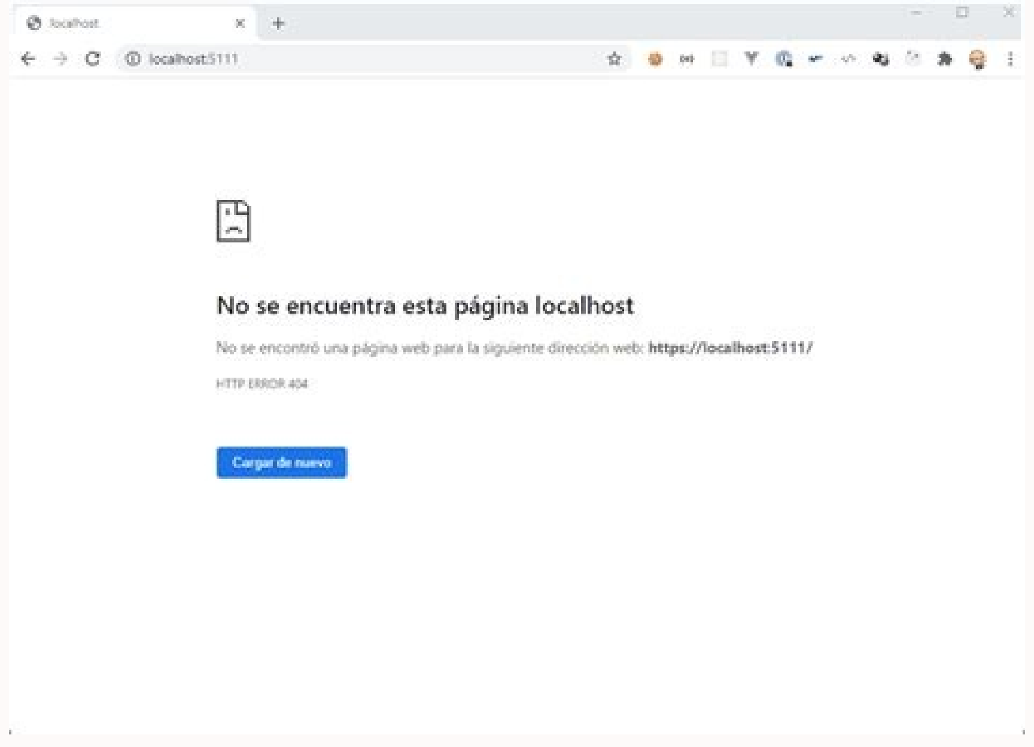
Dangote firewall authentication

Customer has some issues when external users try to logon/authenticate in Cognos from a different Domain using OS signon. Is there any specific port that needs to be opened ? N/A The standard Windows authentication dialog box is displayed.
User/Computer login and authentication The following protocols and ports are required: * TCP/445 and UDP/445; Microsoft-DS for Server Message Block (SMB) over IP traffic * TCP/88 and UDP/88; Kerberos authentication * UDP/389; Lightweight Directory Access Protocol (LDAP) ping * TCP/53 and UDP/53; Domain Name Service (DNS) File access The following protocols and ports are required: * TCP/445 and UDP/445; SMB over IP traffic Establishing an explicit trust between Active Directory (AD) domains The following protocols and ports are required: * TCP/445 and UDP/445; SMB over IP traffic * TCP/389 and TCP/636; LDAP, where 636 is for Secure Sockets Layer (SSL) * UDP/389; LDAP ping * TCP/88 and UDP/88; Kerberos authentication * TCP/53 and UDP/53; DNS Validating and authenticating a trust The following protocols and ports are required: * TCP/445 and UDP/445; SMB over IP traffic * TCP/389 and TCP/636; LDAP * UDP/389; LDAP ping * TCP/88 and UDP/88; Kerberos authentication * TCP/53 and UDP/53; DNS * TCP/135 and UDP/135; Remote Procedure Call (RPC) endpoint mapper * a range of RPC ports, which should be restricted when firewalling AD replication, mutual authentication and Domain Controller (DC) location The following protocols and ports are required: * TCP/135 and UDP/135; RPC endpoint mapper * RPC service port for AD access; you must lock to a fixed port when firewalling * RPC service port for AD replication; you must lock to a fixed port when firewalling * TCP/88 and UDP/88; Kerberos authentication * TCP/389 and TCP/636; LDAP * UDP/389; LDAP ping * TCP/3268 and TCP/3269; Global Catalog (GC) LDAP, where 3269 is for SSL * TCP/445 and UDP/445; SMB over IP traffic * TCP/53 and UDP/53; DNS * UDP/123; Network Time Protocol (NTP) Non-AD ports that are also required The following protocols and ports are required: * TCP/137 and UDP/137; Network Basic Input-Output System (NetBIOS) name service * UDP/138; NetBIOS datagram service * TCP/139; NetBIOS session service [{"Product":{"code":"SS9S5U","label":"Cognos 8 Planning"},"Business Unit":{"code":"BU053","label":"Cloud & Data Platform"},"Component":"Contributor","Platform":[{"code":"PF033","label":"Windows"}],"Version":"8.1","Edition":"","Line of Business":{"code":"LOB10","label":"Data and AI"}},{"Product":{"code":"SSPN2D","label":"Cognos Planning"},"Business Unit":{"code":"BU059","label":"IBM Software w\/o TPS"},"Component":"Contributor","Platform":[{"code":"PF033","label":"Windows"}],"Version":"8.1","Edition":"","Line of Business":{"code":"LOB10","label":"Data and AI"}}]   Select Configure>Access>FW Authentication in the J-Web user interface if you are using SRX5400, SRX5600, or SRX5800 platforms.OrSelect Configure>Authentication>FW Authentication in the J-Web user interface.The Firewall Authentication configuration page appears. Table 1 explains the contents of this page.