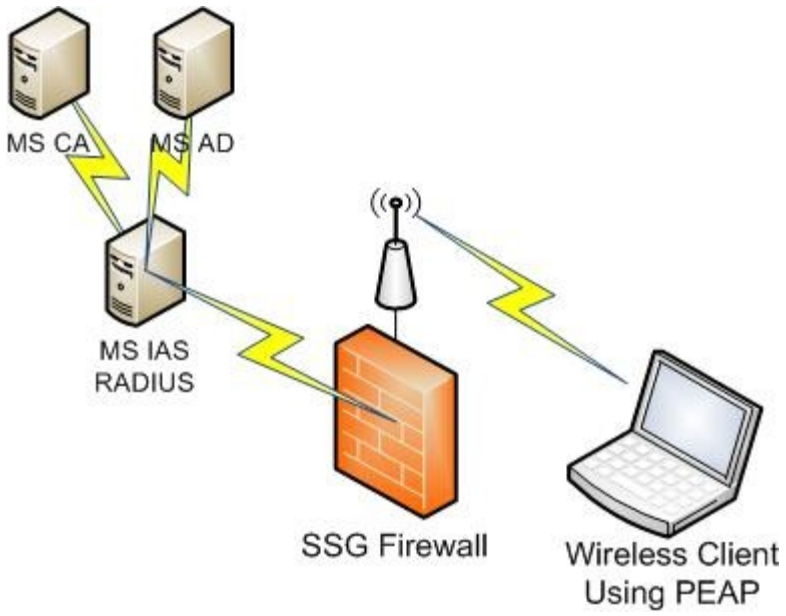
ScreenOS Wireless RADIUS Authentication with Microsoft Server 2003 IAS

Product: ScreenOS

Version: 6.2R7 or above

There is a RADIUS bug in code below this release that can cause a system reboot when RADIUS authentication is denied for the client.

Network Topology:



Description:

Create a RADIUS authentication wireless segment on a ScreenOS firewall. This uses the Microsoft IAS server component that is free with Windows server 2003. The configuration does require a active directory domain and a Microsoft certificate authority. All components are included with the Server 2003 OS and can be installed on a single server.

Microsoft Domain Setup

This configuration was tested using a Microsoft Server 2003 infrastructure. This infrastructure requires that three roles are setup on the domain:

- Active Directory Domain Controller
- Certificate Authority

- Internet Authentication Server (IAS) - this is the Microsoft implementation of RADIUS

These three roles can all exist on the same server without any issues in a small network or they can be existing and distributed on other servers in an existing setup. The configuration of this infrastructure is outlined in this technet article.

Deployment of Protected 802.11 Networks Using Microsoft Windows

http://technet.microsoft.com/en-us/network/cc917481.aspx

Windows XP client Setup

After this is configured the wireless client software on the affected computers will also need to be configured. And the certificates needed for the authentication methods chosen will need to be distributed to the clients. The document also above outlined the group policy options for these setting changes and certificate distribution.

When you connect to the SSID for the wireless segment the protocol needs to be changed to Protected EAP in the properties of the wireless interface.

- Select the ssid and again pick properties
- Select the authentication tab and change from smart card to certificate authentication
- Setup Peap on client wireless connection

ScreenOS Configuration

The Juniper ScreenOS wireless enabled firewall will be configured to communicate with this Microsoft RADIUS infrastructure to authenticate clients. There are two basic steps to the process.

1. Configure the RADIUS authentication server
2. Configure the wireless interface for 802.1x using this server

Configuration:

1-Add a RADIUS Authentication Server

For this example the following are the parameters

Primary RADIUS server 192.168.1.10

Secondary RADIUS server (optional) 192.168.1.11

RADIUS passphrase YourPassword

The auth server name is radserver

ScreenOS Wireless RADIUS Authentication with Microsoft Server 2003 IAS

CLI

lab-> set auth-server radserver server-name 192.168.1.10

lab-> set auth-server radserver backup1 192.168.1.11

lab-> set auth-server radserver account-type 802.1x

lab-> set auth-server radserver radius secret YourPassword

Web

Configuration - Auth - Auth Servers

Fill in the form

2-Configure a wireless interface to use the RADIUS server

For this example the SSID is MyWireless on the wireless0 interface using "radserver" as the authentication server.

CLI

lab-> set ssid name MyWireless

lab-> set ssid MyWireless authentication 802.1x auth-server radserver

lab-> set ssid MyWireless interface wireless0

Web

Wireless - SSID

Select new and fill in the form

Verification:

When connecting there are sessions and statistics on the firewall and logs generated on the Microsoft IAS server.

IAS Server

In the IAS mmc the logging area shows the location of the log file.

Default: Windows\system32\logs

There will be log entries for all connection attempts whether rejected or accepted.

ScreenOS Wireless RADIUS Authentication with Microsoft Server 2003 IAS

Firewall

Sessions shows actively connected devices while the statistics show the counts since the last reset.

CLI

lab->get dot1x session

lab->get dot1x statistics

Web

Network - 802.1x - Statistics or Sessions