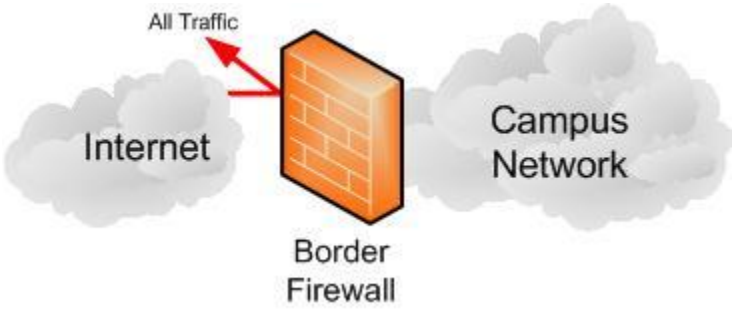
Firewall Overview

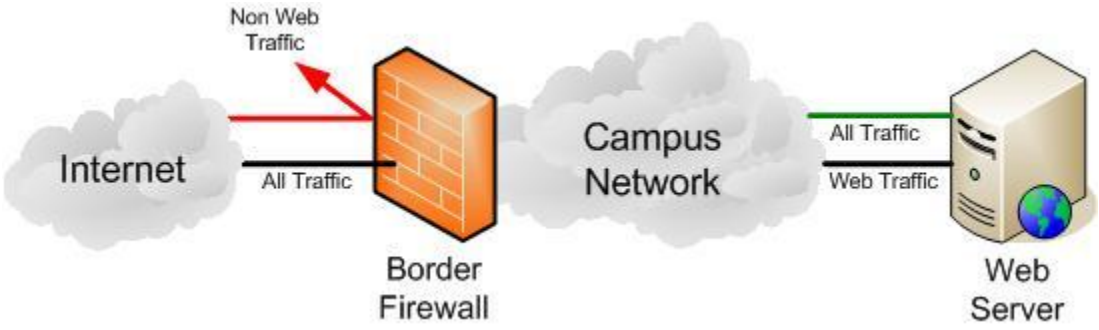
Firewall Overview

The Chico State campus utilizes a closed border firewall to help protect campus resources by preventing unauthorized access to campus systems from the Internet. The closed border firewall only filters traffic coming into the campus network from the Internet, traffic originating from campus systems freely interact with systems on the Internet. The philosophy behind a closed border firewall is that only those systems requiring access by systems outside the firewall have rules to allow traffic to their services. The closed border firewall automatically protects new systems brought online within the firewall perimeter because access rules do not exist in the firewall configuration. The closed border firewall only protects the border of the campus. Systems residing within the perimeter of the border firewall are still susceptible from attacks originating on other campus systems.



Firewall Exceptions

Firewall exceptions are rules that allow access to campus servers from the Internet. The following diagram illustrates a firewall exception for a web server with HTTP and HTTPS services. The port numbers for these services are 80 and 443 respectively and allow the server to serve websites to the Internet as well as encrypted access to the websites.

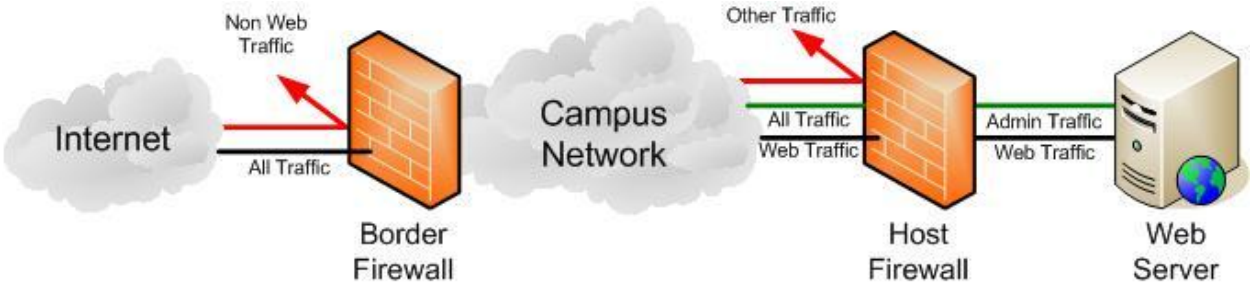


The Information Security Office analyzes all firewall exception requests prior to approval.

