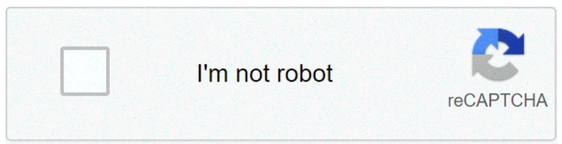

Continue

How to configure zone based firewall on cisco ios

IntroductionThe Cisco IOS Zone Based Firewall is one of the most advanced form of Stateful firewall used in the Cisco IOS devices. The zone based firewall (ZBFW) is the successor of Classic IOS firewall or CBAC (Context-Based Access Control). Cisco first implemented the router-based stateful firewall in CBAC where it used ip inspect command to inspect the traffic in layer 4 and layer 7.Even though ASA devices are considered as the dedicated firewall devices, Cisco integrated the firewall functionality in the router which in fact will make the firewall a cost effective device. The zone based firewall came up with many more features that is not available in CBAC. The ZBFW mainly deals with the security zones, where we can assign the router interfaces to various security zones and control the traffic between the zones. Also the traffic will be dynamically inspected as it passes through the zones. In addition to all the features which is available in classic IOS firewall, Zone based firewall will support Application inspection and control for HTTP, POP3, Sun RPC, IM Applications and P2P File sharing.For advanced configuration of IOS Zone Based Firewall refer Based Firewall Vs CBACCBACZone Based FirewallInterface Based ConfigurationZone Based ConfigurationControls Inbound and Outbound access on an interfaceControls Bidirectional access between zones.Uses inspect statements and stateful ACLsUses Class-Based Policy language-Not supported-Support Application Inspection and ControlSupport from IOS Release 11.2Support from IOS Release 12.4 (6) TThis document will guide you to configure a basic Zone Based Policy Firewall in an IOS router. Here I am going to divide the entire configuration into logical sets and finally will combine them to the get the full configuration.ZBFW Configuration ProcedureThe below are the configuration tasks that you need to follow:Configure ZonesAssign Router Interfaces to zonesCreate Zone PairsConfigure Interzone Access Policy (Class Maps & Policy Maps)Apply Policy Maps to Zone PairsConfiguration ScenarioFigure 1.In this example we have three zones.Inside Zone - Private LANDMZ Zone - DMZ hostsOutside Zone - InternetHere I am defining a rule set for our ZBFW:1. From Inside to Outside -http,icmp and pop3 is allowed2. From Outside to Inside -icmp is allowed3. From Inside to DMZ -http and icmp is allowed4. From Outside to DMZ -http is allowedDefault Rules of Zone Based FirewallInterzone communication is Denied, traffic will be denied among the interfaces that are in the different zones unless we specify a firewall policy.Intrazone communication is Allowed, traffic will flow implicitly among the interfaces that are in the same zone.All traffic to Self zone is AllowedSelf Zone is created automatically by the router while we create the other zones in a Zone Based Firewall.Task 1 : Configure ZonesIn this example (refer Figure 1) we have three zones. Inside ,Outside, DMZ.To configure zones in a router, connect the router via putty or console, switch to the global configuration mode and type the command as below:Router(config)#zone security INSIDERouter(config)#zone security OUTSIDERouter(config)#zone security DMZTask 2 : Assign Router Interfaces to ZonesWe have to assign the router interface to a particular zone. Here I am going to assign Gigabyte Ethernet 0/0 to INSIDE zone , Ge0/1 to OUTSIDE zone and Ge0/2 to DMZ zone.To achieve this we have to go to the particular interface and attach that interface to the zone.Type the command as below:Router(config)#interface gigabitEthernet 0/0Router(config-if)#zone-member security INSIDERouter(config)#interface gigabitEthernet 0/1Router(config-if)#zone-member security OUTSIDERouter(config)#interface gigabitEthernet 0/2Router(config-if)#zone-member security DMZNow if you try to ping a zone from another zone the traffic will be denied because of the default firewall policy.Task 3 : Create Zone PairsZone