Enthüllung der Netzwerkintelligenz:

Nutzung von GFI ClearView zur Verbesserung der GFI KerioControl-Richtlinien

GFI Software™

Einführung

In der heutigen dynamischen und vernetzten digitalen Landschaft sind effektives Netzwerkmanagement und Sicherheit von größter Bedeutung. Das komplexe Zusammenspiel zwischen der Gewinnung von Echtzeiteinblicken in Netzwerkaktivitäten und der zeitnahen Umsetzung dieser Erkenntnisse in entscheidende Maßnahmen steht im Mittelpunkt der modernen Cybersicherheit. Dieses Dokument beleuchtet die kraftvolle symbiotische Beziehung zwischen zwei hochmodernen Lösungen: GFI ClearView und GFI KerioControl.

Beispielanwendungsfälle

Eine effiziente Bandbreitennutzung hängt von zwei wesentlichen Maßnahmen ab:

1. Festlegung von Bandbreitenschwellen für uneingeschränkten Datenverkehr – sei es benutzerspezifisch oder unternehmensweit.
2. Einrichtung von Bandbreitenreservierungen für geschäftskritische Anwendungen.

#1 Kontrolle von Durchsatzspitzen durch nicht-kritische Anwendungen

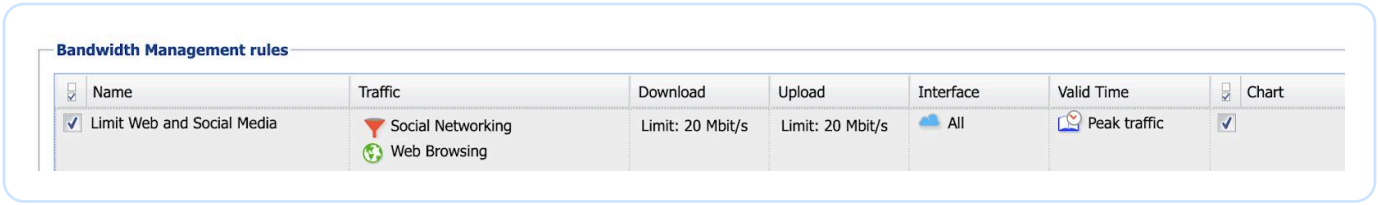
Top 30 Inbound Application Groups

Name [-] Hide Details	Packets	Data (MB)	Throughput (kbps) Average	Throughput (kbps) Max	Flows	RTT (ms)
GFI Products	1362698153	1919432.337	473.03	614040.34	1653	128
Social Networking	240479290	300250.544	933.77	29746.08	547	134
Web	446026750	206028.255	46.15	335043.23	17188	132

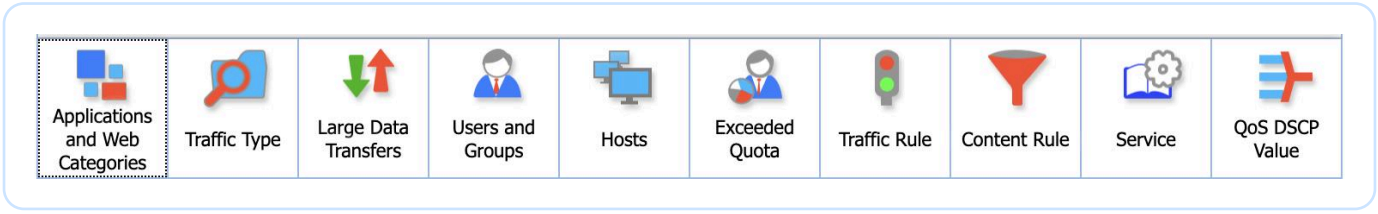
Wie im obigen GFI ClearView-Bild dargestellt, wiesen die drei wichtigsten eingehenden Anwendungsgruppen folgende Spitzenwerte für die Durchsatznutzung auf (Durchsatz in kbps - maximal):