Firewall Best Practices

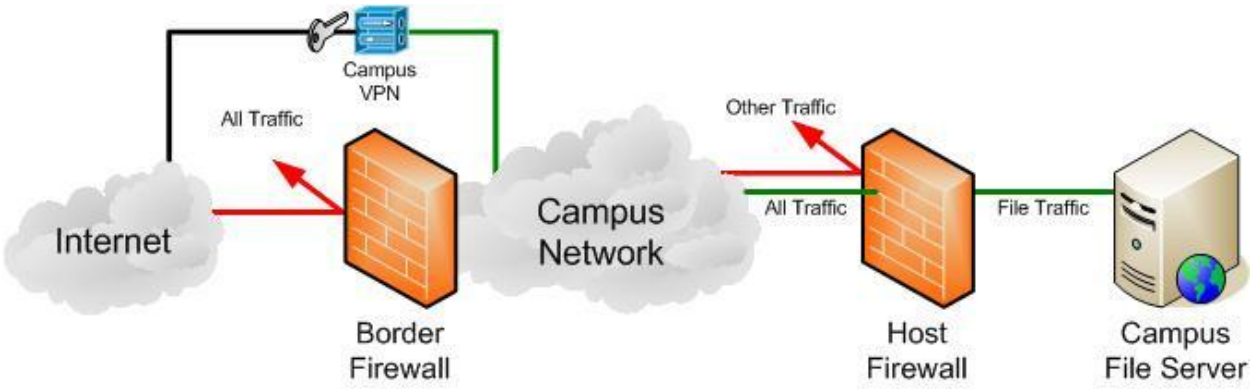
A correctly configured firewall will allow access services only by authorized users or systems. The closed border firewall protects campus resources from malicious users and systems on the Internet but does not address malware or issues residing on the campus network. To protect against threats originating from within the campus network the Information Security Office recommends using a host-based firewall as a best practice.

The following diagram illustrates how the campus border firewall and host-based firewall work in conjunction to limit access only to the HTTP and HTTPS services running on a web server on the campus network. The host-based firewall continues to allow access to the HTTP and HTTPS services, but further restricts access to the web server by allowing only system management protocols from campus systems.

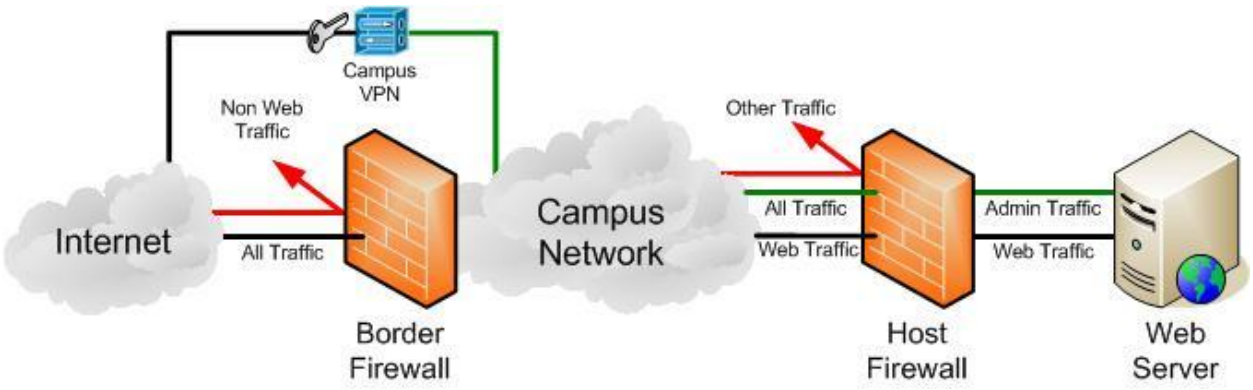


Virtual Private Networks (VPN)

The following diagram illustrates a common scenario where campus users store files on a campus file server. The border firewall blocks all access to the file server and the host-based firewall allows only access to the file services from campus resources. The Campus VPN allows campus users to authenticate to the campus network and gain access to the services provided by the file server.



The following diagram illustrates another common scenario where System Administrators use the Campus VPN to connect to the web server via management protocols from off campus.



The following diagram illustrates the preferred scenario for server administrators and vendors connecting to the web server via management protocols over a special management VPN. This diagram also illustrates the best practice of having server administrator management stations reside on a management subnet with limited access by the campus network.