



SANGFOR



NGAF

Best Practices for Scenarios_Bandwidth Management

Version 8.0.17



Change Log

Date	Change Description
July 13, 2020	Version 8.0.17 document release.
May 17, 2021	Document update.

CONTENT

Chapter 1 Scenario	1
Chapter 2 Basic Configuration	1
Chapter 3 Advanced Configuration	3

Chapter 1 Scenario

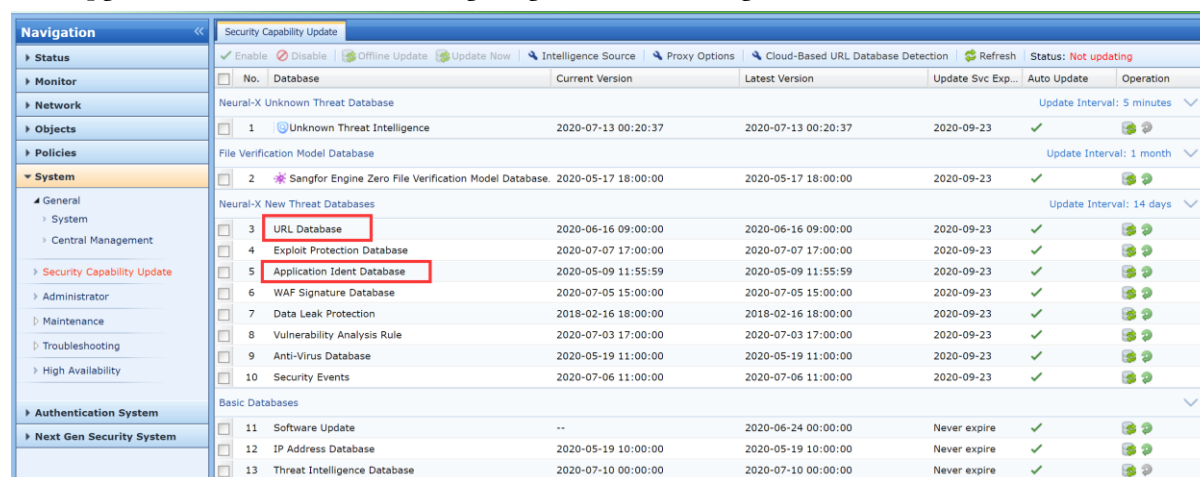
A small and medium-sized enterprise has limited network bandwidth, and increasing the bandwidth requires more costs. A large number of people on the network currently browse Youtube during work hours, which results in low work efficiency and at the same time online video takes up a lot of bandwidth. Customers want to optimize bandwidth use.

The difference between limited bandwidth and guaranteed bandwidth:

The guaranteed channel is based on the guaranteed minimum bandwidth value. In the case of high bandwidth usage, the priority of high bandwidth usage is guaranteed. The guaranteed bandwidth is suitable for users with high priority, such as management; or web browsing, mail, office OA and other priorities High application. Limited channel mainly limit the maximum bandwidth available to users, and are suitable for ordinary employees or low-priority applications such as downloads and p2p.

