BURSTEK™

The World's Choice for Internet Security.

Internet Access Policies

A new CEO has just been appointed to oversee a large manufacturing company. The outgoing CEO, while friendly, was replaced by the Board of Directors for falling production numbers and increased Information Technology costs.

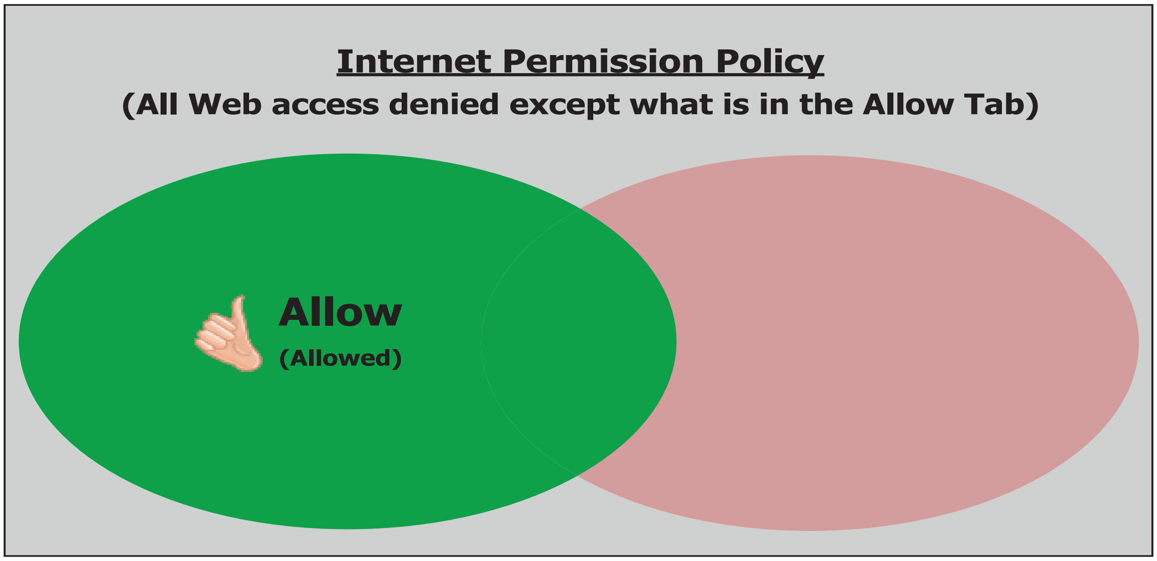
The new CEO sits down with his department heads to discuss the various issues and how to resolve them. A re-occurring theme begins to emerge - employees are spending a lot of time surfing the Web instead of working. Streaming media sites playing Internet radio can be heard around the office; virus and malware infections have increased causing major outages and costly downtime; the company no-longer has a safe working environment due to accidental downloads of inappropriate materials.

The CEO realizes that 'cyber slacking' occurs whenever employees have access to the Web; however, he recognizes far greater risks include litigation, regulatory investigations, security breaches, business interruptions, lost productivity, and malicious intruder attacks. He immediately implements an Internet Acceptable Use Policy. Responsibility for ensuring adherence to this new policy is assigned to the department heads; enforcement of same policy is assigned to Human Resources.

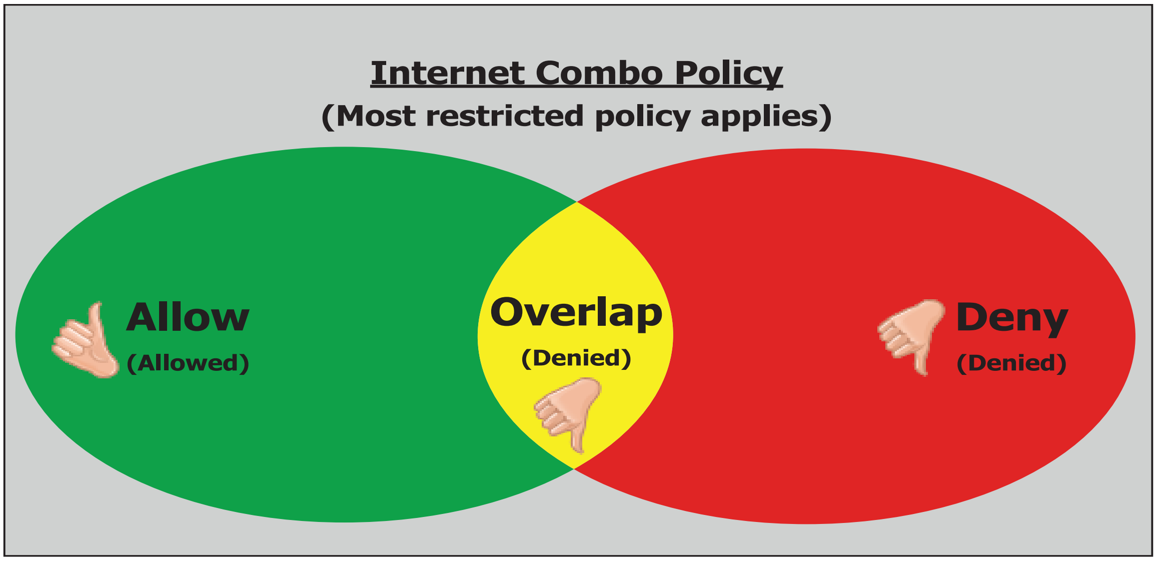
The Department heads quickly turn to the CIO and present their requirements. They need to view their individual department's Internet activity to identify any breaches to the company AUP. They also want to ensure that access to supplier and business websites is not interrupted.

