ASA 릴리스 9.(x) 인터넷 컨피그레이션을 통한 3개의 내부 네트워크 연결 예

목차

소개

이 문서에서는 3개의 내부 네트워크와 함께 사용할 Cisco ASA(Adaptive Security Appliance) 버전 9.1(5)을 설정하는 방법에 대해 설명합니다.고정 경로는 간소화를 위해 라우터에서 사용됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco ASA(Adaptive Security Appliance) 버전 9.1(5)을 기반으로 합니다.

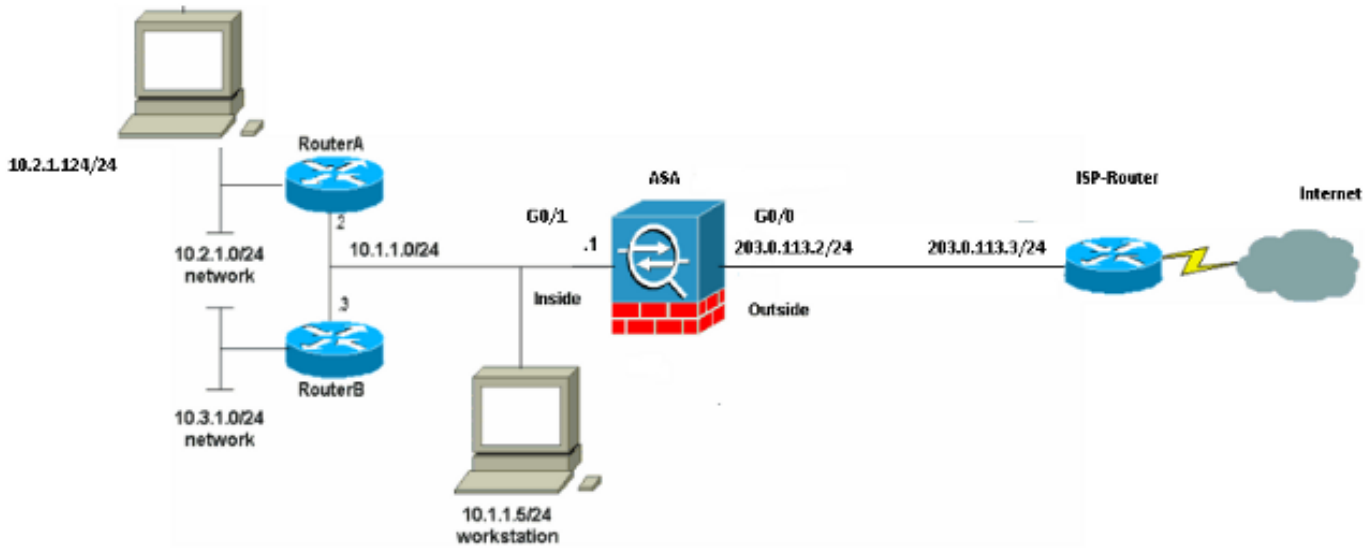
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고:이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램



참고:이 컨피그레이션에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이 주소는 랩 환경에서 사용된 RFC 1918 주소입니다.

ASA 9.1 구성

이 문서에서는 이러한 구성을 사용합니다.Cisco 디바이스에서 **write terminal** 명령의 출력이 있는 경우 Output Interpreter(등록된 고객만)를 사용하여 잠재적인 문제 및 수정 사항을 표시할 수 있습니다.

구성

- 라우터 A 컨피그레이션
- 라우터 B 컨피그레이션
- ASA 버전 9.1 이상 컨피그레이션

라우터 A 컨피그레이션

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
boot-start-marker
```

```
boot-end-marker
!
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line 33
no activation-character
no exec
transport preferred none
transport input all
```

```
transport output all
line aux 0
line vty 0 4
password ww
login
!
!
end

RouterA#
```

라우터 B 컨피그레이션

```
RouterB#show running-config
Building configuration...