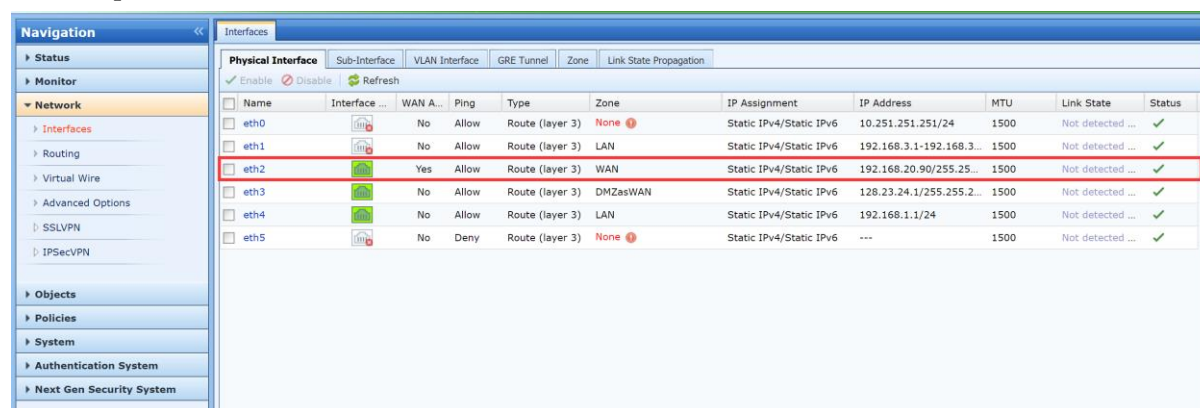
Chapter 2 Basic Configuration

1. Bandwidth management uses a database to identify application, so make sure that the database has been upgraded to the latest before configuring bandwidth management.



No.	Database	Current Version	Latest Version	Update Svc Exp...	Auto Update	Operation
Neural-X Unknown Threat Database						
1	Unknown Threat Intelligence	2020-07-13 00:20:37	2020-07-13 00:20:37	2020-09-23	✓	
File Verification Model Database						
2	Sangfor Engine Zero File Verification Model Database	2020-05-17 18:00:00	2020-05-17 18:00:00	2020-09-23	✓	
Neural-X New Threat Databases						
3	URL Database	2020-06-16 09:00:00	2020-06-16 09:00:00	2020-09-23	✓	
4	Exploit Protection Database	2020-07-07 17:00:00	2020-07-07 17:00:00	2020-09-23	✓	
5	Application Ident Database	2020-05-09 11:55:59	2020-05-09 11:55:59	2020-09-23	✓	
6	WAF Signature Database	2020-07-05 15:00:00	2020-07-05 15:00:00	2020-09-23	✓	
7	Data Leak Protection	2018-02-16 18:00:00	2018-02-16 18:00:00	2020-09-23	✓	
8	Vulnerability Analysis Rule	2020-07-03 17:00:00	2020-07-03 17:00:00	2020-09-23	✓	
9	Anti-Virus Database	2020-05-19 11:00:00	2020-05-19 11:00:00	2020-09-23	✓	
10	Security Events	2020-07-06 11:00:00	2020-07-06 11:00:00	2020-09-23	✓	
Basic Databases						
11	Software Update	--	2020-06-24 00:00:00	Never expire	✓	
12	IP Address Database	2020-05-19 10:00:00	2020-05-19 10:00:00	Never expire	✓	
13	Threat Intelligence Database	2020-07-10 00:00:00	2020-07-10 00:00:00	Never expire	✓	

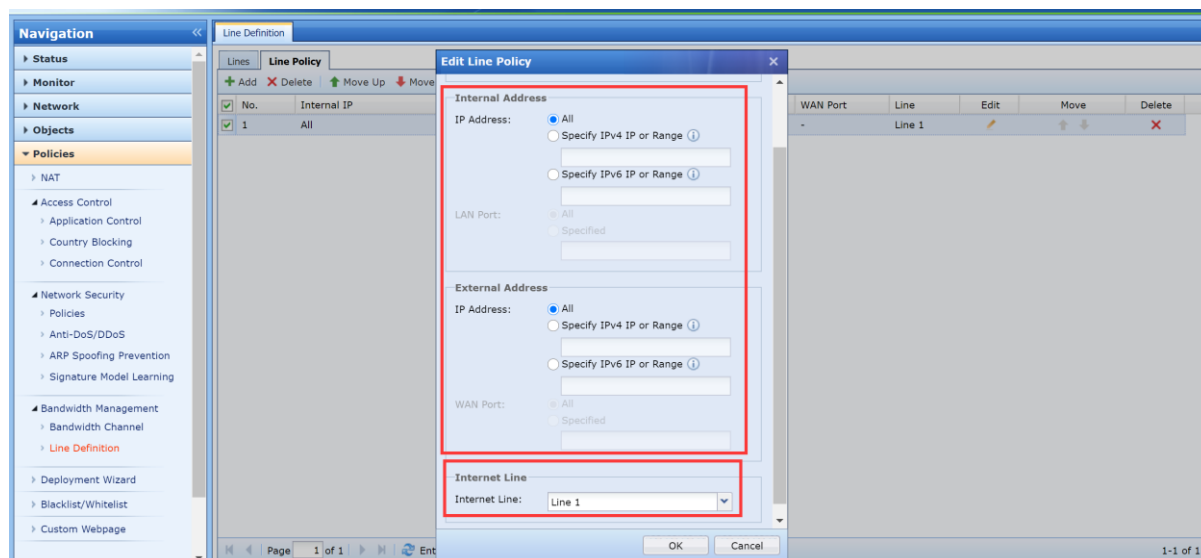
2. Check the network port configuration, determine which port is the WAN port and check whether the "WAN attribute" is checked. When configuring the line for bandwidth management, you **can only select** network ports with "WAN attribute".