The CIO chooses Burstek's bt-WebFilter and bt-LogAnalyzer suite because of its ease of use, customization, and flexibility. WebFilter will block and control access based on departmental requirements. LogAnalyzer's reporting will help Human Resources ensure enforcement of the AUP.

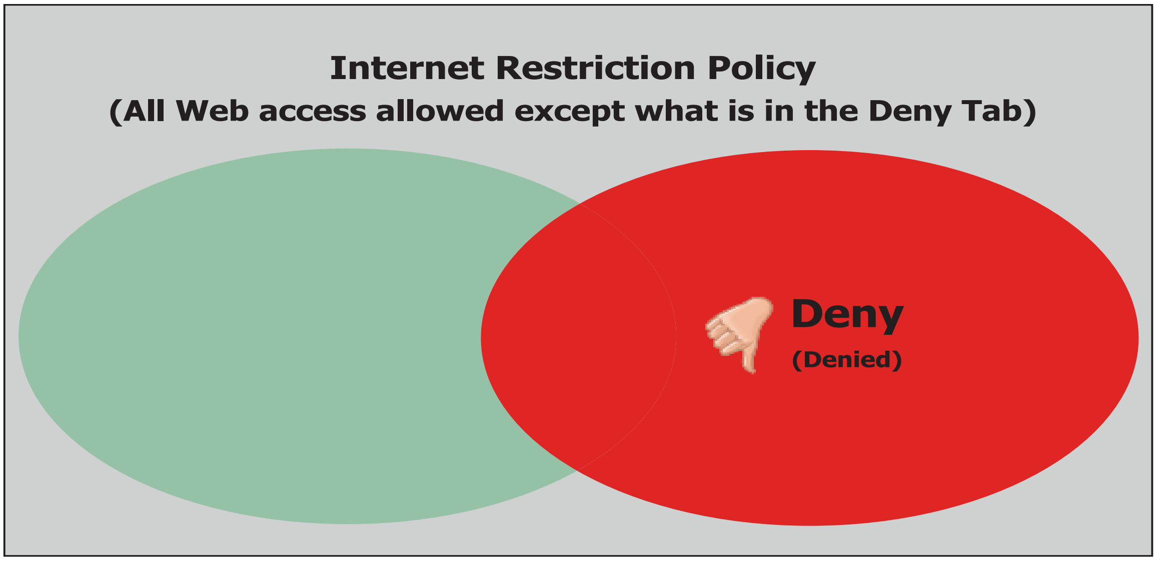
For the Production and Shipping departments, a **'Permissions Policy'** type is chosen. This policy prevents all access to the Internet except for websites specifically authorized.


Internet Permission Policy
(All Web access denied except what is in the Allow Tab)
Allow
(Allowed)

For the Marketing department, a **'Combination Policy'** type is implemented. This provides the flexibility of allowing access to specific areas of a website instead of the whole website.



For the remaining departments, a **'Restriction Policy'** is selected allowing full Internet access for all users except to sites/categories specifically denied including additional URL's that the department may wish to exclude.


Internet Restriction Policy
(All Web access allowed except what is in the Deny Tab)
Deny
(Denied)

The following day each department head received a customized report for their department listing their users and the categories visited.
The CIO and CEO each received a report detailing usage statistics for the entire company.