

## Cisco CBAC – The Poor Mans Firewall

### CBAC Overview

The Cisco IOS Firewall Feature Set is a module that can be added to the existing IOS to provide firewall functionality without the need for hardware upgrades. There are two components to the Cisco IOS Firewall Feature Set in Intrusion Detection (which is an optional bolt-on) and Context-Based Access Control (CBAC). CBAC maintains a state table for all of the outbound connections on a Cisco router by inspecting tcp and udp connections at layer seven of the OSI model and populating the table accordingly. When return traffic is received on the external interface it is compared against the state table to see if the connection was originally established from within the internal network, and then either permitted or denied. Although basic this is a very effective mechanism to prevent unauthorized access to the internal network from external sources such as the internet.

### CBAC Application-specific support

Cisco have also built in some additional functionality into CBAC in terms of application-specific inspection that enables the router to recognize and identify application specific data flows such as HTTP, SMTP, TFTP, and FTP. Understanding these applications and their data flows empowers the router to identify malformed packets or suspect application data flows and permit or deny accordingly. CBAC also provides the flexibility of downloading Java code from trusted sites, but it denying untrusted sites.

### CBAC and Denial of Service (DOS) Attacks

Denial-Of-Service (DOS) attack protection is also in-built with real-time logging of alerts as well as pro-active responses to mitigate the threat. To do this CBAC can be configured to manage half-open TCP connections which are used in TCP SYN flood attacks to overload a targets resources resulting in a denial of service to legitimate users. To do this CBAC uses timeouts and thresholds, which are configurable, to determine how long state information for each connection should be kept for sessions and when to drop them. Note that UDP and ICMP require that an idle-timer limit is used to determine when a connection should be terminated. A very useful command to identify a DOS attack is 'ip inspect audit-trail' which logs all DOS connections including source and destination IP address and TCP or UDP ports allowing you to pin-point the exact source and destination of the attack.

### Configuring CBAC

There are five steps to configuring CBAC on a Cisco router in order for it to function correctly. These are as follows:

1. Choose an interface to which inspection will be applied. This can be an internal or external interface as CBAC is only concerned with the direction of the first packet initiating the connection which is identified when applying CBAC to an interface.
2. Configure an IP access list in the correct direction on the selected interface to allow traffic through for CBAC to inspect.
3. Configure global timeouts and thresholds for established connections or sessions.
4. Define an inspection rule specifying exactly which protocols will be inspected by CBAC.
5. Apply the inspection rule to the interface in the correct direction.

### About the Author

Nicholas Evra is a Senior IT Consultant for a Professional Services IT Organisation based in London, UK. As well as designing and developing network and security solutions for clients, Nicholas also regularly contributes technical tips and articles on [Networkblue.net](http://Networkblue.net). Networkblue.net is a technical resource for novices and expert's alike providing free articles and tips on numerous cisco topics such as [Cisco's CBAC](#) and other [network security](#) topics.

Source: <http://www.articlemint.com>