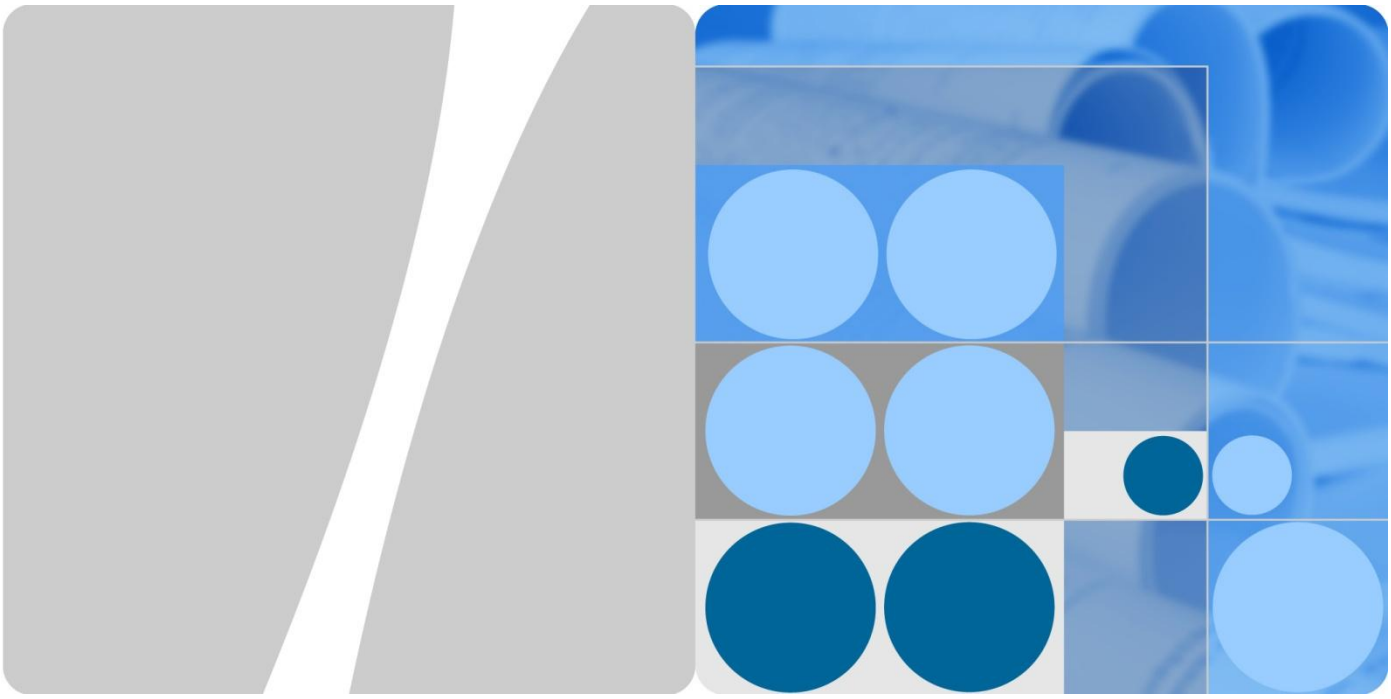


USG6000 Series Next Generation Firewall Intelligent Uplink Selection

Technical White Paper

Issue V1.1

Date 2014-06-18

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2014. 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 Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. 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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Keyword:

NGFW

Abstract:

This document describes the principle and solution of the intelligent uplink selection technology for Huawei NGFW.

Abbreviation	Full Spelling
NGFW	Next Generation Firewall

Copyright © Huawei Technologies Co., Ltd.

Contents

Copyright © Huawei Technologies Co., Ltd.

1 Technical Background

The rapid development of computer network technologies and e-commerce brings huge and deep impacts on various aspects of the human society. To provide better network access services, enterprises lease links from carriers to prevent risks due to the single link failure and obtain more bandwidth resources.

The traditional method of combining common routes and policy-based routing meets the requirement of multi-carrier link access to a certain extent. However, this method is complicated and cannot be dynamically adjusted based on network structure changes. On such a network, packets cannot intelligently select links.

Copyright © Huawei Technologies Co., Ltd.

2 Concepts and Principles

2.1 Intelligent Uplink Selection

On a network with links provided by different carriers, the bandwidth, access quality, and destination network segment may vary with links. Consequently, the link usage is low or the access quality is unsatisfactory.

