WIKIPEDIA

# Context-based access control

**Context-based access control** (**CBAC**) is a feature of firewall software, which intelligently filters TCP and UDP packets based on application layer protocol session information. It can be used for intranets, extranets and internets.[1]

CBAC can be configured to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network needing protection. (In other words, CBAC can inspect traffic for sessions that originate from the external network.) However, while this example discusses inspecting traffic for sessions that originate from the external network, CBAC can inspect traffic for sessions that originate from either side of the firewall. This is the basic function of a stateful inspection firewall.[2]

Without CBAC, traffic filtering is limited to access list implementations that examine packets at the network layer, or at most, the transport layer. However, CBAC examines not only network layer and transport layer information but also examines the application-layer protocol information (such as FTP connection information) to learn about the state of the TCP or UDP session.[3] This allows support of protocols that involve multiple channels created as a result of negotiations in the FTP control channel. Most of the multimedia protocols as well as some other protocols (such as FTP, RPC, and SQL*Net) involve multiple control channels.

CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions (sessions that originated from within the protected internal network).

CBAC works through deep packet inspection and hence Cisco calls it 'IOS firewall' in their Internetwork Operating System (IOS).

CBAC also provides the following benefits:

- Denial-of-service prevention and detection
- Real-time alerts and audit trails

## See also

- Access control list
- Attribute-based access control (ABAC)
- Discretionary access control (DAC)
- Graph-based access control (GBAC)
- Lattice-based access control (LBAC)
- Mandatory access control (MAC)
- Organisation-based access control (OrBAC)
- Role-based access control (RBAC)
- Rule-set-based access control (RSBAC)
- Capability-based security
- Location-based authentication

- Risk-based authentication
- Role hierarchy

## References

1. "Context-Based Access Control" (https://www.techtutsonline.com/context-based-access-control/). *TechTutsOnline*. 2015-09-11. Retrieved 2019-05-22.
2. "Context-Based Access Control (CBAC): Introduction and Configuration" (https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/13814-32.html). *Cisco*. Retrieved 2019-05-22.
3. Dan, Author (2012-03-09). "Context-Based Access Control (CBAC)" (http://danscourses.com/context-based-access-control-cbac/). *Danscourses*. Retrieved 2019-05-22.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Context-based_access_control&oldid=988427203"

**This page was last edited on 13 November 2020, at 02:49 (UTC).**