

Table of Contents

Chapter 1 EAD Configuration.....	1-1
1.1 Introduction to EAD.....	1-1
1.2 Network Application of EAD Configuration.....	1-1
1.3 EAD Configuration.....	1-2
1.4 EAD Configuration Examples.....	1-3
Chapter 2 EAD Configuration Commands.....	2-1
2.1 EAD Configuration Commands.....	2-1
2.1.1 security-policy-server.....	2-1

Chapter 1 EAD Configuration

1.1 Introduction to EAD

By means of monitoring the received data, endpoint admission defense (EAD) solution enhances the capacity of network terminals for proactively defending themselves against the spread of virus within the network. Meanwhile, by imposing an accessing restriction on terminals that do not meet the security requirements, EAD prevents unsafe terminals from causing damages to the whole network.

EAD solution entails cooperation of the switch, the AAA server, the security policy server and the security client in order to conduct a security evaluation on the end users and to dynamically control their access rights.

When EAD is enabled, the switch will decide whether a session control packet is valid or not by checking its source IP address.

- Only those session control packets that are sent from the Authentication Servers or Security Policy Servers are taken as valid.
- Based on the instructions from the session control packets, the switch will dynamically adjust the VLAN, the rate, the packet scheduling priority, and the access control list (ACL) of the terminals, and thereby dynamically control the access rights of end users.

1.2 Network Application of EAD Configuration

Before terminals can get access to the network, EAD will conduct a compulsory check on their security states, and based on the result of the check, implement the mandatory user access control policy. Thus, EAD can effectively segregate terminals that do not meet security requirements and compel users to upgrade their virus databases and to install system patches. [Figure 1-1](#) illustrates EAD's network application.

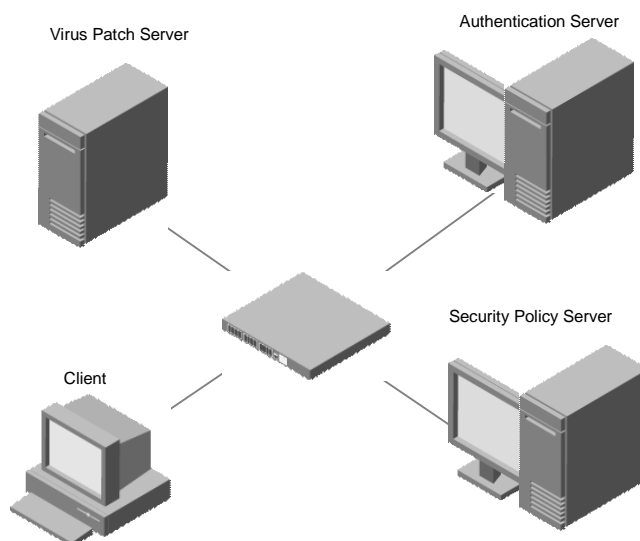


Figure 1-1 Network application of EAD configuration

After the IDs of end users have been authenticated, the security client (software installed on the end users' PCs) will check the security states of end users, and interact with the security policy server. If the end users do not meet the security and authentication standards, the security policy server will send ACL control packets to the switch, which will only grant the end users access to the virus patch server.

Only after end users have installed the virus patches, and the security standards of end users have met the security and authentication standards, will the security client forward the security state of end users to the security policy server, which will once again send out an ACL packet, allowing the switch to grant the end users access to the network so that they can access more network resources.

1.3 EAD Configuration

EAD configuration is as follows:

- Configure user attributes, such as user names, user types, and user passwords. When configuring local authentication, you need to set user attributes on the switch. To configure remote authentication, you need to set user attributes on AAA servers.
- Configure RADIUS scheme.
- Configure the IP address of security policy server.
- Configure the association of the domain and the RADIUS scheme.

EAD mainly applies to RADIUS authentication.

This section focuses on how to configure the IP addresses of security policy servers. For more related configuration procedures, refer to the security part of *Quidway S5600 Series Ethernet Switches Operation Manual*.

Table 1-1 EAD Configuration Tasks

Configuration Procedure	Command	Description
Enter system view	system-view	—
Enter RADIUS scheme view	radius scheme <i>radius-scheme-name</i>	—
Configure the IP addresses of security policy servers	security-policy-server <i>ip-address</i>	For each RADIUS scheme, a maximum of eight security policy servers with different IP addresses can be configured.

1.4 EAD Configuration Examples

Notes:

The ways to configure remote server authentication for Telnet users and FTP users are similar. Therefore, the following section will describe the remote authentication for Telnet users only.

