The zone based firewalls computer science essay

Technology, Computer

The purpose of this paper is to provide an overview of Zone-Based firewalls. In particular we are going to briefly present the firewall evolution from their beginning until today and under of which conditions we arrived on zone-based firewalls. Furthermore we analyze the differences between zone-based firewall and some other firewall policies. Finally we both describe the several advantages of zone-based policy and the critical factors in order a zone-based firewall to work correctly.

Introduction

“ Expecting the world to treat you fairly because you are a good person is a little like expecting a bull not to attack you because you are a vegetarian”. This phrase of Dennis Wholey suits in our case because we will talk about security. Actually we will talk about a new specific tool from which we expect security: The Zone-Based firewalls. Internet and web is changing dramatically day by day. There is nothing same after 2002 when the WEB 2. 0 came to our lives. Many things were changed and are still changing. Thus the needs are still changing as well. One of those needs is security. In order to keep our system secure we use antivirus software, firewalls and in some cases we choose the appropriate settings in order an employer to have only the necessary privileges in the machines of a company’s network. In this paper we will talk about a specific firewall type called Zone-Based Firewall. There are several types of firewalls. There are software-based and hardware-based firewalls, there are statefull and stateless firewalls. But all of them have a common scope: To reduce the underlying dangers of the untrusted zone (external network such as Internet) that could damage the trusted zone (any type of internal network).

As the picture shows firewall works as a protective bridge between the two zones

Firewalls

History of Firewalls

The concept of a wall to keep out intruders is not something new and it also dates back thousands of years and we could mention early firewall forms in the past. A good example is that over hundreds years ago European kings have been building castles with high walls and moats to protect themselves from invading armies (Kenneth Ingham 2002)

The term “ firewall” was in use by Lightoler as early as [1764] to describe walls which separated the parts of a building most likely to have a fire (e. g., a kitchen) from the rest of a structure. These physical barriers prevented or slowed a fire’s spread throughout a building, saving both lives and property. A related use of the term arose in connection with steam trains, as described by Schneier [2000]:

According with a Cisco research [1] Jeff Mogul from Digital Equipment Corp. published the first paper on firewall technology in 1988

What is a Firewall

“ Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures.” (Karen Scarfone, Paul Hoffman 2009)

Firewalls control the traffic of the incoming and outgoing packets of the Internet. They can also infect possible attacks in our system, analyze the traffic and the data transferring, distinguish suspicious activities and prevent their completion. Firewalls protect a network from other networks via firewall policy. Firewall policy is a predefined set of rules that makes a firewall to manage and filter the incoming and outgoing traffic in order to reduce the underlying dangers of the greater (and untrusted) Internet against the smaller private networks and their corresponding individual machines.

These packet filtering rules make able administrators to allow or deny based on source or destination IP Address, protocol type, and port number.(Beau Wallace, 2011)

Before we continue we must make comprehensive some critical definitions

Statefull and Stateless routers

Stateless packet filtering routers make forwarding decisions based on the contents of the network (IP) layer header and the transport (TCP/UDP) layer header

Stateful packet filtering routers also make forwarding decisions based on the contents of the network (IP) layer datagram header and the transport (TCP/UDP) layer segment header. However, they also maintain a connection state table, so that they know the current state of a given connection, and do not have to rely solely on the SYN and ACK flag values for this information (the flag values can be spoofed) (Mark Clements, Andrew Adekunle 2010)

A general conclusion of this comparison could be that stateful packet filtering routers are more reliable than stateless packet filtering routers

ACLs

ACL is a list of privileges attached to an object. An ACL makes clear which system processes or users are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies an operation and a subject. I. e in case a file has an ACL that contains (Alice, delete), this would give Alice permission to delete the file (Retrieved from Wikipedia).

1. 3 Introduction to Zone Based Firewalls

The previous feature of Cisco IOS (Internetwork Operating System) was the Content Based Access Control (CBAC). This approach of classic Firewall stateful inspection accomplished traffic filtering by using inception and access lists whose rules applied directly to the physical interfaces. However the CBAC limited the granularity of the firewall policies and caused confusion of the proper application of firewall policies, particularly in scenarios when firewall policies must be applied between multiple interfaces. This happens because all traffic passing through only one interface received the same inspection policy. Therefore nowadays this configure model is not the most effective solution.

Zone based Firewall is a new configuration approach of access control in the IOS firewall. Actually ZBFW is a wrapper for CBAC. This model changes the firewall configuration from the older interface-based model to a more flexible, more easily understood zone-based model. Interfaces are assigned to zones, instead of applying CBAC rules to interfaces. Inter-zone policies offer considerable flexibility and granularity, so different inspection policies can be applied to multiple host groups connected to the same router interface. Cisco's Zone-Based Policy Firewall model was presented in IOS version 12. 4(6)T and enhanced in 12. 4(9)T

Both CBAC and Zone Based-Firewalls are hybrids of statefull and stateless firewalls and also capable of application layer filtering, in addition to their duties at the network and transport layers, however ZFW is fully capable of deep packet inspection, and has the advantage of being able to apply policy across groups of interfaces.

