Contents

Introduction

CBAC (Context-Based Access Conrol)

CBAC provides statefull application layer filtering, including support for unorthodox protocols and multimedia applications. It can examine supported connections for embedded NAT and PAT information and perform the necessary translations. In addition, it can open additional statefull connections for supported applications, such as FTP and H.323.

Features offered by CBAC

Port mapping:- Allows the mapping of ports so that CBAC can perform its application inspection correctly, such as assigning FTP to port 1024 if your FTP server is processing traffic on this port.

Filtering of Java applets:- Filters embedded Java applets on HTTP connections, allowing you to block known malicious sites.

DoS protection:- Detects and prevents Denial of Service (DoS) attacks by limiting the number of connections that a device can set up.

CBAC also provides real time alerts and audit trails.

NOTE:- All the inspection features are applied globally while using CBAC, we don?t have flexibility to do inspection for certain network or interested traffic flow with respect to ip addressing scheme.In order to accomplish the same we can use advance level of IOSFW feature set known as ZBFW(Zone Based Firewall).

Here are the steps to configure CBAC

Step 1. Identify the interfaces as internal and external on your router.

Step 2. Configure the IP ACL rules to filter traffic based on your requiremnet.

Step 3. Now we can change the global timeout values for connections as per requirement.

Step 4. In case if the application is using a nonstandard port number, such as FTP with 1024.Configure Port Application Mapping (PAM).

Step 5. As a next step Configure inspection rules. These rules define what entries are added to the state table and CBAC will open up pin holes for the returning traffic in the ACL rules applied in the opposite direction with respect to inspection rules.

Step 6. Now apply the inspection rules to the respective interface of the router.

Step 7. Final step would be to test the CBAC configuration by passing some interested traffic through the router running CBAC in order to validate the configuration is fine.

Design

Scenario below shows how we can enable IOSFW(CBAC) on a Router.

Internet???(WAN)Router/CBAC(LAN)???Inside host

Router outside interface 1.1.1.1 Router inside interface 192.168.10.1 Inside Host 192.168.10.2 Natted ip address for Inside Host 1.1.1.4

Configuration

```
ip inspect name IOSFW icmp router-traffic
ip inspect name IOSFW tcp router-traffic
ip inspect name IOSFW udp router-traffic

access-list 151 deny ip any any

interface FastEthernet0/0
description **WAN**
ip address 1.1.1.1 255.255.255.0
ip access-group 151 in
ip nat outside
no shut

interface FastEthernet0/1
description **LAN**
ip address 192.168.10.1 255.255.255.0
ip nat inside
ip inspect IOSFW in
no shut

CBAC(config)#ip inspect audit-trail
CBAC(config)#logging buffered debugging
CBAC(config)#logging on
CBAC#
*Mar  1 00:38:30.851: %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session: initiator (192.168.10.2:561

CBAC#sh ip inspect sessions
Established Sessions
Session 669F632C (192.168.10.2:56162)=>(2.2.2.2:23) tcp SIS_OPEN


CBAC#sh ip inspect sessions detailEstablished Sessions
 Session 669F632C (192.168.10.2:56162)=>(2.2.2.2:23) tcp SIS_OPEN
  Created 00:00:11, Last heard 00:00:05
  Bytes sent (initiator:responder) [42:90]
  In  SID 2.2.2.2[23:23]=>1.1.1.4[56162:56162] on ACL INBOUND  (18 matches)
```

Note:

- Turn off inspect for unused protocols(Only use what you require).
- By using the command *router-traffic* along with the desired protocol, inspection is enabled of sessions to/from the router (in addition to session through the router)

Related show Commands

This section provides information you can use to confirm your configuration is working properly.

Other Show Commands

show ip inspect config

show ip inspect interfaces

show ip inspect stat

Debug Commands

debug ip inspect detail

debug ip inspect tcp

debug ip inspect object-cre

debug ip inspect object-del

debug ip inspect event

Certain show commands are supported by the Output Interpreter Tool (registered customers only), which allows you to view an analysis of show command output.

Related Information

Technical Support & Documentation - Cisco Systems