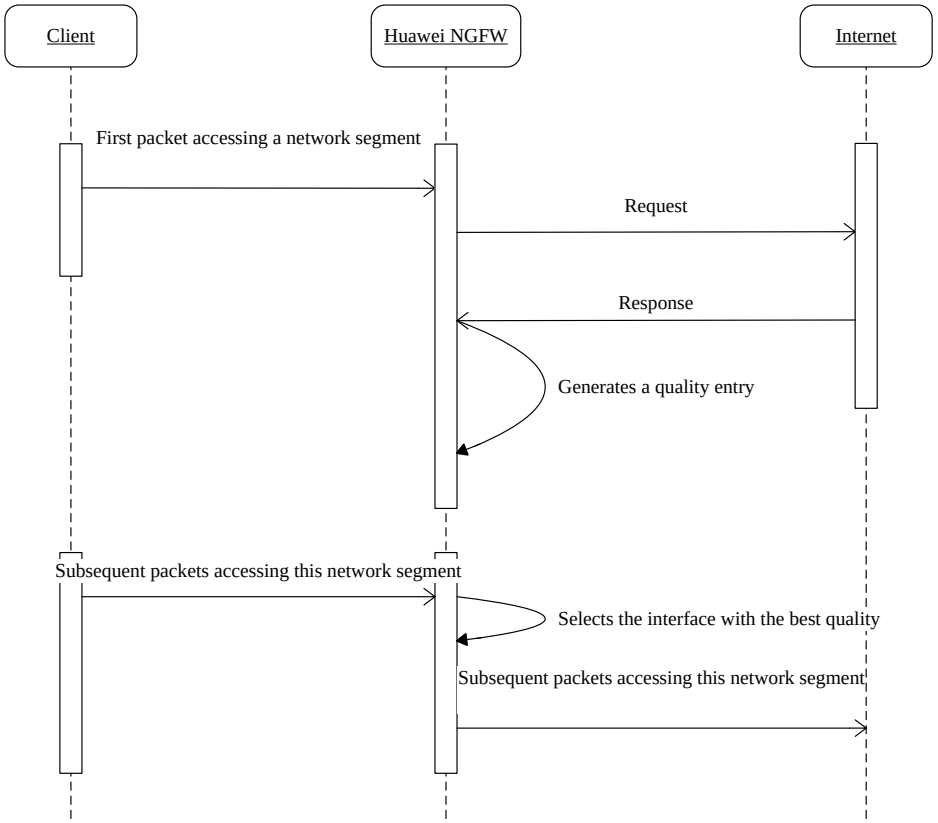
Traditional multi-carrier routing mechanisms include equal-cost routes and policy-based routing. Pure equal-cost routes result in a large amount of cross-carrier access, deteriorating access efficiency. Policy-based routing is difficult to configure and maintain and does not apply to changing network environments.

Huawei NGFW provides link quality- and interface bandwidth-based load balancing, priority-based active/standby backup, transparent DNS proxy, and smart DNS to optimize route selection and improve bandwidth usage, access quality, and user experience.

2.2 Link Quality-based Load Balancing

When an intranet user accesses a network segment for the first time, the NGFW proactively detects all outbound interfaces for the destination address and generates a quality entry based on the detection result. When the user accesses this network segment again, the NGFW selects the optimal outbound interface based on the quality entry. The link quality can be defined based on any combination of the packet loss ratio, delay, and jitter.

Copyright © Huawei Technologies Co., Ltd.



2.3 Interface Bandwidth-based Load Balancing

On a network with links provided by different carriers, bandwidth varies with links. Static routes or policy-based routing cannot properly distribute traffic among the links. As a result, packets are dropped on links with low bandwidth due to congestion, while the links with high bandwidth are idle. The NGFW can perform load balancing based on interface bandwidth to prevent the previous situation. With the overload protection function, the NGFW automatically adjusts the link selection mode to select an idle interface if the incoming or outgoing traffic on an interface exceeds the pre-set overload protection threshold.

2.4 Priority-based Active/Standby Backup

On a network with links provided by different carriers, the carriers can be prioritized. For example, if carrier A has a higher priority than carrier B, packets are preferentially transmitted through carrier A's link. If carrier A's link is down or overloaded, packets are transmitted through carrier B's link.

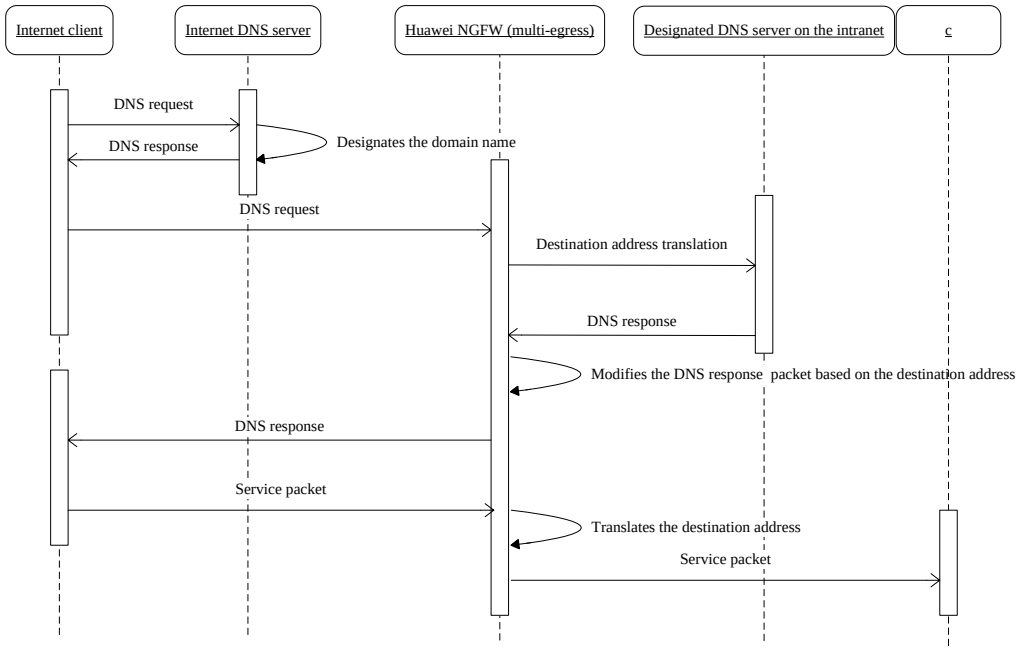
Copyright © Huawei Technologies Co., Ltd.

2.5 Transparent DNS Proxy

A DNS request is sent to obtain the destination address of a service packet. Then, a proper route is selected to forward the packet. If all intranet PCs share the DNS server provided by a carrier, these PCs probably learn the IP addresses of the carrier. Consequently, the carrier's link is too busy, affecting service access.

Transparent DNS proxy helps the NGFW evenly distribute DNS packets among the DNS servers provided by different carriers based on carriers' link bandwidth and priorities. The NGFW acts as the DNS proxy to allow DNS packets transmitted through carrier A's link to access carrier A's DNS server and DNS packets transmitted through carrier B's link to access carrier B's DNS server. In addition, the NGFW performs load balancing among the links of one carrier to maximize bandwidth usage.

2.6 Smart DNS Server

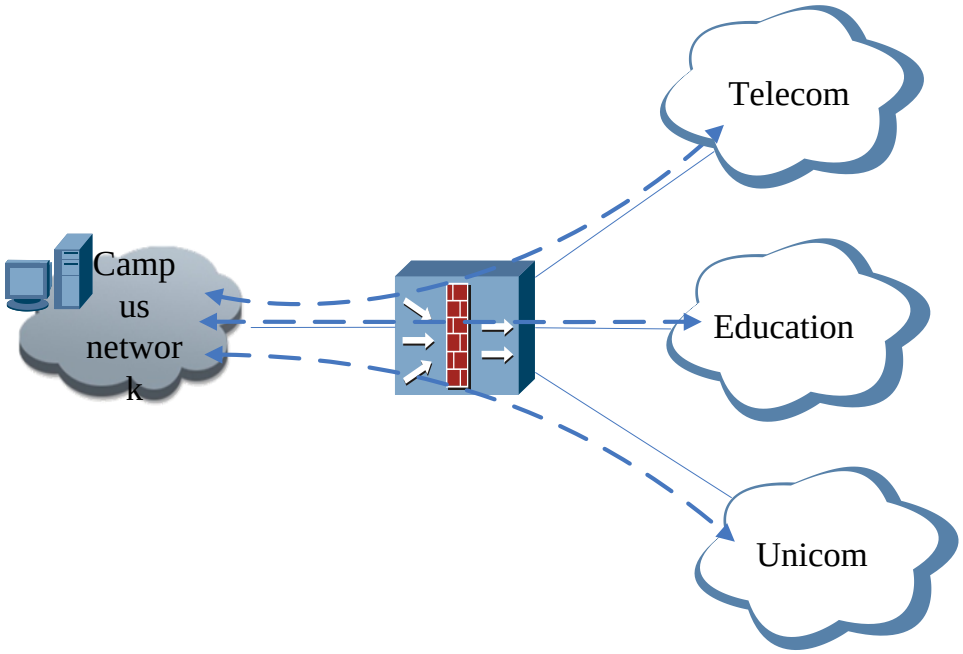


An enterprise leases links from multiple carriers, and the carriers designate an intranet server to process DNS packets accessing intranet servers. When an Internet user accesses intranet resources in domain name mode, the DNS response packet from the designated DNS server travels through the NGFW. The smart DNS module on the NGFW searches routes based on the DNS packet and translates the address carried in the DNS packet into the public address corresponding to the outbound interface. This mechanism ensures that the DNS packet is forwarded to the desired carrier network, improving network access quality

Copyright © Huawei Technologies Co., Ltd.

3 Typical Applications

3.1 Campus Network Gateway



A campus network probably leases links from multiple carriers to connect to the education network. As network connections are complicated, traffic is not evenly distributed among the links, resulting in low link usage, network congestion, and poor network access experience.

After Huawei NGFW is deployed on the campus network egress, transparent DNS proxy, carrier route, and interface bandwidth-based load balancing work together to properly allocate service traffic among the links, improving bandwidth usage and service access quality.

Copyright © Huawei Technologies Co., Ltd.