Name	Interface	WAN A..	Ping	Type	Zone	IP Assignment	IP Address	MTU	Link State	Status
eth0		No	Allow	Route (layer 3)	None	Static IPv4/Static IPv6	10.251.251.251/24	1500	Not detected ...	✓
eth1		No	Allow	Route (layer 3)	LAN	Static IPv4/Static IPv6	192.168.3.1-192.168.3...	1500	Not detected ...	✓
eth2		Yes	Allow	Route (layer 3)	WAN	Static IPv4/Static IPv6	192.168.20.90/255.25...	1500	Not detected ...	✓
eth3		No	Allow	Route (layer 3)	DMZasWAN	Static IPv4/Static IPv6	128.23.24.1/255.255.2...	1500	Not detected ...	✓
eth4		No	Allow	Route (layer 3)	LAN	Static IPv4/Static IPv6	192.168.1.1/24	1500	Not detected ...	✓
eth5		No	Deny	Route (layer 3)	None	Static IPv4/Static IPv6	---	1500	Not detected ...	✓

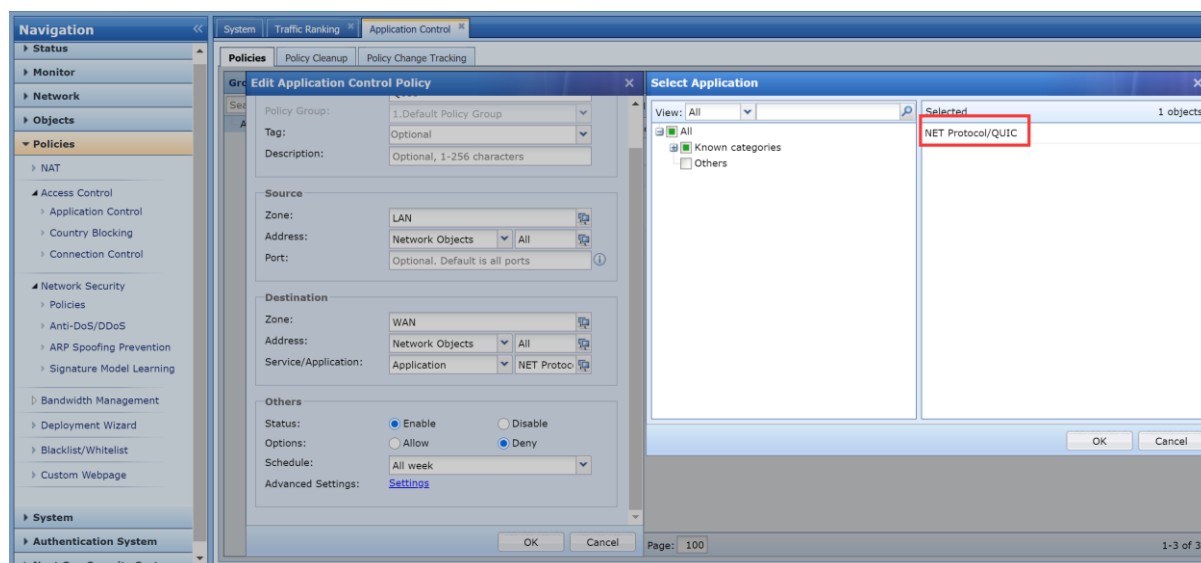
Only network ports configured with WAN attributes can be selected.