I. Network diagram requirements

In an environment as illustrated in [Figure 1-2](#), through configuration of the switch, the RADIUS server can implement remote authentication for Telnet users currently using the switch, and the security policy server can control the users' EAD operations.

The configuration tasks are described as follows:

- Connect the authentication server (responsible for authenticating RADIUS servers) with the switch. The IP address for the authentication server is 10.110.91.164, and the switch uses port 1812 to communicate with the authentication server.
- Set the type of the authentication server to be standard.
- Set the cipher text password for communication between the switch and the authentication RADIUS server to be expert.
- Configure the switch to remove the user domain name from the user name before sending it to the RADIUS server.
- Configure the security policy server, with the IP address being 10.110.91.166.
- Configure virus patch server, with the IP address being 10.110.91.168.

II. Network diagram

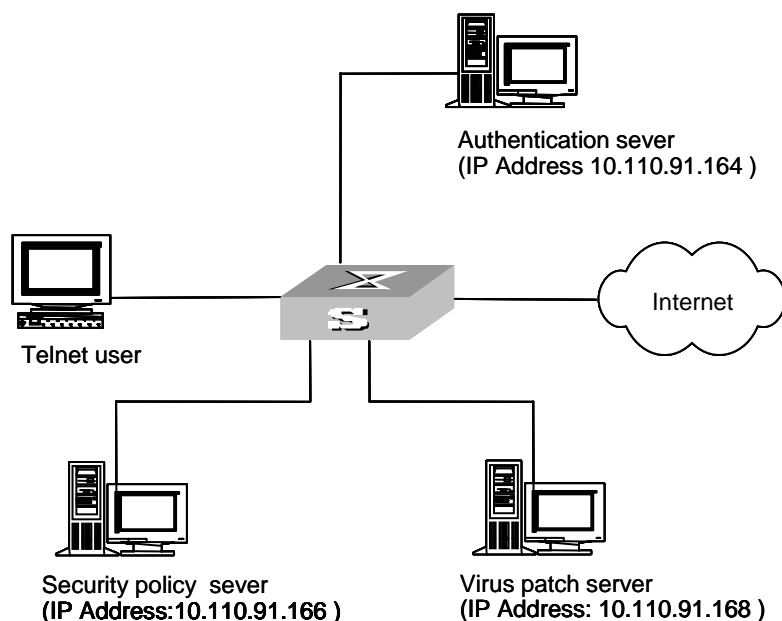


Figure 1-2 network diagram for standard EAD configuration

III. Configuration Procedures

To configure Telnet users' attributes on the authentication server, refer to the configuration guide for the authentication server.

Configure Telnet users to use remote authentication, that is, the scheme mode.

```
<Quidway> system-view
[Quidway] user-interface vty 0 4
[Quidway-ui-vty0-4] authentication-mode scheme
```

Configure domain.

```
[Quidway] domain system
[Quidway-isp-system] quit
```

Configure RADIUS scheme.

```
[Quidway] radius scheme cams
[Quidway-radius-cams] primary authentication 10.110.91.164 1812
[Quidway-radius-cams] key authentication expert
[Quidway-radius-cams] server-type standard
[Quidway-radius-cams] user-name-format without-domain
```

Configure the IP address for the security policy server.

```
[Quidway-radius-cams] security-policy-server 10.110.91.166
```

Configure the association of the domain and the RADIUS scheme.

```
[Quidway-radius-cams] quit
[Quidway] domain system
```

```
[Quidway-isp-system] radius-scheme cams
```

Chapter 2 EAD Configuration Commands

2.1 EAD Configuration Commands

2.1.1 security-policy-server

Syntax

```
security-policy-server ip-address  
undo security-policy-server [ ip-address | all ]
```

View

RADIUS scheme view

Parameter

ip-address: The IP address of security policy server.

all: The IP addresses of all the security policy servers.

Description

Use the **security-policy-server** command to configure the IP address of a security policy server.

Use the **undo security-policy-server** command to remove the IP address configuration of a security policy server.

For each RADIUS scheme, a maximum of eight security policy servers with different IP addresses can be configured. While users are surfing the Internet, the switch will only respond to the session control packets sent from the authentication server and the security policy server.

Example

Configure the IP address of the security policy server to be 192.168.0.1.

```
<Quidway>system-view  
System View: return to User View with Ctrl+Z.  
[Quidway] radius scheme Quidway  
[Quidway-radius-Quidway] security-policy-server 192.168.0.1  
[Quidway-radius-Quidway] display current-configuration  
...  
radius scheme Quidway  
primary authentication 1.1.11.29 1812  
secondary authentication 127.0.0.1 1645  
user-name-format without-domain
```

```
security-policy-server 192.168.0.1
```