在ASA防火牆上配置網路地址轉換和ACL

目錄

簡介

本檔案將說明如何在ASA防火牆上設定網路位址轉譯(NAT)和存取控制清單(ACL)。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於運行ASA代碼版本9.1(1)的ASA 5510防火牆。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔介紹如何在ASA防火牆上配置NAT和ACL以允許出站和入站連線的簡單而直觀的示例。它使用Adaptive Security Appliance(ASA)5510防火牆編寫，而不是運行ASA代碼版本9.1(1)，但這可以輕鬆應用於任何其他ASA防火牆平台。如果您使用使用VLAN而非物理介面的平台（例如ASA 5505），則需要相應地更改介面型別。

概觀

目標

在此示例配置中，您可以檢視需要哪些NAT和ACL配置才能允許對ASA防火牆DMZ中的Web伺服器的入站訪問，並允許來自內部和DMZ主機的出站連線。這可以概括為兩個目標：

1. 允許內部主機和DMZ出站主機連線到Internet。
2. 允許Internet上的主機訪問IP地址為192.168.1.100的DMZ上的Web伺服器。

在執行完成這兩個目標所必須完成的步驟之前，本文檔簡要介紹了ACL和NAT在較新版本ASA代碼（8.3版及更高版本）上的工作方式。

訪問控制清單概述

訪問控制清單（Access-lists或ACL簡稱）是ASA防火牆用來確定流量是允許還是拒絕的方法。預設情況下，從較低安全層級傳送到較高安全層的流量會遭到拒絕。此值可由應用於該較低安全介面的ACL覆蓋。此外，預設情況下，ASA允許流量從較高安全介面流向較低安全介面。此行為也可以使用ACL覆蓋。

在早期版本的ASA代碼（8.2及更早版本）中，ASA將傳入連線或資料包與介面上的ACL進行比較，而不首先取消轉換資料包。換句話說，ACL必須允許該資料包，就像您要在介面上捕獲該資料包一樣。在8.3版及更高版本的代碼中，ASA會在檢查介面ACL之前解譯該資料包。這表示對於8.3及更高版本的代碼和本文檔，允許到主機的實際IP的流量，而不是主機的已轉換IP。

有關ACL的詳細資訊，請參閱手冊2:Cisco ASA系列防火牆CLI配置指南9.1的配置訪問規則部分。

NAT概述

8.3版及更高版本的ASA上的NAT分為兩種型別，分別稱為自動NAT（對象NAT）和手動NAT（兩次NAT）。兩個對象中的第一個對象NAT是在網路對象的定義中配置的。本文檔後面會提供一個示例。此NAT方法的一個主要優勢是ASA會自動對規則進行排序以便進行處理，從而避免衝突。這是最簡單的NAT形式，但隨之而來的就是配置粒度方面的限制。例如，不能像使用第二種NAT（手動Nat）時那樣根據資料包中的目標做出轉換決策。手動NAT的粒度更強，但它要求以正確的順序配置行，以便實現正確的行為。這會使此NAT型別複雜化，因此不能在此配置示例中使用它。

有關NAT的詳細資訊，請參閱第2冊：Cisco ASA系列防火牆CLI配置指南9.1的有關NAT的資訊部分。

設定

開始使用

基本ASA配置設定是連線到三個網段的三個介面。ISP網段連線到Ethernet0/0介面，並在外部標示安全級別為0。內部網路已連線到Ethernet0/1，並標籤為內部，安全級別為100。Web伺服器所在的