3. After the line is created, you need to configure the line policy to define the line.



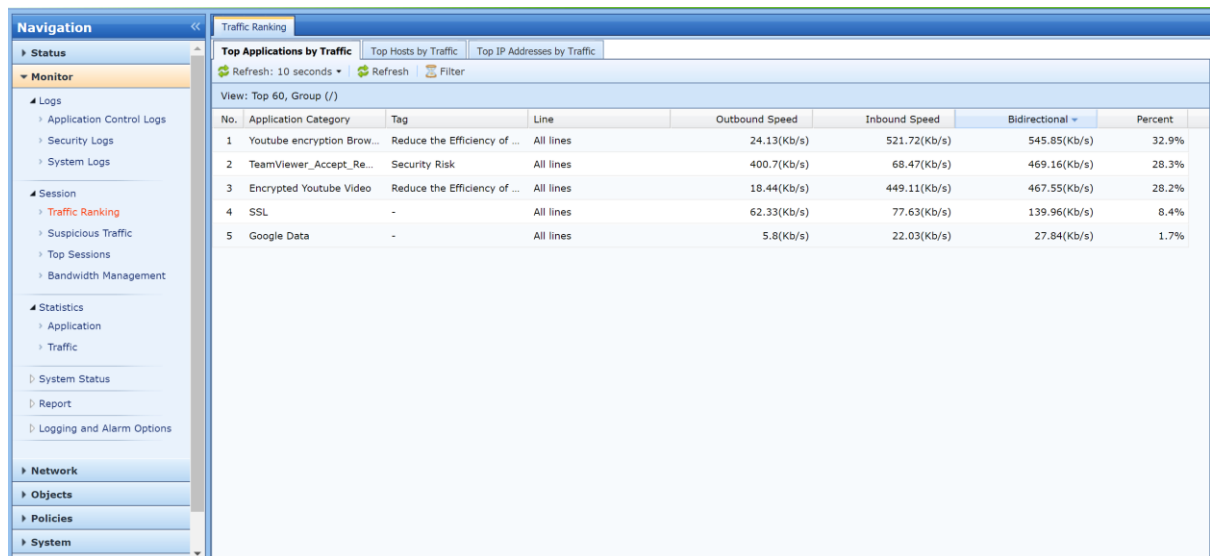
Chapter 3 Advanced Configuration

1. Now some websites use the QUIC protocol, and the current device cannot decrypt the QUIC protocol or even recognize the URL in the data packet, so it is recommended to block the QUIC protocol during testing. After deny the QUIC protocol, the browser will automatically negotiate to use the https protocol for data interaction.