(Junos OS Release 19.1R1 and later releases) Select Configure>Users>FW Authentication in the J-Web user interface.The Firewall Authentication configuration page appears. Table 1 explains the contents of this page.Click one:OK/Save—Saves the configuration and returns to the main configuration page.Commit Options>Commit—Commits the configuration and returns to the main configuration page.Reset—Resets your entries and returns to the main configuration page.Cancel—Cancels your entries and returns to the main configuration page.Table 1: Add Firewall Authentication Configuration DetailsField FunctionActionPass-through SettingsDefault ProfileSpecifies the profile that the policies use to authenticate users.

The options available are:Nonestu-access-profilejuniper-access-profileSelect an option.HTTP BannerLoginDisplays the login prompt for users logging in using HTTP.–FailedDisplays failed login prompt for users logging in using HTTP.–SuccessDisplays a successful login prompt for users logging in using HTTP.–FTP BannersLoginDisplays the login prompt for users logging in using FTP.–FailedDisplays failed login prompt for users logging in using FTP.–SuccessDisplays a successful login prompt for users logging in using FTP.–Telnet BannersLoginDisplays the login prompt for users logging in using telnet.–FailedDisplays failed login prompt for users logging in using telnet.–SuccessDisplays a successful login prompt for users logging in using telnet.–Web-auth-settingsDefault ProfileSpecifies the profile that the policies use to authenticate users. The options available are:Nonestu-access-profilejuniper-access-profileSelect an option.Banner SuccessDisplays a successful login prompt for users logging in using Web authentication banner.–Web-auth logo uploadLogo imageIndicates an image to be chosen for the Web authentication logo.Note: For the good logo image, the image format must be in .gif and the resolution must be 172x65.–BrowseNavigates to the available logo image on the user's local disk.Navigate to the logo image.Upload FileUploads the image.Click the button to upload the image.Restore Juniper logoRestores the default Juniper Networks logo.Click the button to restore the Juniper Networks logo.   data-mc-breadcrumbs-count=6 data-mc-toc=True> To enable your users to authenticate, you create user accounts and groups. When a user connects to the Authentication Portal with a web browser on a computer or mobile device and authenticates to the Firebox, the user credentials and computer IP address are used to find whether the configuration includes a policy that applies to the traffic that the computer sends and receives. To create a Firebox user account: After you have added a user to a group and created policies to manage the traffic for the user, the user can open a web browser on a computer or mobile device to authenticate to the Firebox. To require multi-factor authentication (MFA) when a user authenticates, specify AuthPoint as the authentication server for the user or group. To enable and use AuthPoint as an authentication server your Firebox must runFireware v12.7 or higher and you must configure a Firebox resource in AuthPoint. For detailed steps to configure AuthPoint MFA for the Firebox Authentication Portal, go to Firebox Authentication with AuthPoint.

