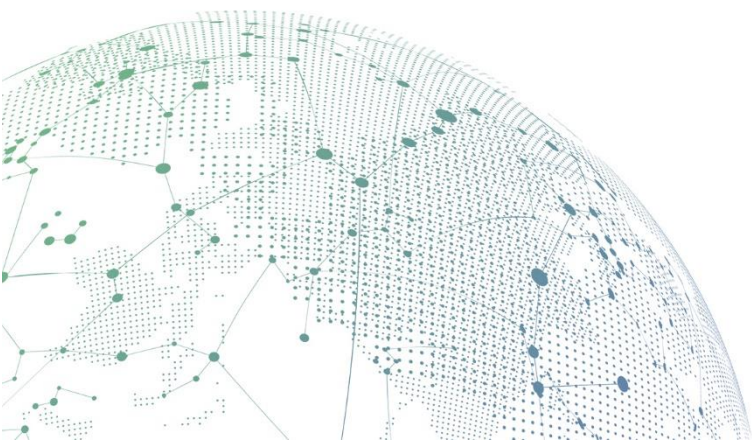




# NGAF

## Best Practices for Scenarios\_Country Blocking

Version 8.0.17



## Change Log

Date	Change Description
June 14, 2020	Version 8.0.17 document release.
May 17, 2021	Document update.

# CONTENT

Chapter 1 Function Introduction .....	1
Chapter 2 Scenario .....	1
Chapter 3 Best Practice .....	1
3.1 Configuration.....	1
3.2 Information Query .....	2
Chapter 4 Precautions .....	3

# Chapter 1 Function Introduction

Country Blocking, based on the IP of the country/region, filters access requests, reduces the attack surface, and improves the security of intranet-related business systems.

## Chapter 2 Scenario

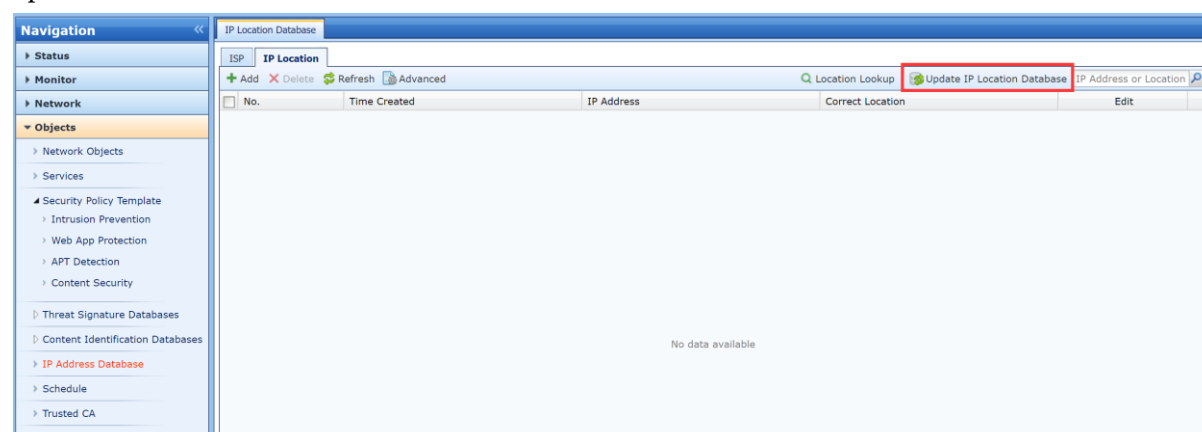
Hacker attacks are usually carried out in the form of a proxy server, and are mainly based on overseas proxy servers. And we have learned that most of the business systems of users do not actually need to provide services overseas, or only a small amount of overseas needs to provide services, and some special business systems only need to provide services to individual provinces within the country.

Based on the above background, after understanding the service scope of the business system with users, we can reduce the source of attacks and improve relevant business security through regional control.