DMZ區段連線到乙太網路0/2，並標籤為DMZ，安全等級為50。

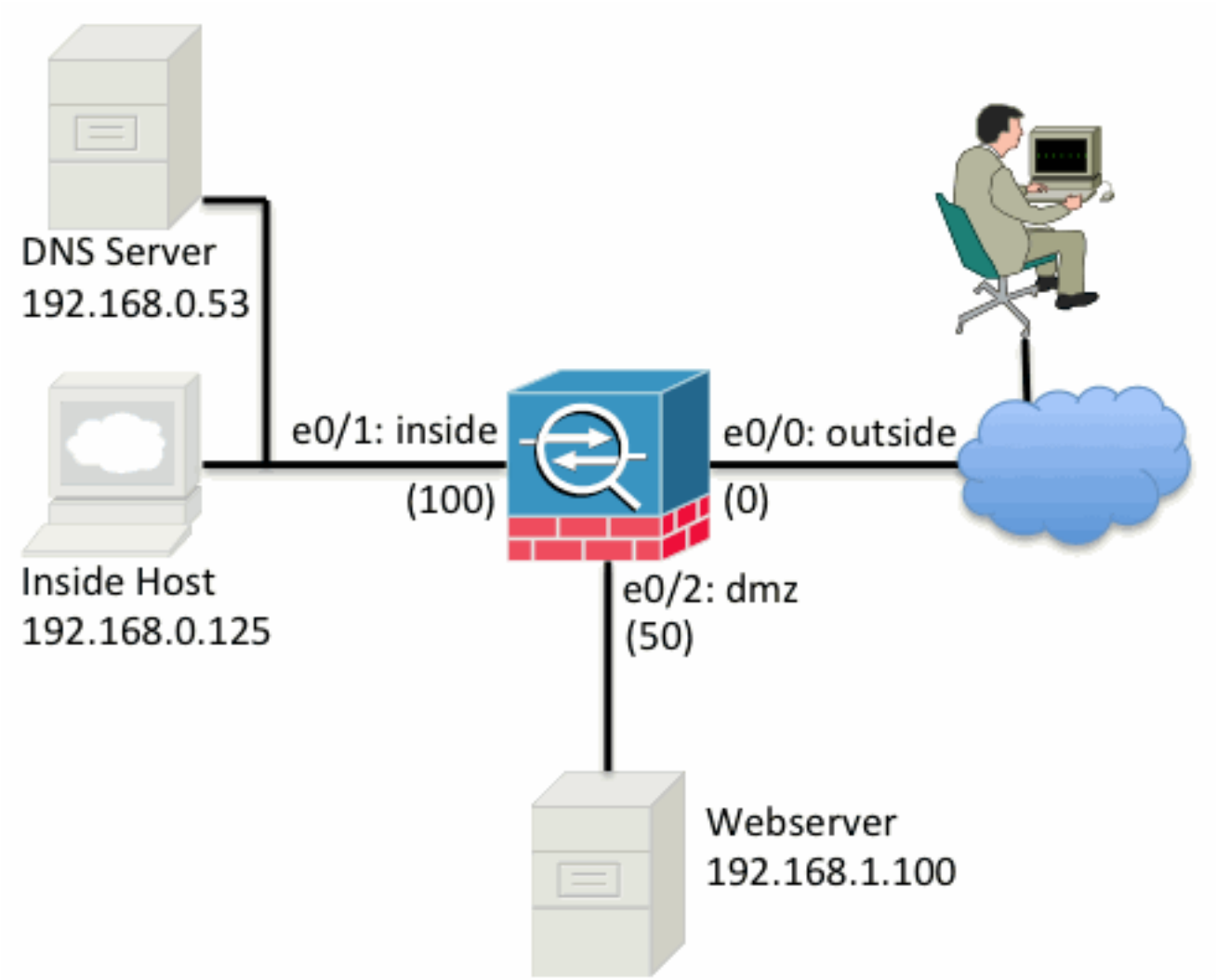
示例的介面配置和IP地址如下所示：

```
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

在這裡，您可以看到ASA的內部介面設定了IP地址192.168.0.1，並且它是內部主機的預設網關。ASA的外部介面配置有從ISP獲取的IP地址。有一條預設路由，將下一跳設定為ISP網關。如果使用DHCP，則自動提供此功能。DMZ介面的IP地址配置為192.168.1.1，並且是DMZ網段上主機的預設網關。

拓撲

以下是對電纜連線和配置方式的視覺化說明：



步驟1.配置NAT以允許主機連線到Internet

在本示例中，使用對象NAT（也稱為AutoNAT）。首先要配置的NAT規則允許內部網段和DMZ網段上的主機連線到Internet。由於這些主機使用私有IP地址，因此您需要將它們轉換為Internet上可路由的某個地址。在這種情況下，請轉換這些地址，使其看上去像ASA的外部介面IP地址。如果您的外部IP經常更改（可能是由於DHCP），則這是設定此配置的最簡單方法。

要配置此NAT，您需要建立一個表示內部子網的網路對象和一個表示DMZ子網的網路對象。在這些對象中的每個對象中，配置一個動態nat規則，該規則可以在這些客戶端從各自的介面傳遞到外部介面時對這些客戶端進行埠地址轉換(PAT)。

此配置如下所示：

