SANGFOR

# NGAF

## Application Control - Best Practice

Version 8.0.8

# Change Log

| Date | Change Description |
| --- | --- |
| July 2, 2019 | Version 1.0 document release. |
| | |

# CONTENT

# Chapter 1 Introduction

Application control policy controls data packets based on the TCP/IP definition range of interactive data packets or the characteristics of the application layer to prevent unauthorized data packets from interacting.

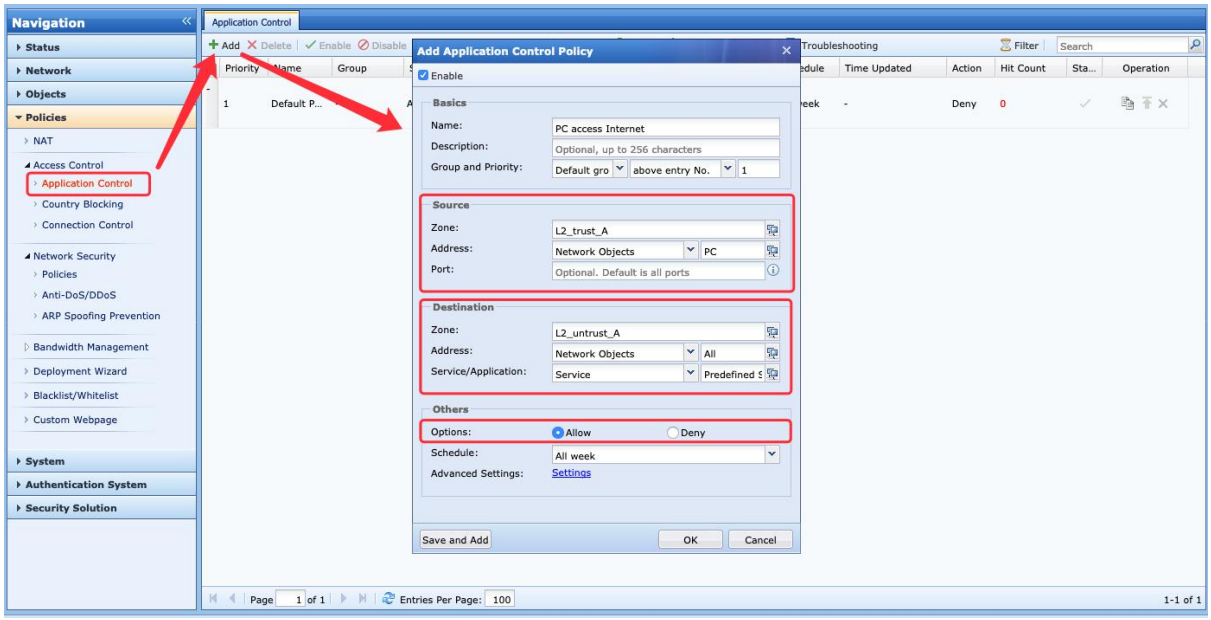
# Chapter 2 Best Practices

By applying application control policies, the interactive data from both parties in the communication are defined and controlled in the principle of minimizing access permissions, so as to greatly reducing the range under attack and the security risks. The suggestion here is for reference only. It depends on the actual environment for special circumstances.

**Note:** The application control policy intercepts all interaction behaviors by default. Set at least one corresponding allow policy to ensure the normal network access.

## 1 Suggestions on PC Network Access

For users who do not have any specific control requirement for the PC network access, it is recommended to preset the IP segment and zones for the PC, and allow the network access (from LAN to WAN) for all applications on the PC. The configuration is as follows:

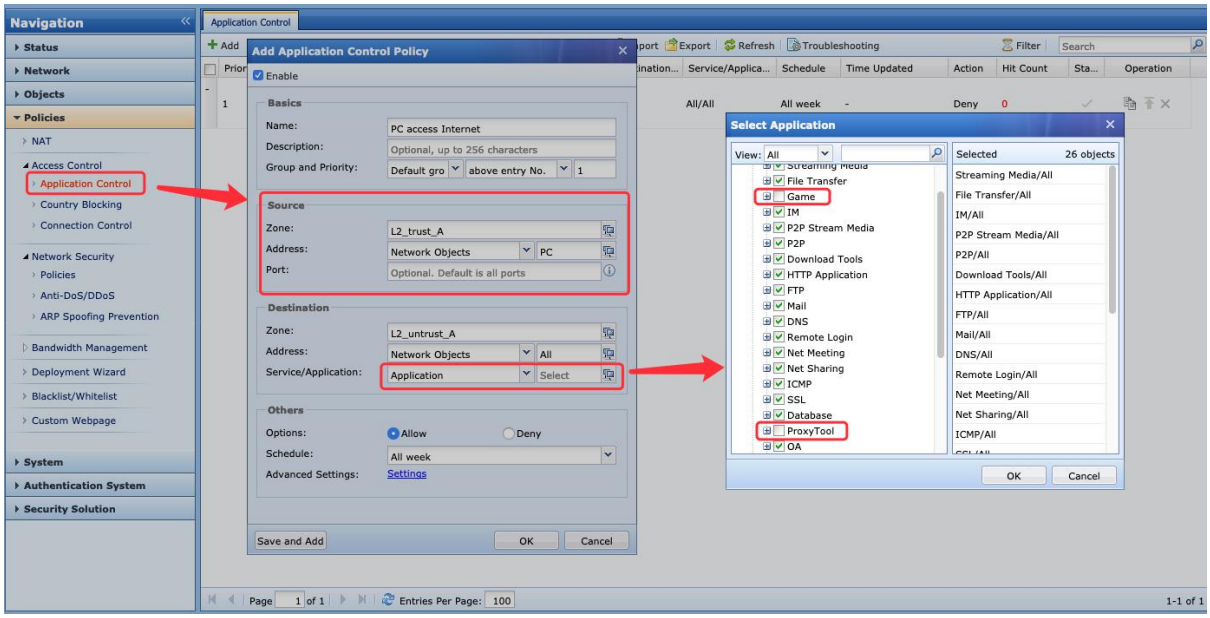



**Note:** Many administrators like to use one policy to allow all IP access requests from bi-direction. This practice is not recommended. It only needs to allow the data access from LAN to WAN if there are no special circumstances with the PC.

**Note:** Pay attention to the scenario that: the NGAF is deployed in bridge mode or virtual wire mode, and the customer have a DHCP server in the WAN outside the AF (for example, set DHCP for the gateway devices connected to the AF). In this scenario, it needs to allow at least the DHCP service from WAN to LAN: UDP ports 67 & 68, to make sure the connected PCs can obtain the DHCP address.

### 1.1 With Specific Control Requirements

For users have specific requirements for the PC network access (for example, the PC can access the network, but cannot play online games or use proxy tools). The configuration is as follows.



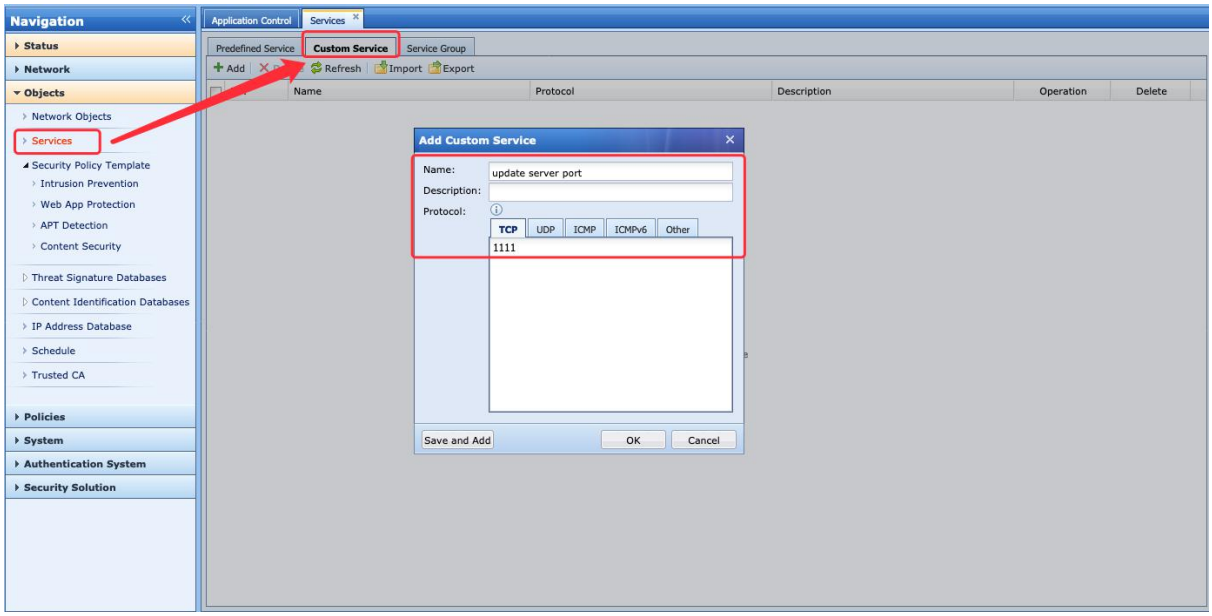

**Note:** The "Service/Application" is a radio option, and specific choice depends the user's needs. If the user does not allow a specific destination port in the WAN to be accessed, it is more appropriate to choose "Service".

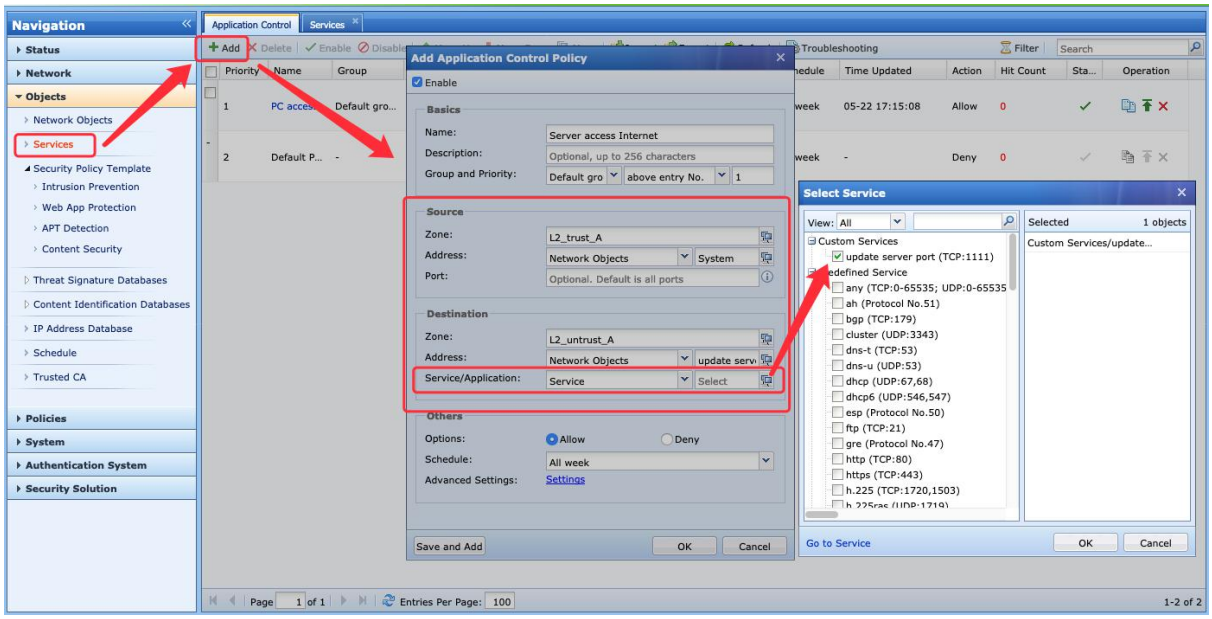
# 2 Suggestions on the Server Network Access

## 2.1 Server Network Access is Required

Generally, it happens when a server needs to access some specific resources, such as regularly updating software or synchronizing data to a specific server. In this situation, it is recommended to ask the user about the destination IP to be accessed or even the port of the destination IP.

For example, the server of a portal website needs to access a synchronization server (200.200.200.200:1111) on the public cloud to push synchronous data regularly.






## 2.2 Server Network Access is Not Required

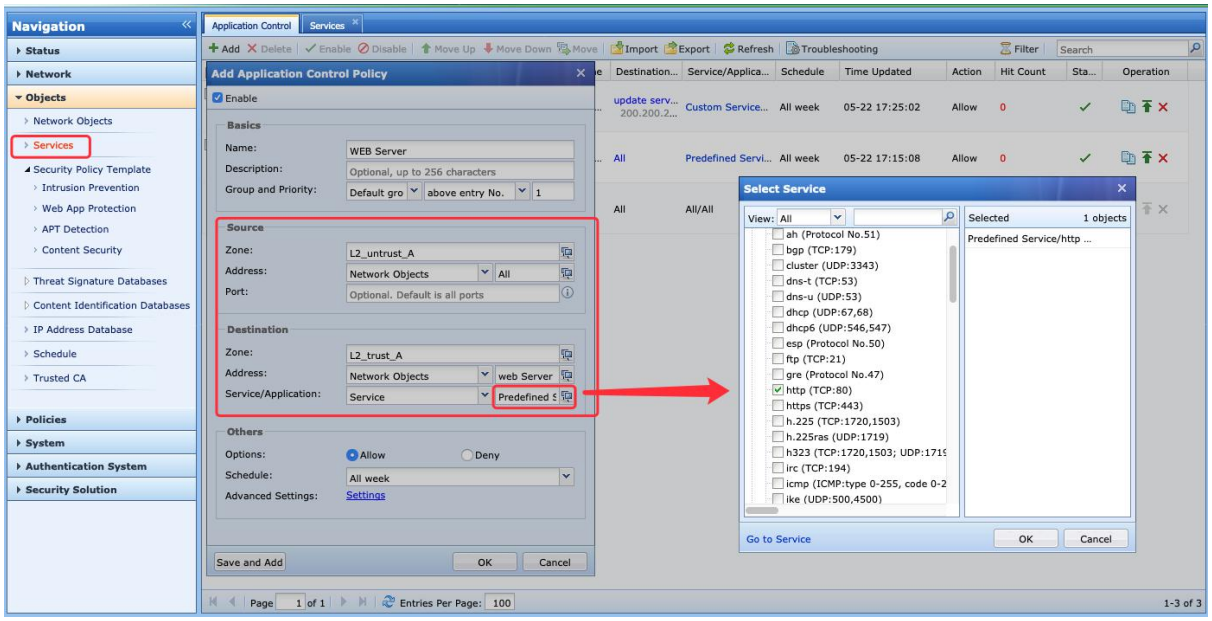
In this situation, it does not need to configure any "Allow" policy for the direction from the server to the WAN zone. The default policy will be applied to intercept network access behaviors of the server.

# 3 Suggestions on Public Publishing of the Server

## 3.1 Not Configure DNAT in NGAF

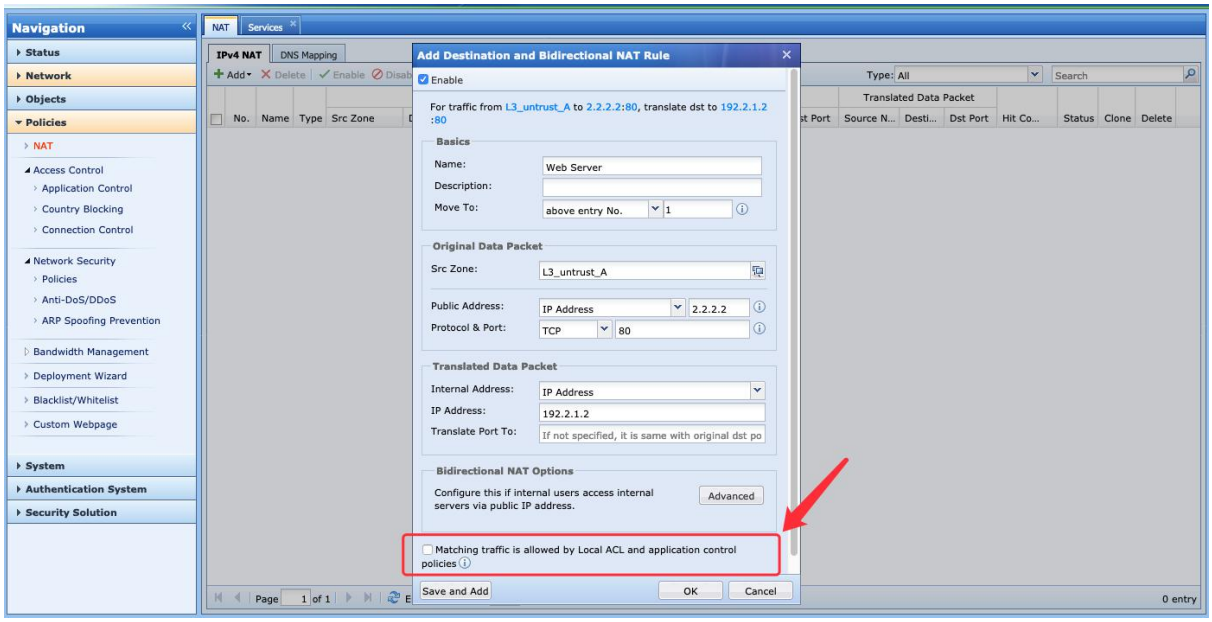
This scenario is relatively simple. The user-related servers only need the ports/services that can publish to public. Other ports/services are still not allowed.

For example, the portal website only needs the HTTP ports for public publishing.




## 3.2 Configure DNAT in NGAF

In this scenario, note that in the DNAT policy, all content of DNAT are allowed to be accessed by application control policies by default. When in the environment of full mapping for a public network IP, it is recommended to negotiation with the user and uncheck this option, and manually enable services in the application control policies.




# Chapter 3 Precautions

- Be careful to enable the "Persistent Connection" in the [Application Control] - [Advanced Settings]. Only enable alone for specific servers with requirements (if needed). Avoid too many of enabled servers to prevent slow release of the device links, which will affect the device performance.
- Be careful to enable the "Logging" in the [Application Control] - [Advanced Settings]. It is suggested to save the logs into the "External Data Center" if the amount of items to be logged is large, to avoid too many logs appears in the default Internal Data Center, which will affect device performance.
- The [Application Control] - [Troubleshooting] includes three functions: "Policy Validity Check", "Policy Troubleshooting" and "Group Management." You may introduce these functions to users to embody the simple and easy-to-use features of the product.

# Chapter 4 Contact Us

| | |
|---|---|
| Technical Support Email: | tech.support@sangfor.com |
| Technical Support Hotline: | International Service Centre: +60 12711 7129 (7511)<br><br>Malaysia: 1700 81 7071<br><br>Hong Kong: +852 81257201<br><br>Singapore: +65 3152 9370<br><br>Other Regions: +60-12-7117511 (7129) |
| Technical Support Community: | http://community.sangfor.com |
| Official Website: | http://www.sangfor.com |

SANGFOR