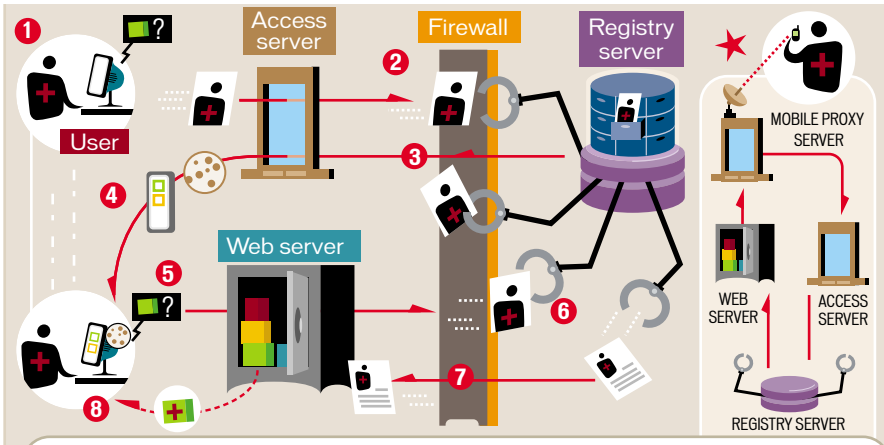
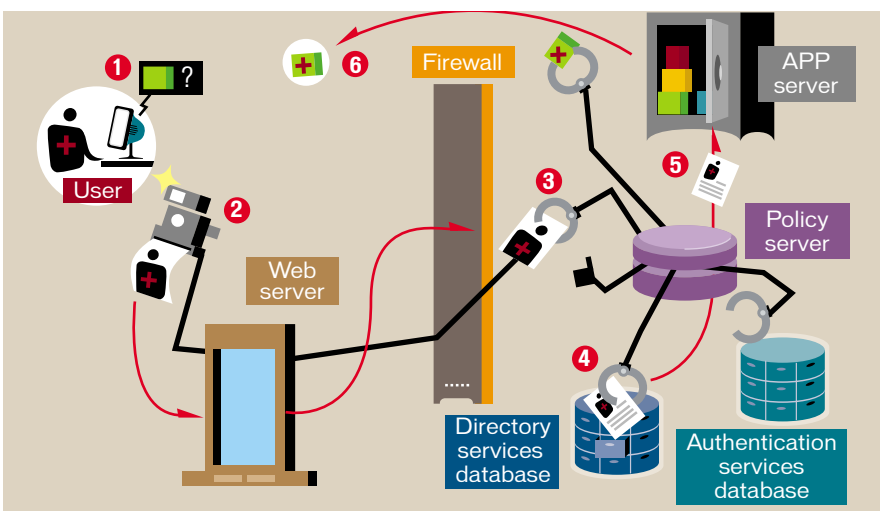
HOW THEY WORK:
THREE APPROACHES TO AUTHORIZATION MANAGEMENT

A Entrust



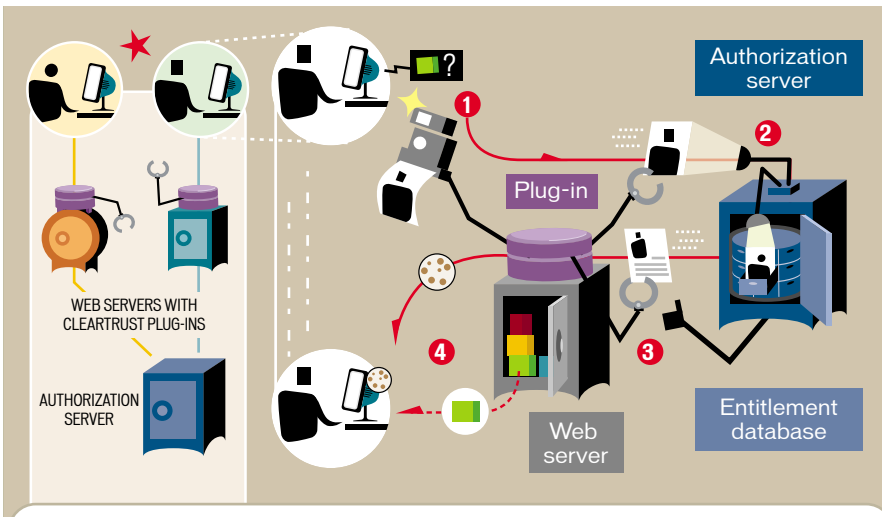
1 With Entrust's GetAccess authorization management system, users navigate to the Access Server's log-in screen to access secure resources. 2 This server passes the authentication request to the Registry Server, 3 which returns user verification and profile information to the Access Server, along with cookies containing the authorized resource list, user roles, and other information. 4 The Access Server encrypts the cookies and returns a custom navigation menu to the user. 5 When the user chooses an application, the runtime service on the Web server intercepts the request, decrypts the cookies, and 6 verifies the session with the Registry Server. 7 The registry server then passes the user ID, preferences, roles and application-specific data to the application on the Web Server so that it can 8 deliver the appropriate level of information to the user. ★ The Mobile Proxy Server manages sessions for cookie-less computers such as wireless devices.

B Netegrity



1 In Netegrity's SiteMinder architecture, when a user requests a protected resource from the Web server, 2 a Web agent pulls the user's credentials from the browser and 3 passes them to the SiteMinder policy server, which in turn 4 authenticates the user using the stored credentials in the directory services or authentication services databases. 5 The policy server passes the information to the application, 6 which personalizes the content based on the user's privileges. Netegrity integrates with existing directories and databases, rather than creating its own.

C Securant



★ Securant's authorization design avoids integration complexities by separating content and applications onto different Web servers. The administrator creates a business rule for each resource on the protected Web site that defines which users are authorized to access which applications. 1 The first time a user requests a protected resource, a ClearTrust plug-in on the Web application server prompts the user for credentials. 2 It passes the results to the authorization server, which polls the Securant entitlement database and 3 returns user authorization information to the plug-in. 4 Finally, the plug-in enforces access control for the resource. An encrypted cookie, passed to the browser, allows for subsequent accesses.