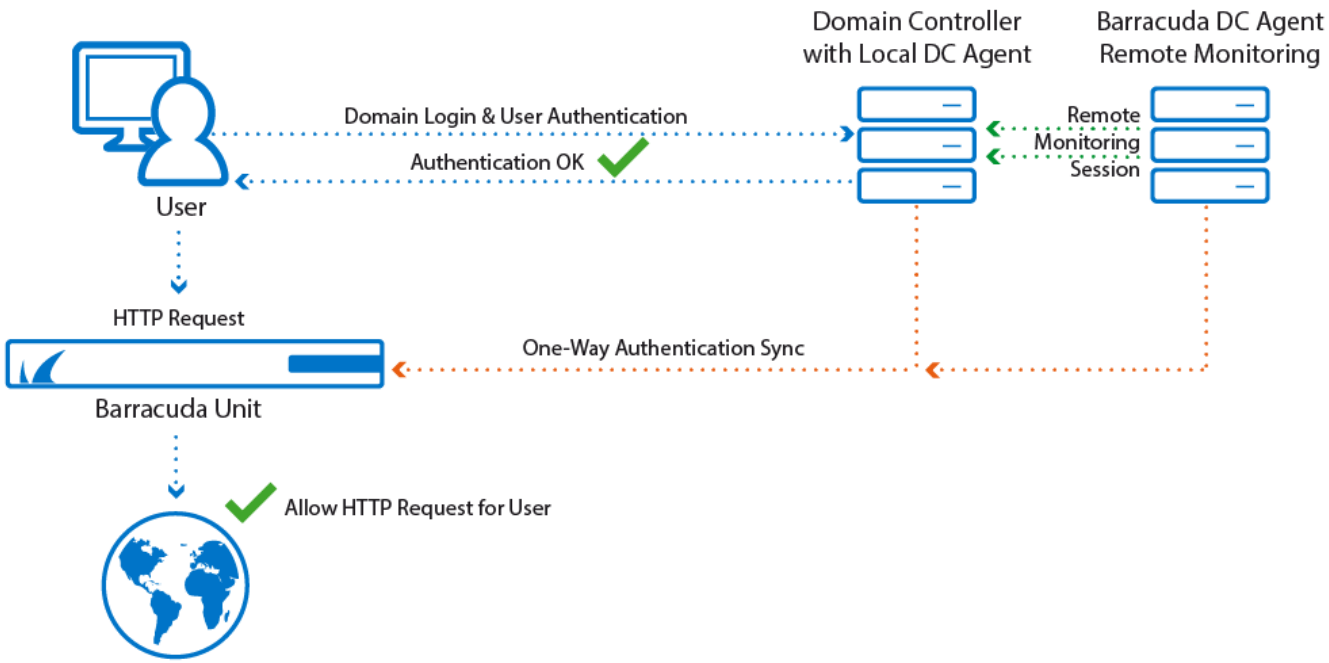
About the Barracuda DC Agent

https://campus.barracuda.com/doc/5472271/

You can install the Barracuda DC Agent either on the domain controller or on a dedicated Windows PC on the office network. The Barracuda DC Agent periodically checks the domain controller for login events and to obtain a record of authenticated users. The IP addresses of authenticated users are mapped to their username and group context. The list of authenticated users is provided to the Barracuda Session Manager on your Barracuda Networks product, allowing true single sign-on capabilities.

Due to the way Apple devices authenticate users with Windows Active Directory, the Barracuda DC Agent is unable to pick up Mac user logins to Windows Active Directory. The Barracuda DC Agent can, however, capture user logins from wireless devices such as iPads or iMacs if the user is authenticating via WAP against a RADIUS server.

A typical use case scenario: Alice comes into her office in the morning and logs into her workstation. She enters her user credentials and is authenticated by the domain controller. The Barracuda DC Agent recognizes that Alice has authenticated herself within the corporate network domain and forwards this information to all connected Barracuda Networks products. These systems now give Alice access to services or network areas for which a valid user or Microsoft Active Directory group context is required. Alice does not need to re-enter any credentials because her initial authentication by Active Directory is reused.



Exclusions

The Barracuda DC Agent lets you manually exclude IP addresses of user client PCs or known multi-user computer systems and provides a "learning mode" that proposes the exclusion of suspicious systems. Due to the complexity of today's network environments and multi-user computer systems, a user-to-IP association is not always possible or required. For example, you can exclude the HTTP Proxy and Terminal Server because they allow multiple users and use a single IP address for authentication against domain controllers.

If you install the Barracuda DC Agent on your domain controller(s) for use with clients authenticating via LDAP, and then later add users in terminal environments using Kerberos or NTLM authentication, you must exclude the IP addresses of these terminal servers in the DC Agent monitor **Filters** tab. These IP addresses are exceptions and associated login events (for LDAP logins) should be ignored by the Barracuda DC Agent. See How to Get and Configure the Barracuda DC Agent for details.

Remote Monitoring

If you install the Barracuda DC Agent on a dedicated computer system instead of the Active Directory server, you can also remotely monitor Active Directory.

Figures

1. DC-Agent-Schematics.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.