- 614 Mbps - GFI Produkte
- 29 Mbps - Soziale Netzwerke
- 335 Mbps - Web

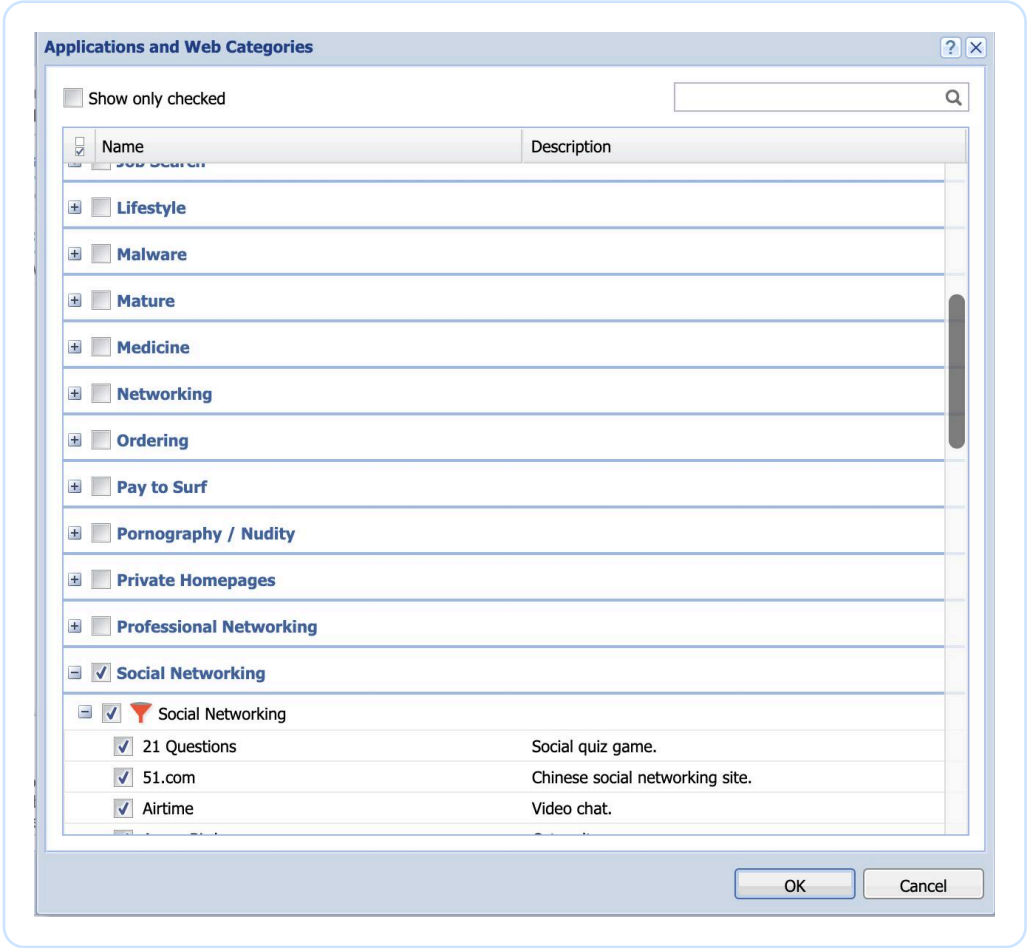
Dies deutet darauf hin, dass während der Spitzenlasten kritische Anwendungen aufgrund der Last, die durch diese nicht-kritischen Anwendungen verursacht wurde, unter Leistungseinbußen leiden könnten. Um dem entgegenzuwirken, kann eine QoS-Richtlinie innerhalb von KerioControl konfiguriert werden, insbesondere während der Spitzenzeiten. Folgendes stellt eine Beispielrichtlinie dar:



Es ist wichtig zu beachten, dass das obige Beispiel nur drei Kategorien zeigt, während eine reale Umgebung mehrere Anwendungstypen umfassen würde. GFI KerioControl verwaltet diese Komplexität nahtlos und kann Tausende von Anwendungen und Websites identifizieren. Es erleichtert die Erstellung von QoS-Richtlinien über verschiedene Kategorien hinweg.



