1085
3. Consider implementing geographic-based access controls for international traffic
4. Review wireless coverage due to detected weak signal strengths
5. Regularly review and update security policies
6. Implement detailed logging for critical systems
7. Consider implementing network segmentation
8. Review and optimize policy configuration regularly

8. POTENTIAL SECURITY CONCERNS

- Detected 20111 forwarded connections using high-risk applications
- Identified 297 instances of abnormally high forward traffic volume
- Detected forward traffic to potentially suspicious countries: China

==
END OF REPORT
==

PART 2: AI-POWERED INSIGHTS

Security Analysis:
AI security analysis not available

Traffic Analysis:
AI traffic analysis not available

==
END OF REPORT
==