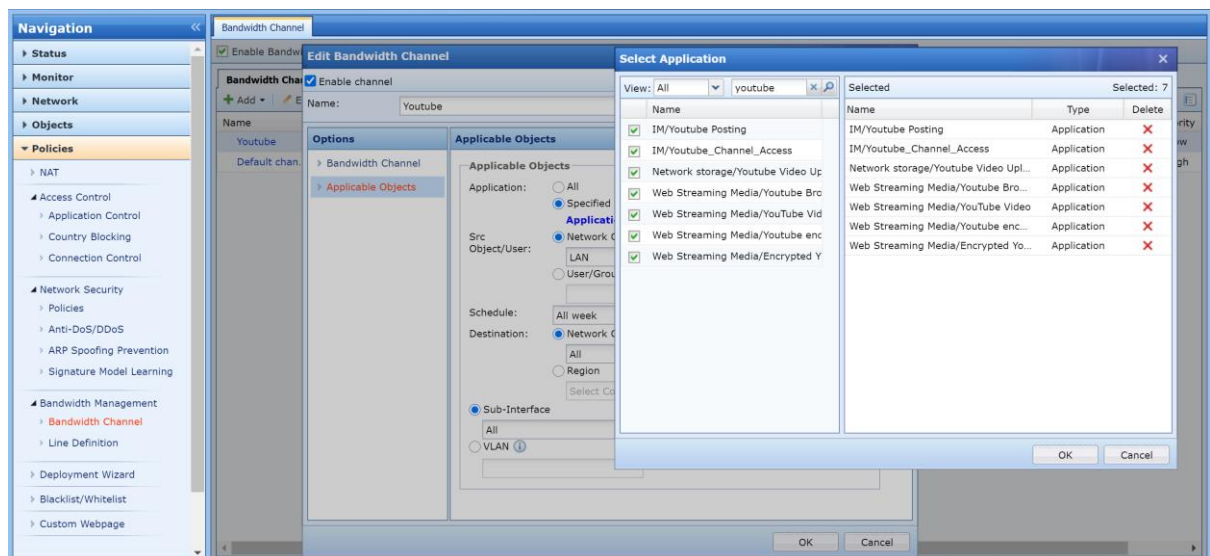


2. The **most important point** is to see which rules the application traffic is recognized by NGAF. Only then can the application rules be selected in the bandwidth management policy.

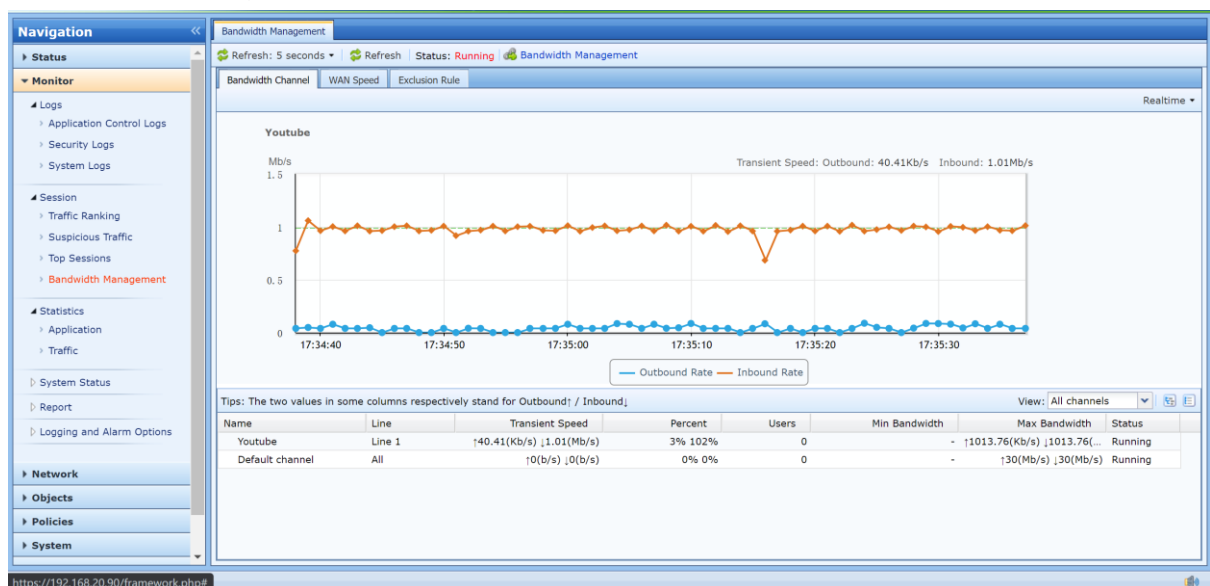
Bandwidth Management



Select the corresponding application rule in the bandwidth management policy.



Then check the traffic status to see if the traffic has entered the flow control channel corresponding to the bandwidth management policy.





SANGFOR

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc