



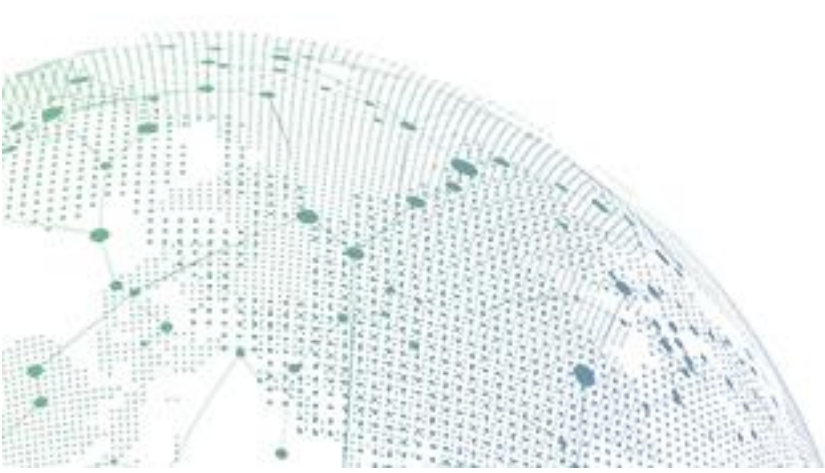
SANGFOR



IAM

Proxy Server Environment Deployment

Version 12.0.13



Change Log

Date	Change Description
Sept 19, 2018	Version 12.0.13 document release

CONTENT

Chapter 1 Application Scenario	1
1.1 Proxy server with dual network card (IAM as bridge or route mode)	1
1.2 Proxy server with dual network card (IAM as Bypass mode)	2
1.3 Proxy server with single network card (IAM as bridge mode)	3

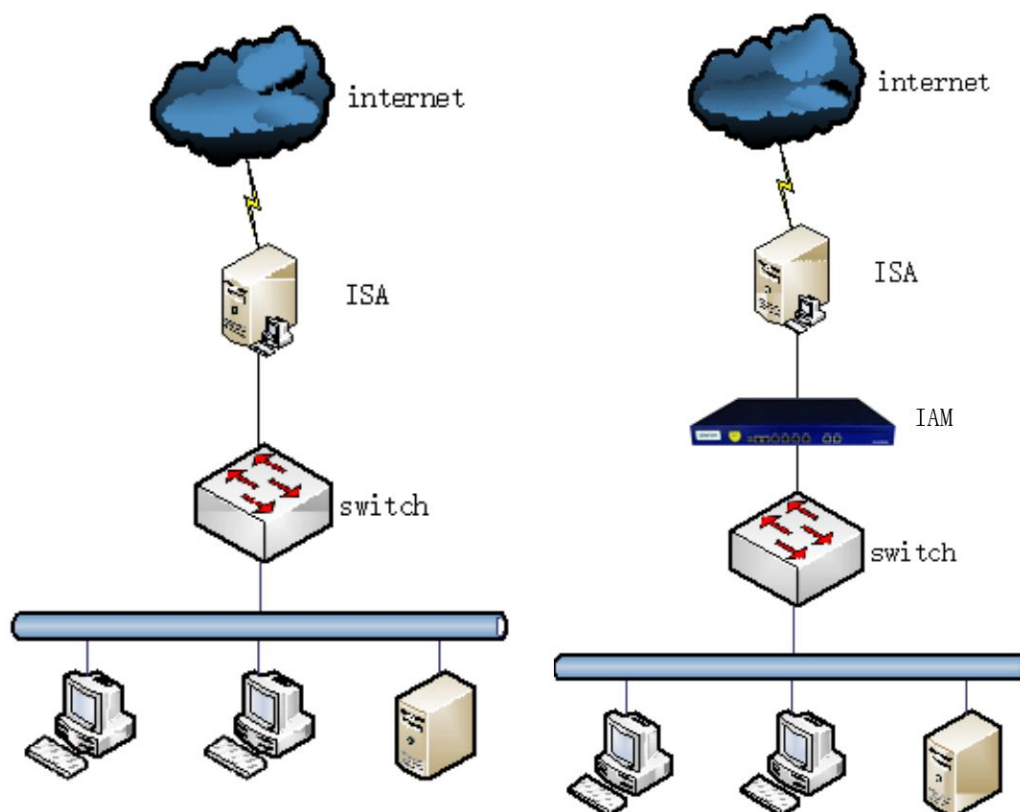
Chapter 1 Application Scenario

In the intranet network proxy server environment, all user data are sent to the proxy server user with the proxy server's IP as the destination IP. In real scenario, the real data will be encrypted by the proxy server before send to internet.

In such a network environment, if you want apply different Internet access policies for online users to record the real public access network data, then the deployment will be different with others network deployment.

Applicable scenario: Users online via proxy server and IAM need to accurately identify user online traffic and do the access control.

1.1 Proxy server with dual network card (IAM as bridge or route mode)



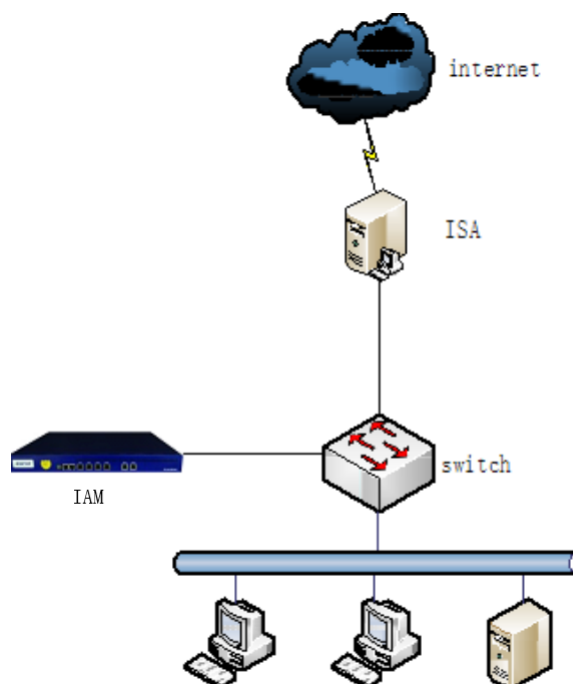
Configuration:

1. Device can deploy in route mode or bridge mode. We recommend use bridge mode as it need the less changing on the network configuration. But we need to make sure the internal data flow must go through IAM, or the proxy server

must locate in the WAN direction of the IAM.

2. Fill in IAM IP in IE proxy server exceptions list.
3. Fill in the proxy server IP and port in [System]-[General]-[Advanced]-[Proxy]

1.2 Proxy server with dual network card (IAM as Bypass mode)



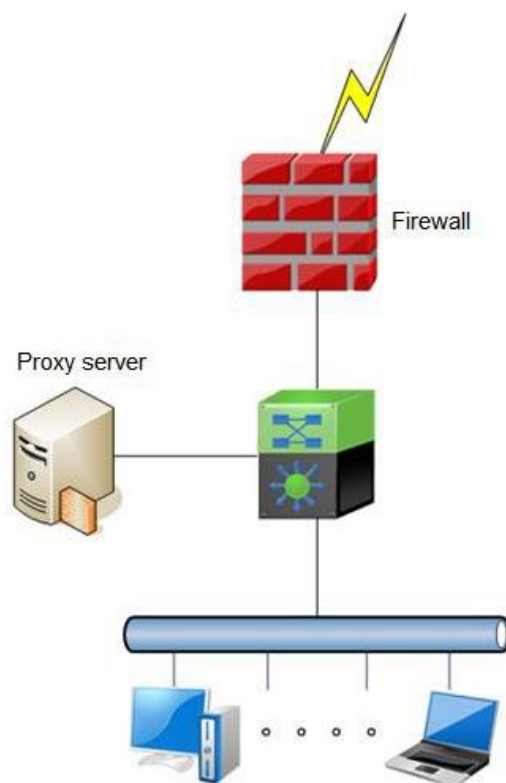
Configuration:

1. If only for audit or control only the TCP protocol data, the device may take the bypass mode deployment for monitoring data sent from internal network to proxy server.
2. Fill in the proxy server IP and port in Proxy>Proxy Services

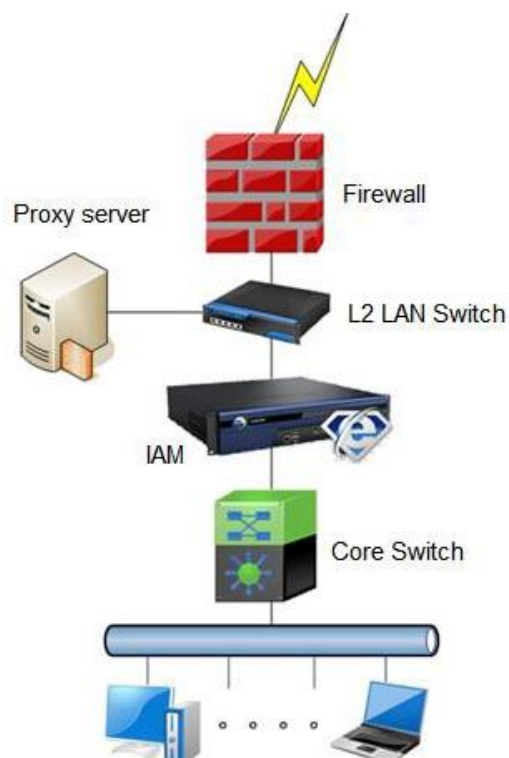
1.3 Proxy server with single network card (IAM as bridge mode)

Data flow as below:

PC>Switch>Proxy Sever>Switch>Firewall>Internet



Solution 1:



1. Add a L2 LAN switch between firewall, proxy server and core switch. We can relocate the proxy server to firewall interface, but if proxy server and firewall is not in a same VLAN, we need to re-plan the proxy server and firewall IP range.
2. Deploy the IAM between L2 LAN switch and ensure online traffic only pass once to the IAM.
3. Enter proxy server IP in "Proxy server settings" of IAM.

The screenshot displays the Sangfor IAM 12.0.13 configuration interface. The top navigation bar includes the Sangfor logo and the version number. The left sidebar contains a 'Navigation' menu with categories such as Status, Proxy, Objects, Users, Access Mgt, Bandwidth Mgt, Endpoint Device, Security, WiFi Access, and System. The 'System' category is expanded, showing sub-menus like Network, Firewall, and General. The 'Advanced' configuration page is selected, and the 'Proxy' category is highlighted in the 'Category' list. The main content area shows the 'Proxy' configuration page with a text input field for IP addresses and a 'Commit' button.

One IP address or range per row. Example: 192.168.0.1-192.168.0.6
It inspects proxied packet from specified IP addresses, to enhance application identification accuracy. If none is specified, all packets will be inspected.

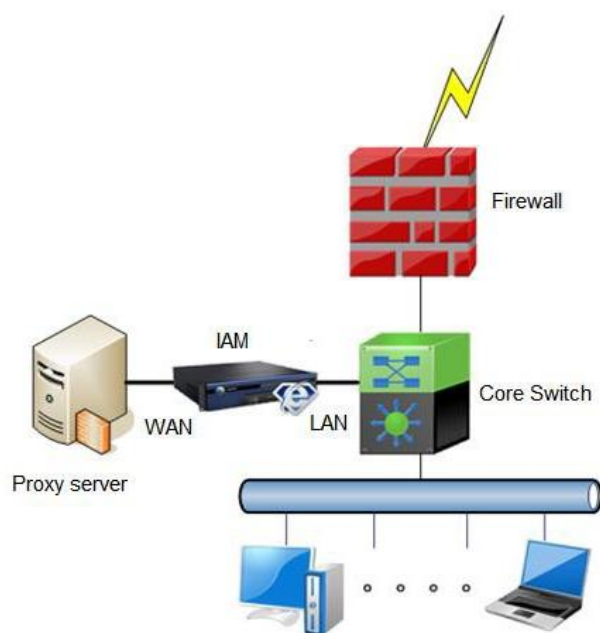
Type here

Commit

4. If the users group does not have privilege to access via proxy server, kindly refer configuration steps as per following links.

http://community.sangfor.com/plugin.php?id=sangfor_databases:index&mod=viewdatabase&tid=775

Solution 2:



1. Deploy IAM between proxy server and core switch.
2. Due to traffic will flow twice via the IAM, the online users list will show public IP as the online user.
3. Need to enable the following setting in [Users]-[Advanced]

The screenshot shows the SANGFOR IAM 12.0.13 web interface. The 'Advanced' settings for 'Authentication Options' are displayed. The 'Open auth for data flow from WAN to LAN interface' checkbox is highlighted with a red box. Other settings include:

- Lockout Period (mins): 1
- Delete accounts inactive for too long a time:
- Days Being Inactive: 30
- Auto remove MAC bindings when open authentication expires:
- Allow account to be bound with limited endpoints:
- Max Endpoints: 0
- Address Changes and Conflicts Handling:
 - Re-authentication is required if MAC address changes:
 - Take action if user logs in on a second IP address with an account that does not allow concurrent login:
 - Reject request and notify user that account is being used on other endpoint:
 - Disconnect earliest endpoint and allow new endpoint:
- Open Authentication Options:
 - Enable cookie-based authentication:
 - Period(days): 30
- Security Options:
 - Enable password strength requirements:
 - Settings:
 - Use SSL to encrypt username and password:
 - Domain Name:
 - Device Certificate: *.ppns.ac.id (Upload or Create CSR)
- Other Options:
 - DNS service is available even user is not authenticated or is locked:
 - Redirect HTTPS requests(not using proxy) to captive portal if user is not authenticated:
 - For Internet access using proxy, password submission is Web based:
 - Username of domain user is domain account plus domain name:
 - Open auth for data flow from WAN to LAN interface:
 - Disable sorting by user/group:



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