.

1. 4 Zone Based Firewall vs CBAC

Zone-Based Firewall
CBAC

Zone Based Configuration

Interface Based Configuration

Controls Bidirectional access between zones

Controls Inbound and Outbound access on an interface

Uses Class-Based Policy Language

Uses inspect statements and stateful ACLs

Support Application Inspection and Control

Not Supported

Support from IOS Release 12. 4 (6) T

Support from IOS Release 11. 2

Rules of Zone-Based Firewall

Router network interfaces’ membership in zones is subject to several rules that govern interface behavior, as is the traffic moving between zone member interfaces (Cisco):

A zone must be configured before interfaces can be assigned to the zone.

An interface can be assigned to only one security zone.

All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router.

Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone.

In order to permit traffic to and from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone.

The self zone is the only exception to the default deny all policy. All traffic to any router interface is allowed until traffic is explicitly denied.

Traffic cannot flow between a zone member interface and any interface that is not a zone member. Pass, inspect, and drop actions can only be applied between two zones.

Interfaces that have not been assigned to a zone function as classical router ports and might still use classical stateful inspection/CBAC configuration.

If it is required that an interface on the box not be part of the zoning/firewall policy. It might still be necessary to put that interface in a zone and configure a pass all policy (sort of a dummy policy) between that zone and any other zone to which traffic flow is desired.

From the preceding it follows that, if traffic is to flow among all the interfaces in a router, all the interfaces must be part of the zoning model (each interface must be a member of one zone or another).

The only exception to the preceding deny by default approach is the traffic to and from the router, which will be permitted by default. An explicit policy can be configured to restrict such traffic.

Configuration

Now we will move onto some of the specifics. A correct ZBFW policy will always involve creating class-maps, policy-maps, zones, zone-pairs, and assigning interfaces into the zones. Let's see the configuration steps

Step 1 – Define the Zone Names

zone security OUTSIDE

```
zone security INSIDE
```

Step 2 – Define the Zone Pairs (direction of traffic flow)

```
zone-pair security EGRESS source INSIDE destination OUTSIDE

zone-pair security INGRESS source OUTSIDE destination INSIDE
```

Step 3 – Define the Protocols for Inspection

```
class-map type inspect match-any EGRESS-WEB

match protocol http

match protocol https

class-map type inspect match-any EGRESS-SVCS

match protocol dns

match protocol ntp

match protocol icmp
```

Step 3 – Create a Policy Maps for Zone Pairs

```
policy-map type inspect EGRESS

class EGRESS-WEB

inspect

# note: some available options include drop, police, pass, etc.
```

```
class EGRESS-SVCS

inspect
```

Note – In this first example, we’re doing a simple setup with no publicly accessible servers (DMZ). Since the return for all traffic that was permitted outbound will be implicitly allowed on ingress, we don’t need a policy map for that direction.

Step 4 – Assign the Policy Map to a Zone Pair

```
zone-pair security EGRESS source INSIDE destination OUTSIDE

service-policy type inspect EGRESS
```

Step 5 – Allocate Interfaces into Zones

```
interface Vlan1

zone-member security INSIDE

interface FastEthernet4

zone-member security OUTSIDE
```

Step 6 – Verification

```
show policy-map type inspect zone-pair sessions
```

a screencapture of “ show policy-map type inspect zone-pair sessions”

Summarization

ZBFW offers following features

Application inspection

Statefull inspection

Local URL filtering

Transparent firewall

Things to remember about ZBFW

The policies configured from one zone to another are unidirectional in nature.

By default the traffic flow between the inter-zones is “ DENY ALL”.

By default the traffic flow to or from “ SELF” zone to another zone is “ ALLOW ALL” and we can restrict the same with the help of class-maps along with respective actions.

By default the traffic flow between the intra-zones is “ Allow ALL” and we can’t restrict or apply any kind of inspection to the same.

An interface can be assigned to only one security zone.

Traffic cannot flow between a zone-member interface and any interface which is not a *zone-member, so that means every interface should be assigned to a zone.

We can apply multiple classes along with respective action per zone-pair.

Steps to configure ZBFW

Identify and define network zones.

Determine the traffic flow between the respective zones.

Define class-maps to describe traffic between zones.

Associate class-maps with policy-maps to define actions to the respective traffic flow.

Set up zone pairs for any policy other than deny all.

Assign policy-maps to zone-pairs.

Now assign interfaces to zones.

The final step would be validate the configuration by passing some interested traffic.

Conclusion

Finally in this paper we briefly presented the evolution of firewalls from their beginning until today. Furthermore we mentioned how and under of which conditions zone-based firewalls have been created. We also described the rules and the steps in order a zone based firewall to work correctly. Last but not least we referred the advantages of zone-based policy and we compared them with previous firewall features such as CBAC in order to comprehend what more we have to expect. We should also mention that in specific technical issues such as Zone-Based Firewall rules or Zone-Based firewall configuration we mainly informed from Cisco because according to our justification nobody is more appropriate to orientate us about Zone-Based firewalls than the creator of Zone-Based Firewalls