## Chapter 3 Best Practice

### 3.1 Configuration

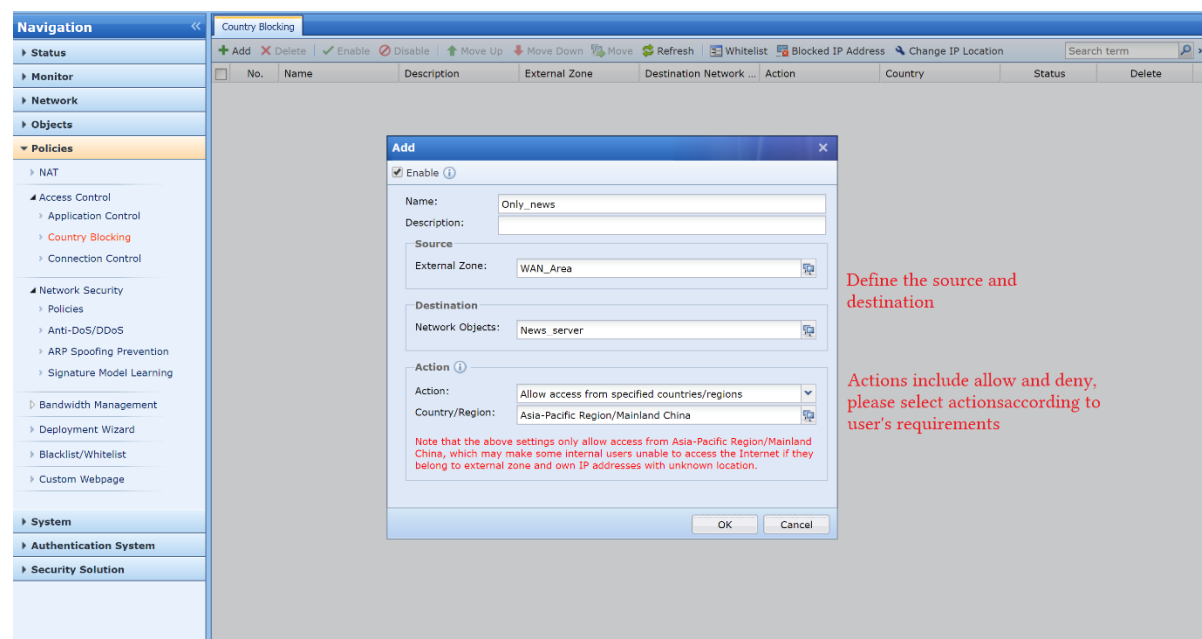
Country Blocking judges the IP location based on the IP Location database, so please update the IP Location database before configuring. It should be noted that the IP location database needs to be updated online.



Confirm with the customer which intranet systems need protection and the service range of the intranet business system. For example: News Server only needs to provide services to users in China. The

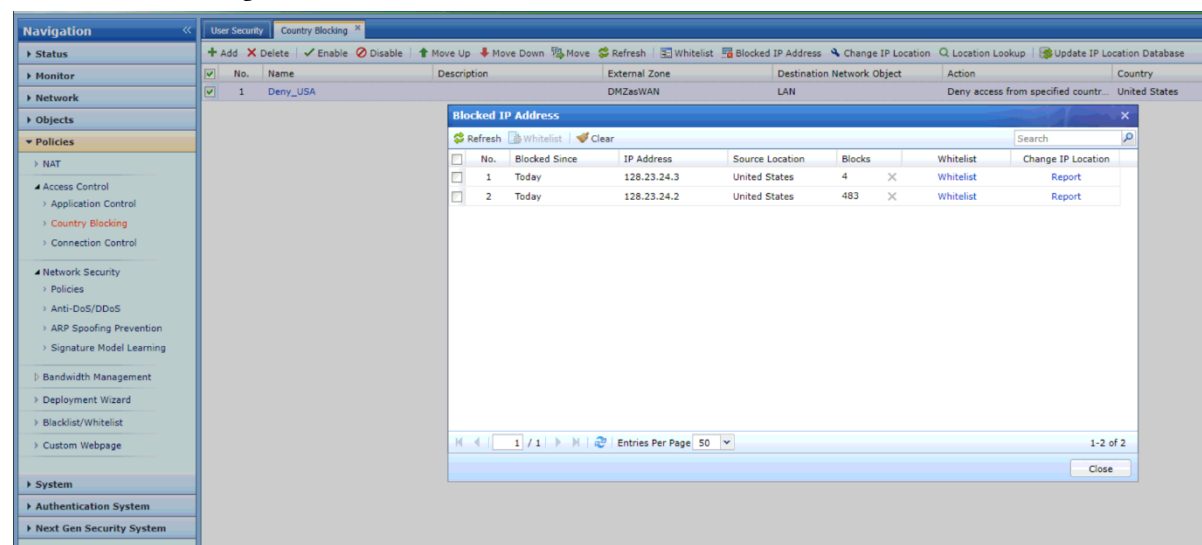
## Country Blocking

configuration is as follows:



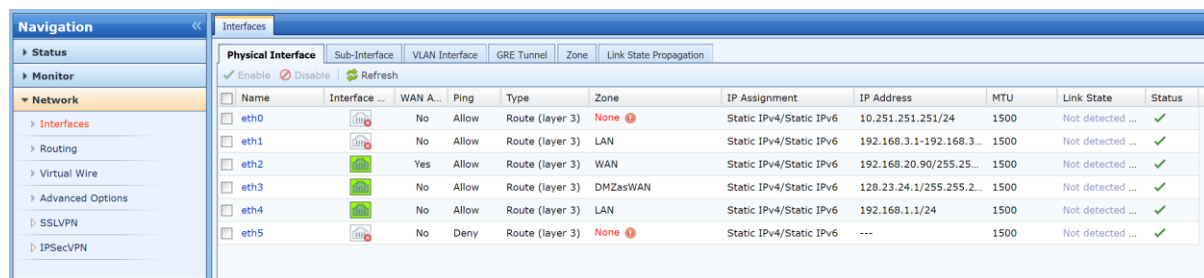
## 3.2 Information Query

When a hacker trigger an interception condition, [Country Blocking]-[ Blocked IP Address] will record the related access logs as follows:

