How to Configure an External Authentication Service

https://campus.barracuda.com/doc/13305789/

By integrating the Barracuda NextGen Firewall X-Series with your existing authentication server, you can configure access rules that apply to specific users and groups without having to create local user accounts on the X-Series Firewall. The X-Series Firewall supports the following external authentication services:

Barracuda DC Agent

The Barracuda DC Agent runs on the domain controller or a dedicated Windows PC in the office network. The DC Agent continuously checks the domain controller for login events to create a list of users and their associated IP addresses. The list of authenticated users is provided to the X-Series Firewall, allowing for true single sign-on capabilities. You can download the Barracuda DC Agent directly from the X-Series Firewall Web UI.

For information, see How to Configure Barracuda DC Agent Authentication and Barracuda DC Agent for User Authentication

Barracuda Terminal Server Agent (TS Agent)

The Barracuda Terminal Server Agent (TS Agent) authenticates users logged into a Microsoft Terminal Server. Because users on a Terminal Server all use the same source IP address, the Barracuda TS Agent maps each user to a specified source port range and sends this mapping to the X-Series Firewall. The X-Series Firewall can thus determine the user for each connection from the terminal server by the source port.

For more information, see How to Configure TS Agent Authentication.

Active Directory

Microsoft Active Directory (MSAD) is a directory service that allows authentication and authorization of users in a network. It has been included with all Windows Server operating systems since Windows 2000 Server. MSAD is used for single sign-on for many services. Permissions are managed by group. Users inherit the permissions of all the groups that they are members of. Backward-compatibility for

older services is provided by NTLM/MS-CHAP options that you can activate and configure on the MSAD server. All information is kept in a single directory information tree.

For more information, see How to Configure MSAD Authentication.

NTLM

If your network uses an NT LAN Manager (NTLM) authentication server, your NTLM domain users are transparently authenticated using their Microsoft Windows credentials. This single sign-on method of access control is provided by transparent proxy authentication against your NTLM server. To enable transparent proxy authentication against your NTLM server, you must join the X-Series Firewall to the NTLM domain as an authorized host.

For more information, see How to Configure NTLM Authentication.

LDAP

Lightweight Directory Access Protocol (LDAP) is used for storing and managing distributed information services in a network. LDAP is mainly used to provide a single sign-on solution. It follows the same X.500 directory structure as MSAD.

For more information, see How to Configure LDAP Authentication.

RADIUS

Remote Access Dial In User Service (RADIUS) is a networking protocol providing authentication, authorization, and accounting. The X-Series Firewall uses RADIUS authentication for the IPsec, Client-to-Site, and SSL VPN.

For more information, see How to Configure RADIUS Authentication.

Wi-Fi Access Point

The X-Series Firewall can parse authentication information contained in the syslog stream of supported wireless access points. Wi-Fi access points typically use authentication services such as

RADIUS servers to authenticate users before allowing them to connect. The X-Series Firewall monitors the syslog files sent by the Wi-Fi access points for usernames and the associated IP address of logged-in users. Depending on the access point, the X-Series Firewall receives login and/or logout information.

For more information, see How to Configure Wi-Fi Access Point Authentication.

OCSP

Online Certificate Status Protocol (OCSP) is a protocol used to check if X.509 certificates have been revoked by their respective certificate authorities (CAs). The X-Series Firewall uses the information provided by OCSP to verify the authenticity of a certificate. For integration with OCSP-based online digital certification verification:

1. Go to the **USERS > External Authentication** page.
2. Click the **OCSP** tab.
3. Enter the settings for your OCSP server and then click **Save**.