Innerhalb der Anwendungs- und Webkategorien stehen Ihnen über 140 Kategorien (P2P, Streaming, Musik, Fernsehen, soziale Netzwerke usw.) zur Verfügung, jede mit Dutzenden von einzelnen Anwendungen und Websites.



#1.1 Verbesserung des obigen Szenarios

Häufig stammen Fälle unerwünschten Verhaltens – wie übermäßige Nutzung sozialer Netzwerke – von einer Handvoll Anwendungen oder Benutzer. Die interaktiven Grafiken von GFI ClearView ermöglichen eine tiefere Untersuchung solcher Verhaltensweisen. Wenn Sie beispielsweise auf "Soziale Netzwerke" klicken, können Sie spezifische problematische Anwendungen innerhalb dieser Gruppe aufdecken und weiter die Benutzer oder Hosts identifizieren, die übermäßig aktiv sind.

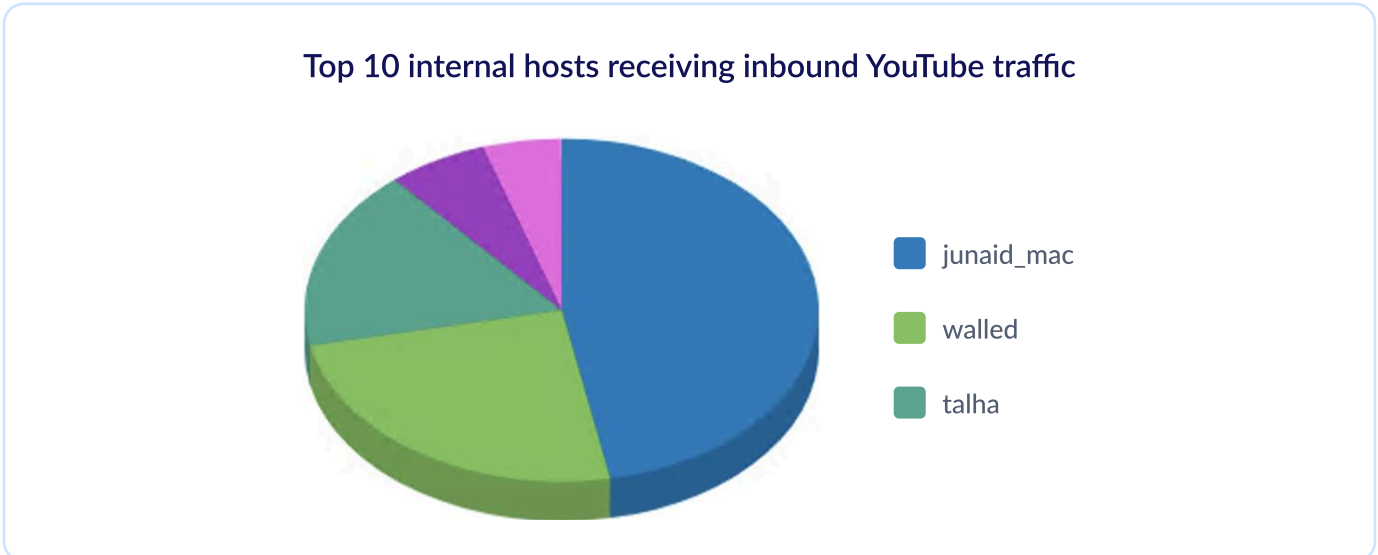
Top 30 Inbound Application Groups

Name [-] Hide Details	Packets	Data (MB)	Throughput (kbps) Average	Throughput (kbps) Max	Flows	RTT (ms)
GFI Products	1362698153	1919432.337	473.03	614040.34	1653	128
Social Networking	240479290	300250.544	933.77	29746.08	547	134
Web	446026750	206028.255	46.15	335043.23	17188	132