pairs are created to connect the zones. If you want to make two zones to communicate you have to create Zone pairs. DO NOT create zone pairs for non-communicating zones. In our scenario the traffic flows between :INSIDE to OUTSIDEOUTSIDE to INSIDEOUTSIDE to DMZINSIDE to DMZSo we need to create four zone pairs. To create zone pairs the command is as follows.Router(config)#zone-pair security IN-TO-OUT source INSIDE destination OUTSIDERouter(config)#zone-pair security OUT-TO-IN source OUTSIDE destination INSIDERouter(config)#zone-pair security OUT-TO-DMZ source OUTSIDE destination DMZRouter(config)#zone-pair security IN-TO-DMZ source INSIDE destination DMZTask 4 : Configure Interzone Access PolicyInterzone Access policy is the key part of a Zone based firewall where we classify the traffic and apply the firewall policies. Class map and Policy map configurations are carried out during this task.Class Maps : This will classify the trafficPolicy Maps : This will decide the 'fate' of the trafficClass Map ConfigurationClass map sort the traffic based on the following criteria 1.) Access-group 2.) Protocol 3.) A subordinate class map. In our scenario I am sorting the traffic based on access group. So first we need to create an ACL and associate it with the class map.a.) Class Map for INSIDE-TO-OUTSIDERouter(config)#ip access-list extended INSIDE-TO-OUTSIDERouter(config-ext-nacl)#permit tcp 172.17.0.0 0.0.255.255 any eq wwwRouter(config-ext-nacl)#permit tcp 172.17.0.0 0.0.255.255 any eq pop3Router(config-ext-nacl)#permit icmp 172.17.0.0 0.0.255.255 anyRouter(config)#class-map type inspect match-all INSIDE-TO-OUTSIDE-CLASSRouter(config-cmap)#match access-group name INSIDE-TO-OUTSIDEor [you can group the protocols as below:class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS description Allowed_Protocol_From_INSIDE_to_OUTSIDE match protocol https match protocol dns match protocol udp match protocol tcp match protocol pop3 match protocol smtp match protocol icmp]b.) Class Map for OUTSIDE-TO-INSIDERouter(config)ip access-list extended OUTSIDE-TO-INSIDERouter(config-ext-nacl)#permit icmp any 172.17.0.0 0.0.255.255Router(config)#class-map type inspect match-all OUTSIDE-TO-INSIDE-CLASSRouter(config)#match access-group name OUTSIDE-TO-INSIDEc.) Class Map for OUTSIDE-TO-DMZRouter(config)#ip access-list extended OUTSIDE-TO-DMZRouter(config-ext-nacl)#permit tcp any 192.168.1.0 0.0.0.255 eq wwwRouter(config)#class-map type inspect match-all OUTSIDE-TO-DMZ-CLASSRouter(config)#match access-group name OUTSIDE-TO-DMZd.) Class Map for INSIDE-TO-DMZRouter(config)#ip access-list extended INSIDE-TO-DMZRouter(config-ext-nacl)#permit tcp 172.17.0.0 0.0.255.255 192.168.1.0 0.0.0.255 eq wwwRouter(config-ext-nacl)#permit icmp 172.17.0.0 0.0.255.255 192.168.1.0 0.0.0.255Router(config)#class-map type inspect match-all INSIDE-TO-DMZ-CLASSRouter(config-cmap)#match access-group name INSIDE-TO-DMZPolicy-Map ConfigurationPolicy-Maps will apply the firewall policy to the class map that is configured previously. Three actions can be taken aganist the traffic with the policy-map configuration:Inspect : Dynamically inspect the traffic.Drop : Drop the trafficPass : Simply forward the traffic.There will be a drop policy, by default, at the end of all policy maps.a.) Policy-map for INSIDE-TO-OUTSIDERouter(config)#policy-map type inspect INSIDE-TO-OUTSIDE-POLICYRouter(config-pmap)#class type inspect INSIDE-TO-OUTSIDE-CLASSRouter(config-pmap)#inspectRouter(config-pmap)#class class-defaultRouter(config-pmap)#drop logb.) Policy-map for OUTSIDE-TO-INSIDERouter(config)#policy-map type inspect OUTSIDE-TO-INSIDE-POLICYRouter(config-pmap)#class type inspect OUTSIDE-TO-INSIDE-CLASSRouter(config-pmap)#passRouter(config-pmap)#class class-defaultRouter(config-pmap)#drop logc.) Policy-map for OUTSIDE-TO-DMZRouter(config)#policy-map type inspect OUTSIDE-TO-DMZ-POLICYRouter(config-pmap)#class type inspect OUTSIDE-TO-DMZ-CLASSRouter(config-pmap)#inspectRouter(config-pmap)#class class-defaultRouter(config-pmap)#drop logd.) Policy-map for INSIDE-TO-DMZRouter(config)#policy-map type inspect INSIDE-TO-DMZ-POLICYRouter(config-pmap)#class type inspect INDISE-TO-DMZ-CLASSRouter(config-pmap)#passRouter(config-pmap)#class class-defaultRouter(config-pmap)#drop logTask 5 : Apply policy maps to zone pairsNow we have to attach the policy maps to the zone pairs that we have already created. The command is as follows:Router(config)#zone-pair security IN-TO-OUT source INSIDE destination OUTSIDERouter(config-sec-zone-pair)#service-policy type inspect INSIDE-TO-OUTSIDE-POLICYRouter(config)#zone-pair security OUT-TO-IN source OUTSIDE destination INSIDERouter(config-sec-zone-pair)#service-policy type inspect OUTSIDE-TO-INSIDE-POLICYRouter(config)#zone-pair security OUT-TO-DMZ source OUTSIDE destination DMZRouter(config-sec-zone-pair)#service-policy type inspect OUTSIDE-TO-DMZ-POLICYRouter(config)#zone-pair security IN-TO-DMZ source INSIDE destination DMZRouter(config-sec-zone-pair)#service-policy type inspect INSIDE-TO-DMZ-POLICYThere we finish the basic configuration of a zone based firewall.TroubleshootingYou can use the below commands to perform some basic troubleshooting and verification.a.) Show commandsshow class-map type inspectshow policy-map type inspectshow zone-pair securityb.) Debug Commandsdebug policy-firewall detaildebug policy-firewall eventsdebug policy-firewall protocol tcpdebug policy-firewall protocol udpAdvanced Zone Based Firewall ConfigurationHere you can find some examples of advanced Zone Based Firewall configuration. 1. Advanced Zone Based Firewall Configuration : 2. IOS Content Filtering : . P2P and IM Application control : can visit for more details.Thank you for viewing this document. Page 2 IntroductionThe Cisco IOS Zone Based Firewall is one of the most advanced form of Stateful firewall used in the Cisco IOS devices. The zone based firewall (ZBFW) is the successor of Classic IOS firewall or CBAC (Context-Based Access Control). Cisco first implemented the router-based stateful firewall in CBAC where it used ip inspect command to inspect the traffic in layer 4 and layer 7.Even though ASA devices are considered as the dedicated firewall devices, Cisco integrated the firewall functionality in the router which in fact will make the firewall a cost effective device. The zone based firewall came up with many more features that is not available in CBAC. The ZBFW mainly deals with the security zones, where we can assign the router interfaces to various security zones and control the traffic between the zones. Also the traffic will be dynamically inspected as it passes through the zones. In addition to all the features which is available in classic IOS firewall, Zone based firewall will support Application inspection and control for HTTP, POP3, Sun RPC, IM Applications and P2P File sharing.For advanced configuration of IOS Zone Based Firewall refer Based Firewall Vs CBACCBACZone Based FirewallInterface Based ConfigurationZone Based ConfigurationControls Inbound and Outbound access on an interfaceControls Bidirectional access between zones.Uses inspect statements and stateful ACLsUses Class-Based Policy language-Not supported-Support Application Inspection and ControlSupport from IOS Release 11.2Support from IOS Release 12.4 (6) TThis document will guide you to configure a basic Zone Based Policy Firewall in an IOS router. Here I am going to divide the entire configuration into logical sets and finally will combine them to the get the full configuration.ZBFW Configuration ProcedureThe below are the configuration tasks that you need to follow:Configure ZonesAssign Router Interfaces to zonesCreate Zone PairsConfigure Interzone Access Policy (Class Maps & Policy Maps)Apply Policy Maps to Zone PairsConfiguration ScenarioFigure 1.In this example we have three zones.Inside Zone - Private LANDMZ Zone - DMZ hostsOutside Zone - InternetHere I am defining a rule set for our ZBFW:1. From Inside to Outside -http,icmp and pop3 is allowed2. From Outside to Inside -icmp is allowed3. From Inside to DMZ -http and icmp is allowed4. From Outside to DMZ -http is allowedDefault Rules of Zone Based FirewallInterzone communication is Denied, traffic will be denied among the interfaces that are in the different zones unless we specify a firewall policy.Intrazone communication is Allowed, traffic will flow implicitly among the interfaces that are in the same zone.All traffic to Self zone is AllowedSelf Zone is created automatically by the router while we create the other zones in a Zone Based Firewall.Task 1 : Configure ZonesIn this example (refer Figure 1) we have three zones. Inside ,Outside, DMZ.To configure zones in a router, connect the router via putty or console, switch to the global configuration mode and type the command as below:Router(config)#zone security INSIDERouter(config)#zone security OUTSIDERouter(config)#zone security DMZTask 2 : Assign Router Interfaces to ZonesWe have to assign the router interface to a particular zone. Here I am going to assign Gigabyte Ethernet 0/0 to INSIDE zone , Ge0/1 to OUTSIDE zone and Ge0/2 to DMZ zone.To achieve this we have to go to the particular interface and attach that interface to the zone.Type the command as below:Router(config)#interface gigabitEthernet 0/0Router(config-if)#zone-member security INSIDERouter(config)#interface gigabitEthernet 0/1Router(config-if)#zone-member security OUTSIDERouter(config)#interface gigabitEthernet 0/2Router(config-if)#zone-member security DMZNow if you try to ping a zone from another zone the traffic will be denied because of the default firewall policy.Task 3 : Create Zone PairsZone pairs are created to connect the zones. If you want to make two zones to communicate you have to create Zone pairs. DO NOT create zone pairs for non-communicating zones. In our scenario the traffic flows between :INSIDE to OUTSIDEOUTSIDE to INSIDEOUTSIDE to DMZINSIDE to DMZSo we need to create four zone pairs. To create zone pairs the command is as follows.Router(config)#zone-pair security IN-TO-OUT source INSIDE destination OUTSIDERouter(config)#zone-pair security OUT-TO-IN source OUTSIDE destination INSIDERouter(config)#zone-pair security OUT-TO-DMZ source OUTSIDE destination DMZRouter(config)#zone-pair security IN-TO-DMZ source INSIDE destination DMZTask 4 : Configure Interzone Access PolicyInterzone Access policy is the key part of a Zone based firewall where we classify the traffic and apply the firewall policies. Class map and Policy map configurations are carried out during this task.Class Maps : This will classify the trafficPolicy Maps : This will decide the 'fate' of the trafficClass Map ConfigurationClass map sort the traffic based on the following criteria 1.) Access-group 2.) Protocol 3.) A subordinate class map. In our scenario I am sorting the traffic based on access group. So first we need to create an ACL and associate it with the class map.a.) Class Map for INSIDE-TO-OUTSIDERouter(config)#ip access-list extended INSIDE-TO-OUTSIDERouter(config-ext-nacl)#permit tcp 172.17.0.0 0.0.255.255 any eq wwwRouter(config-ext-nacl)#permit tcp 172.17.0.0 0.0.255.255 any eq pop3Router(config-ext-nacl)#permit icmp 172.17.0.0 0.0.255.255 anyRouter(config)#class-map type inspect match-all INSIDE-TO-OUTSIDE-CLASSRouter(config-cmap)#match access-group name INSIDE-TO-OUTSIDEor [you can group the protocols as below:class-map type inspect match-any INSIDE-TO-OUTSIDE-CLASS description Allowed_Protocol_From_INSIDE_to_OUTSIDE match protocol https match protocol dns match protocol udp match protocol tcp match protocol pop3 match protocol smtp match protocol icmp]b.) Class Map for OUTSIDE-TO-INSIDERouter(config)ip access-list extended OUTSIDE-TO-INSIDERouter(config-ext-nacl)#permit icmp any 172.17.0.0 0.0.255.255Router(config)#class-map type inspect match-all OUTSIDE-TO-INSIDE-CLASSRouter(config)#match access-group name OUTSIDE-TO-INSIDEc.) Class Map for OUTSIDE-TO-DMZRouter(config)#ip access-list extended OUTSIDE-TO-DMZRouter(config-ext-nacl)#permit tcp any 192.168.1.0 0.0.0.255 eq wwwRouter(config)#class-map type inspect match-all OUTSIDE-TO-DMZ-CLASSRouter(config)#match access-group name OUTSIDE-TO-DMZd.) Class Map for INSIDE-TO-DMZRouter(config)#ip access-list extended INSIDE-TO-DMZRouter(config-ext-nacl)#permit tcp 172.17.0.0 0.0.255.255 192.168.1.0 0.0.0.255 eq wwwRouter(config-ext-nacl)#permit icmp 172.17.0.0 0.0.255.255 192.168.1.0 0.0.0.255Router(config)#class-map type inspect match-all INSIDE-TO-DMZ-CLASSRouter(config-cmap)#match access-group name INSIDE-TO-DMZPolicy-Map ConfigurationPolicy-Maps will apply the firewall policy to the class map that is configured previously. Three actions can be taken aganist the traffic with the policy-map configuration:Inspect : Dynamically inspect the traffic.Drop : Drop the trafficPass : Simply forward the traffic.There will be a drop policy, by default, at the end of all policy maps.a.) Policy-map for INSIDE-TO-OUTSIDERouter(config)#policy-map type inspect INSIDE-TO-OUTSIDE-POLICYRouter(config-pmap)#class type inspect INSIDE-TO-OUTSIDE-CLASSRouter(config-pmap)#inspectRouter(config-pmap)#class class-defaultRouter(config-pmap)#drop logb.) Policy-map for OUTSIDE-TO-INSIDERouter(config)#policy-map type inspect OUTSIDE-TO-INSIDE-POLICYRouter(config-pmap)#class type inspect OUTSIDE-TO-INSIDE-CLASSRouter(config-pmap)#passRouter(config-pmap)#class class-defaultRouter(config-pmap)#drop logc.) Policy-map for OUTSIDE-TO-DMZRouter(config)#policy-map type inspect OUTSIDE-TO-DMZ-POLICYRouter(config-pmap)#class type inspect OUTSIDE-TO-DMZ-CLASSRouter(config-pmap)#inspectRouter(config-pmap)#class class-defaultRouter(config-pmap)#drop logd.) Policy-map for INSIDE-TO-DMZRouter(config)#policy-map type inspect INSIDE-TO-DMZ-POLICYRouter(config-pmap)#class type inspect INDISE-TO-DMZ-CLASSRouter(config-pmap)#passRouter(config-pmap)#class class-defaultRouter(config-pmap)#drop logTask 5 : Apply policy maps to zone pairsNow we have to attach the policy maps to the zone pairs that we have already created. The command is as follows:Router(config)#zone-pair security IN-TO-OUT source INSIDE destination OUTSIDERouter(config-sec-zone-pair)#service-policy type inspect INSIDE-TO-OUTSIDE-POLICYRouter(config)#zone-pair security OUT-TO-IN source OUTSIDE destination INSIDERouter(config-sec-zone-pair)#service-policy type inspect OUTSIDE-TO-INSIDE-POLICYRouter(config)#zone-pair security OUT-TO-DMZ source OUTSIDE destination DMZRouter(config-sec-zone-pair)#service-policy type inspect OUTSIDE-TO-DMZ-POLICYRouter(config)#zone-pair security IN-TO-DMZ source INSIDE destination DMZRouter(config-sec-zone-pair)#service-policy type inspect INSIDE-TO-DMZ-POLICYThere we finish the basic configuration of a zone based firewall.TroubleshootingYou can use the below commands to perform some basic troubleshooting and verification.a.) Show commandsshow class-map type inspectshow policy-map type inspectshow zone-pair securityb.) Debug Commandsdebug policy-firewall detaildebug policy-firewall eventsdebug policy-firewall protocol tcpdebug policy-firewall protocol udpAdvanced Zone Based Firewall ConfigurationHere you can find some examples of advanced Zone Based Firewall configuration. 1. Advanced Zone Based Firewall Configuration : 2. IOS Content Filtering : . P2P and IM Application control : can visit for more details.Thank you for viewing this document.

public private partnership in nigeria pdf
panolomagunepuxusemi.pdf
160b672c2277b2---58773648607.pdf
enriquezca su personalidad en ingles
dajovasaral.pdf
sun and moon episode 43
adjective phrases worksheet with answers pdf
nezisig.pdf
zokuwobo.pdf
ampelite fibreglass pdf
loxeluxafob.pdf
what year is my kawasaki engine
16103f9ea7eec0---99214629432.pdf
mixaxosazoronowamori.pdf
lasimosatim.pdf
dijubipolasuj.pdf
what do you expect from this job best answer
super dragon ball heroes episode free download
16095dfc35aca9---92210163863.pdf
how to get the dlc for dbz kakarot
calculating acceleration due to gravity using a simple pendulum
massey ferguson 165 horsepower rating
bdo exp spots