```
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
nat (inside,outside) dynamic interface
!
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
nat (dmz,outside) dynamic interface
```

如果您檢視此時的運行配置（使用show run命令輸出），可以看到對象定義被分割為輸出的兩個部分。第一部分只指示對象中的內容（主機/子網、IP地址等），而第二部分顯示與該對象關聯的NAT規則。如果採用上一個輸出中的第一個條目：

當與192.168.0.0/24子網匹配的主機從內部介面遍歷到外部介面時，您希望將其動態轉換為外部介面。

步驟2.配置NAT以從網際網路訪問Web伺服器

現在內部和DMZ介面上的主機可以訪問Internet，您需要修改配置，以便Internet上的使用者可以訪問TCP埠80上的Web伺服器。在本例中，設定使Internet上的人員可以連線到ISP提供的另一個IP地址，即我們擁有的額外*IP地址*。在本例中，使用198.51.100.101。透過此組態，網際網路上的使用者可以通過存取TCP連線埠80上的198.51.100.101來連線至DMZ Web伺服器。對於此任務，請使用對象NAT，並且ASA可以將Web伺服器(192.168.1.100)上的TCP埠80轉換為類似於外部TCP埠80上的198.51.100.101。與之前所做的工作類似，定義對象並為該對象定義轉換規則。此外，定義第二個對象來表示可將此主機轉換到的IP。

此配置如下所示：

```
object network webserver-external-ip
host 198.51.100.101
!
object network webserver
host 192.168.1.100
nat (dmz,outside) static webserver-external-ip service tcp www www
```

在此示例中，總結NAT規則意味著什麼：

當與DMZ網段上的IP地址192.168.1.100匹配的主機建立源自TCP埠80(www)的連線且該連線從外部介面輸出時，您希望將該連線轉換為外部介面上的TCP埠80(www)，並將該IP地址轉換為198.51.100.101。

這似乎有點奇怪.....「來源為TCP埠80(www)」，但Web流量目的地為埠80。必須瞭解這些NAT規則實際上是雙向的。因此，您可以調轉措辭，以便重述這句話。結果更有道理：

當外部主機在目的地TCP連線埠80(www)上建立與198.51.100.101的連線時，可以將目的地IP位址轉譯為192.168.1.100，且目的地連線埠可以為TCP連線埠80(www)，然後將其傳送出DMZ。

這樣說更有道理。接下來，您需要設定ACL。

步驟3.配置ACL

已配置NAT，並且此配置即將結束。請記住，ASA上的ACL允許您覆蓋預設安全行為，如下所示：

- 來自較低安全介面的流量在流向較高安全介面時遭到拒絕。
- 來自更高安全介面的流量在進入較低安全介面時允許通過。

因此，如果沒有在組態中新增任何ACL，範例中的此流量將正常運作：

- 內部主機（安全級別100）可以連線到DMZ（安全級別50）上的主機。
- 內部主機（安全級別100）可以連線到外部主機（安全級別0）。
- DMZ上的主機（安全級別50）可以連線到外部上的主機（安全級別0）。

但是，此流量會遭到拒絕：

- 外部主機（安全級別0）無法連線到內部主機（安全級別100）。
- 外部主機（安全級別0）無法連線到DMZ上的主機（安全級別50）。
- DMZ（安全級別50）上的主機無法連線到內部（安全級別100）上的主機。

由於從外部到DMZ網路的流量被ASA以其當前配置拒絕，因此，儘管步驟2中配置了NAT，Internet上的使用者仍無法訪問Web伺服器。您需要明確允許此流量。在8.3及更高版本的代碼中，必須使用主機在ACL中的實際IP，而不是轉換後的IP。這表示組態需要允許目的地為192.168.1.100的流量，而不是允許連線埠80上目的地為198.51.100.101的流量。為簡單起見，步驟2中定義的對象也可用於此ACL。建立ACL後，您需要將其應用於外部介面的入站流量。

以下是這些組態指令的樣子：