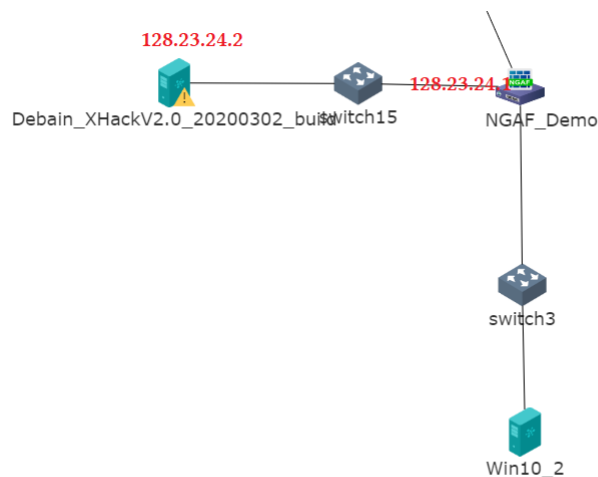


If you want to see the effect immediately, you can try to select a free network port to set the address of other regions, and then connect a PC and set the PC address to the same network segment to simulate the public network environment to access the internal network.

## Country Blocking

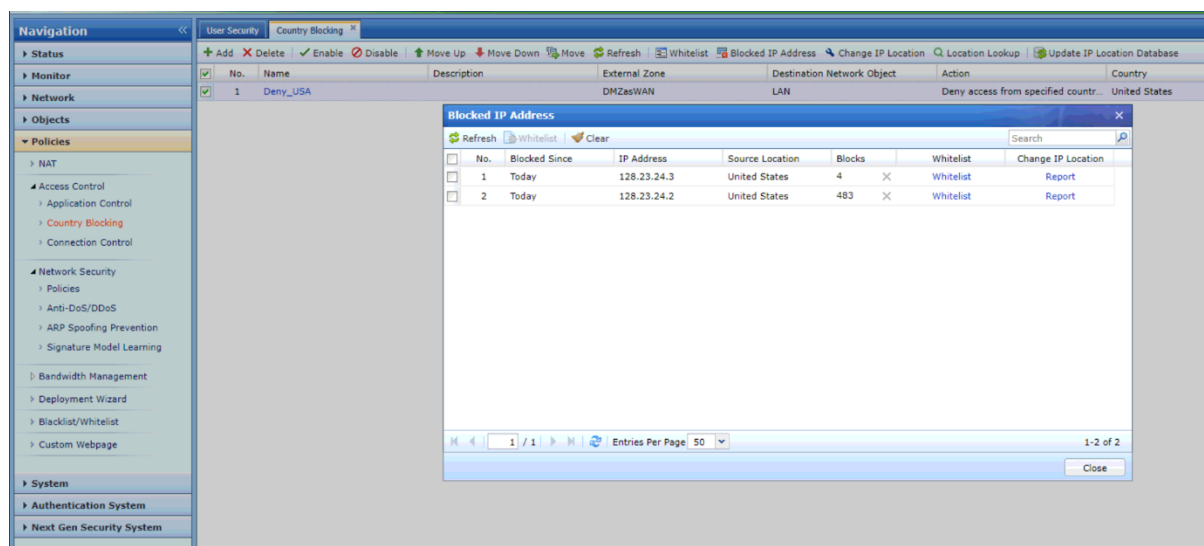


Name	Interface	WAN A...	Ping	Type	Zone	IP Assignment	IP Address	MTU	Link State	Status
eth0		No	Allow	Route (layer 3)	None	Static IPv4/Static IPv6	10.251.251.251/24	1500	Not detected ...	✓
eth1		No	Allow	Route (layer 3)	LAN	Static IPv4/Static IPv6	192.168.3.1-192.168.3...	1500	Not detected ...	✓
eth2		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 ...	✓



Then access the internal PC on the simulated public network PC to simulate an attack.

```
af@debian:~$ telnet 192.168.1.2 3389
```



No.	Blocked Since	IP Address	Source Location	Blocks	Whitelist	Change IP Location
1	Today	128.23.24.3	United States	4	Whitelist	Report
2	Today	128.23.24.2	United States	483	Whitelist	Report

## Chapter 4 Precautions

## Country Blocking

If you want to know which country/region an IP belongs to in advance, you can query through [Country Blocking]-[Location Lookup].

When the device can be connected to the Internet, the address database will be automatically updated, but the IP may be recognized as an error. If a misjudgment occurs, it can be resolved by add to whitelist or correcting it in "Change IP Location".



**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