Top 30 Inbound Applications in Group Social Networking

Name [+] Show Details	Packets	Data (MB)	Throughput (kbps) Average	Throughput (kbps) Max	Flows
YouTube (udp)	240305670	300093.384	963.45	29746.08	464
Twitter	86144	52.228	5.42	1089.86	39
Snapchat (udp)	37443	49.479	506.17	3771.44	8
Instagram (udp)	39279	45.374	576.70	2323.03	5
LinkedIn	9090	8.754	60.19	845.84	18
Facebook Chat (udp)	707	0.792	51.10	119.90	5
Facebook	957	0.532	5.51	47.38	8

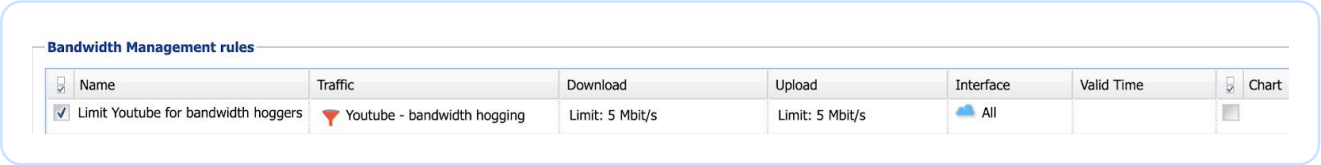
Die Daten zeigen, dass YouTube als Hauptverursacher von Spitzen auftritt und 99 % der Nutzung sozialer Netzwerke ausmacht. Eine genauere Betrachtung zeigt, dass 80 % dieser Nutzung von nur drei Benutzern stammen.



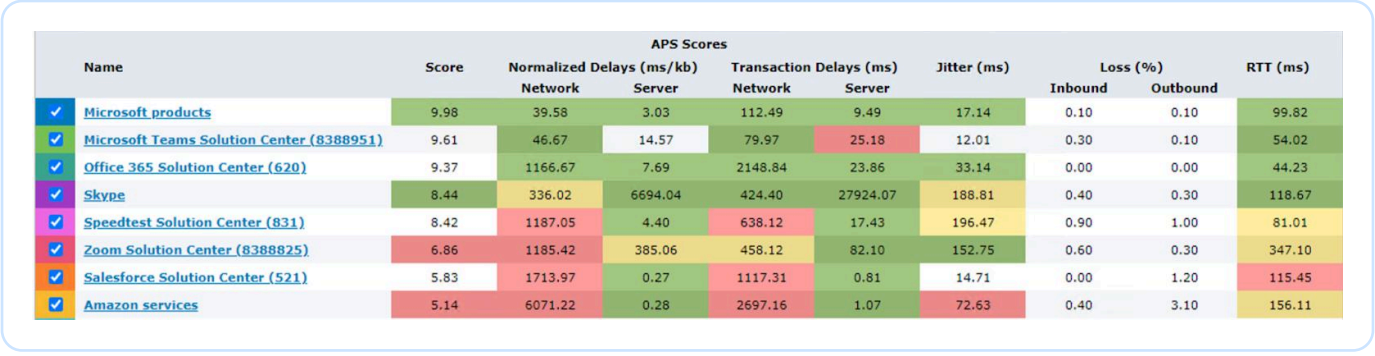
In diesem Szenario kann eine maßgeschneiderte Richtlinie für die Nutzung von YouTube durch diese spezifischen Hosts innerhalb von KerioControl durch die folgenden Schritte erreicht werden:

- Erstellen Sie eine Inhaltsfilterregel:

- Richten Sie eine entsprechende QoS-Richtlinie unter Verwendung der zuvor erstellten Inhaltsregel ein:

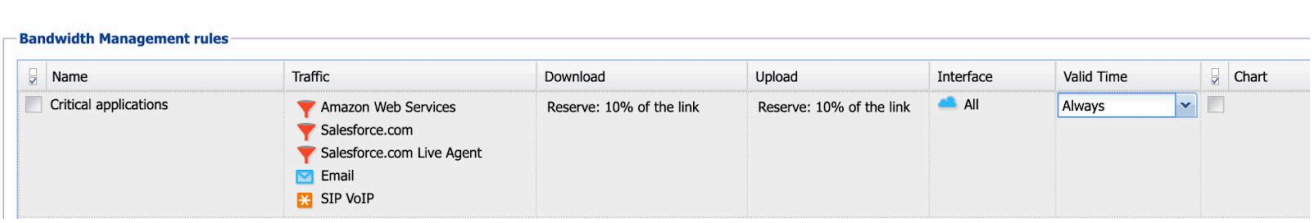


#2 Reservierung von Durchsatz für kritische Anwendungen



Name	Score	APS Scores: Normalized Delays (ms/kb) Network	Normalized Delays (ms/kb) Server	Transaction Delays (ms) Network	Transaction Delays (ms) Server	Jitter (ms)	Loss (%) Inbound	Loss (%) Outbound	RTT (ms)
Microsoft products	9.98	39.58	3.03	112.49	9.49	17.14	0.10	0.10	99.82
Microsoft Teams Solution Center (8388951)	9.61	46.67	14.57	79.97	25.18	12.01	0.30	0.10	54.02
Office 365 Solution Center (620)	9.37	1166.67	7.69	2148.84	23.86	33.14	0.00	0.00	44.23
Skype	8.44	336.02	6694.04	424.40	27924.07	188.81	0.40	0.30	118.67
Speedtest Solution Center (831)	8.42	1187.05	4.40	638.12	17.43	196.47	0.90	1.00	81.01
Zoom Solution Center (8388825)	6.86	1185.42	385.06	458.12	82.10	152.75	0.60	0.30	347.10
Salesforce Solution Center (521)	5.83	1713.97	0.27	1117.31	0.81	14.71	0.00	1.20	115.45
Amazon services	5.14	6071.22	0.28	2697.16	1.07	72.63	0.40	3.10	156.11

Wie im GFI ClearView-Bild dargestellt, zeigen Salesforce- und Amazon-Dienste eine suboptimale Anwendungsleistung und erhalten eine Bewertung von 5 von 10. Dies kann wahrscheinlich auf unzureichende verfügbare Bandbreite während der Spitzenzeiten zurückgeführt werden, die größtenteils durch weniger kritische Anwendungen verursacht wird, die Ressourcen verbrauchen. Mildern Sie dieses Problem, indem Sie eine dedizierte QoS-Richtlinie innerhalb von KerioControl konfigurieren:



Ebenso können Sie Richtlinien für andere kritische Anwendungen wie E-Mail, SIP VoIP-Verkehr, Videokonferenz-Tools usw. konfigurieren. Es ist wichtig zu beachten, dass Sie dies auch nutzen können, um Bandbreite für benutzerdefinierte Anwendungen oder Dienste zu reservieren, die Sie möglicherweise der Öffentlichkeit anbieten. In einem solchen Fall können Sie, wenn Sie eine Verkehrsregel haben, die NAT für Ihr DMZ durchführt, Bandbreite für alle Daten reservieren, die unter diese Verkehrsregel fallen.

Fazit

So wie ein Orchester sowohl Vision als auch Ausführung benötigt, um ein Meisterwerk zu schaffen, erfordert auch die Netzwerksicherheit die Zusammenarbeit dieser beiden außergewöhnlichen Lösungen. Der wachsame Blick von GFI ClearView identifiziert Schwachstellen und Muster, während die schnellen Reaktionen von GFI KerioControl sicherstellen, dass der Rhythmus des Netzwerks ununterbrochen bleibt. Dieses dynamische Duo schützt nicht nur vor Bedrohungen, sondern befähigt auch Administratoren, eine Spitzenleistung zu orchestrieren und ein Netzwerk zu gewährleisten, das im Rampenlicht gedeiht. Gemeinsam verkörpern GFI ClearView und GFI KerioControl die Synergie von Einsicht und Handlung und schaffen ein geschütztes, leistungsstarkes Netzwerk, das als Zeugnis für moderne Cybersicherheitsexzellenz steht.

Testen Sie GFI ClearView 30 Tage kostenlos →

GFI Software™