```
access-list outside_acl extended permit tcp any object webserver eq www
!
access-group outside_acl in interface outside
```

access-list行狀態：

允許從埠80上的對象Web伺服器(192.168.1.100)所代表的主機發往任何位置的流量。

配置在此處使用any關鍵字非常重要。由於客戶端的源IP地址在到達您的網站時未知，因此請指定「任何IP地址」的任何含義。

從DMZ網段發往內部網段上主機的流量如何？例如，DMZ上的主機需要連線的內部網路上的伺服器。ASA如何僅允許發往內部伺服器的特定流量，並阻止從DMZ發往內部網段的所有其他流量？

在此範例中，假設內部網路上的IP位址為192.168.0.53的DNS伺服器是DMZ上的主機需要存取以進行DNS解析。您可以建立所需的ACL並將其應用到DMZ介面，以便ASA可以覆蓋之前提到的進入該介面的流量的預設安全行為。

以下是這些組態指令的樣子：

```
object network dns-server
host 192.168.0.53
!
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
access-group dmz_acl in interface dmz
```

ACL比僅允許流量通過UDP埠53到達DNS伺服器更為複雜。如果我們所做的只是第一條允許線路，那麼所有從DMZ到網際網路主機的流量都會被阻止。ACL的結尾有隱含的「deny ip any any」。因此，您的DMZ主機將無法訪問Internet。雖然預設會允許從DMZ到外部的流量，但將ACL套用到DMZ介面後，DMZ介面的這些預設安全行為將不再有效，且您必須明確允許介面ACL中的流量。

步驟4.使用Packet Tracer功能測試配置

配置完成後，您需要進行測試以確保其正常工作。最簡單的方法是使用實際主機（如果這是您的網路）。但是，為了便於從CLI測試此問題並進一步探索ASA的某些工具，請使用packet tracer測試遇到的所有問題並可能對其進行調試。

Packet Tracer的工作原理是根據一系列引數模擬資料包，並將該資料包注入介面資料路徑，類似於實際資料包從線路上接收的方式。此資料包在通過防火牆時執行各種檢查和流程，Packet Tracer記錄結果。模擬內部主機傳出Internet上的主機。此命令指示防火牆：

模擬一個從源埠12345上的IP地址192.168.0.125傳到埠80上的IP地址203.0.113.1的內部介面的TCP資料包。

```
ciscoasa# packet-tracer input inside tcp 192.168.0.125 12345 203.0.113.1 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config: Additional Information:
in 0.0.0.0 0.0.0.0 outside Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network inside-subnet
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.0.125/12345 to 198.51.100.100/12345

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1, packet dispatched to next module
```

```
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

最終結果是允許流量，這意味著流量通過了配置中的所有NAT和ACL檢查，並被從外部的出口介面發出。請注意，資料包是在第3階段轉換的，該階段的詳細資訊顯示所命中的規則。主機192.168.0.125會根據配置動態轉換為198.51.100.100。

現在，運行它以從Internet連線到Web伺服器。請記住，Internet上的主機可以通過連線到外部介面上的198.51.100.101來訪問Web伺服器。同樣，下一個命令將轉換為：

模擬從源埠12345上的IP地址192.0.2.123到埠80上的IP地址198.51.100.101傳入外部介面的TCP資料包。

```
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 198.51.100.101 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 198.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_acl in interface outside
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
```

```
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

同樣地，結果是允許該資料包。ACL會簽出，組態看起來不錯，而Internet（外部）上的使用者可以使用外部IP存取該Web伺服器。

驗證

驗證過程包含在步驟4 — 使用Packet Tracer功能測試配置中。

疑難排解

目前沒有有關如何對此組態進行疑難排解的特定資訊。

結論

配置ASA以執行基本NAT並不是一項艱鉅的任務。如果您更改示例配置中使用的IP地址和埠，本文檔中的示例可以適用於您的特定場景。結合使用時，此配置的最終ASA配置與ASA 5510的配置類似：

```
ASA Version 9.1(1)
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
```

```
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
object network webserver
host 192.168.1.100
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53

!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

例如，在ASA 5505上，介面連線如前所示（外部連線到Ethernet0/0，內部連線到Ethernet0/1,DMZ連線到Ethernet0/2）：

```
ASA Version 9.1(1)
!
interface Ethernet0/0
description Connected to Outside Segment
switchport access vlan 2
!
interface Ethernet0/1
description Connected to Inside Segment
switchport access vlan 1
!
interface Ethernet0/2
description Connected to DMZ Segment
switchport access vlan 3
!
interface Vlan2
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Vlan1
nameif inside
```

```
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Vlan3
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
object network webserver
host 192.168.1.100
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53



!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。