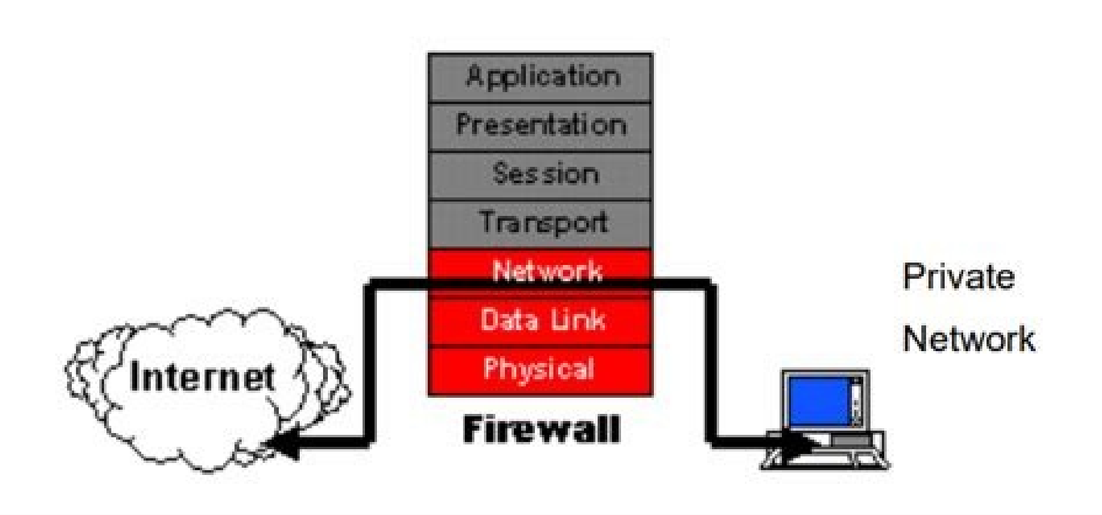


No se encuentra esta página localhost

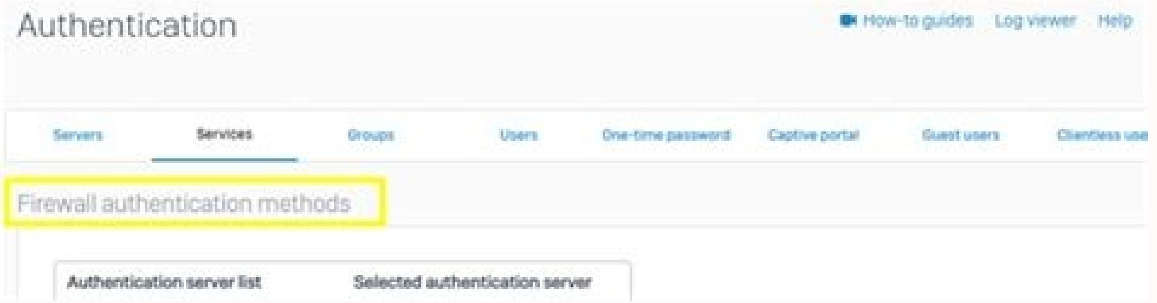
No se encontró una página web para la siguiente dirección web: **https://localhost:5111/**

HTTP ERROR 404

In Fireware v12.5.5 or higher, connections to pages served by the Firebox Web Server must use TLS 1.2 or higher. If you have configured the Firebox with an IPv4 or an IPv6 address, you can use either the IPv4 or the IPv6 address to authenticate to the device over port 4100. To authenticate with an HTTPS connection to the Firebox over port 4100: In a web browser, go to https://:4100.The login page appears. Type the Username and Password. From the Domain drop-down list, select the domain to use for authentication.This option only appears if you can choose from more than one domain. Click Login.



If the credentials are valid, the user is authenticated. Firewall authentication takes precedence over Single Sign-On (SSO) and replaces the user credentials and IP address from your SSO session with the user credentials and IP address you select for Firewall authentication. For more information about how to configure SSO, go to How Active Directory SSO Works.



Related Topics About User Authentication Configure Firebox Account Lockout Settings Add Policies to Your Configuration