Current configuration : 1132 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
duplex auto
speed auto
no cdp enable
!
interface FastEthernet0/1
ip address 10.3.1.1 255.255.255.0
```

```
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
stopbits 1
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password cisco
login
!
!
end

RouterB#
```

ASA 버전 9.1 이상 컨피그레이션

```
ASA#show run
: Saved
:
ASA Version 9.1(5)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa915-k8.bin
```

```
ftp mode passive

!--- Enable informational logging to see connection creation events

logging on
logging buffered informational

!--- Output Suppressed

!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- object will get PAT to the outside interface IP
!--- on the ASA (or 10.165.200.226) for internet bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface

!--- Output Suppressed

!--- Define a default route to the ISP router.


route outside 0.0.0.0 0.0.0.0 203.0.113.3 1

!--- Define a route to the INTERNAL router with network 10.2.1.0.

route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the INTERNAL router with network 10.3.1.0.

route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

웹 브라우저를 사용하여 HTTP를 통해 웹 사이트에 액세스해 보십시오.이 예에서는 198.51.100.100에서 호스팅되는 사이트를 사용합니다. 연결이 성공하면 ASA CLI에서 이 출력을 볼 수 있습니다.

연결

```
ASA(config)# show connection address 10.2.1.124
16 in use, 918 most used
TCP outside 198.51.100.100:80 inside 10.2.1.124:18711, idle 0:00:16, bytes 1937,
flags UIO
```

ASA는 스테이트풀 방화벽이며, 방화벽 연결 테이블의 ***연결***과 일치하기 때문에 웹 서버의 반환 트래픽이 방화벽을 통해 다시 허용됩니다.사전 존재하는 연결과 일치하는 트래픽은 방화벽을 통해 허용되며 인터페이스 ACL에 의해 차단되지 않습니다.

이전 출력에서 내부 인터페이스의 클라이언트는 외부 인터페이스의 198.51.100.100 호스트에 대한

연결을 설정했습니다.이 연결은 TCP 프로토콜로 이루어지며 6초 동안 유휴 상태가 되었습니다.연결 플래그는 이 연결의 현재 상태를 나타냅니다.연결 플래그에 대한 자세한 내용은 ASA TCP Connection Flags(ASA TCP 연결 플래그)를 참조하십시오.

Syslog

```
ASA(config)# show log | include 10.2.1.124

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.2.1.124/18711 to outside:203.0.113.2/18711

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.2.1.124/18711 (203.0.113.2/18711)
```

ASA 방화벽은 정상 작동 중에 syslog를 생성합니다.syslogs는 로깅 컨피그레이션을 기반으로 자세한 범위를 제공합니다.출력은 레벨 6 또는 '정보' 레벨에서 표시되는 두 개의 syslog를 보여줍니다.

이 예에서는 두 개의 syslog가 생성됩니다.첫 번째는 방화벽에서 변환을 구축했다는 로그 메시지, 특히 동적 TCP 변환(PAT)입니다. 트래픽이 내부에서 외부 인터페이스로 이동하는 동안 소스 IP 주소 및 포트와 변환된 IP 주소 및 포트를 나타냅니다.

두 번째 syslog는 방화벽이 클라이언트와 서버 간의 이 특정 트래픽에 대한 연결 테이블에 연결을 구축했음을 나타냅니다.이 연결 시도를 차단하도록 방화벽을 구성했거나 이 연결 생성을 방해하는 다른 요인(리소스 제약 조건 또는 잘못된 컨피그레이션)이 있는 경우 방화벽은 연결이 구축되었음을 나타내는 로그를 생성하지 않습니다.대신 연결이 거부되는 이유 또는 연결이 생성되는 것을 방해하는 요인에 대한 표시가 기록됩니다.

NAT 변환

```
ASA(config)# show xlate local 10.2.1.124
2 in use, 180 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.2.1.124/18711 to outside:203.0.113.2/18711 flags ri idle
0:12:03 timeout 0:00:30
```

이 컨피그레이션의 일부로, 내부 호스트 IP 주소를 인터넷에서 라우팅 가능한 주소로 변환하기 위해 PAT가 구성됩니다.이러한 번역이 생성되었는지 확인하기 위해 NAT 변환(xlate) 테이블을 확인할 수 있습니다.명령 **show xlate는 local** 키워드 및 내부 호스트의 IP 주소와 결합되면 해당 호스트의 변환 테이블에 있는 모든 항목을 표시합니다.이전 출력에서는 내부 인터페이스와 외부 인터페이스 간에 이 호스트에 대해 현재 구축된 변환이 있음을 보여줍니다.내부 호스트 IP 및 포트는 컨피그레이션에 따라 203.0.113.2 주소로 변환됩니다.나열된 플래그(r i)는 변환이 **동적**과 포트맵임을 **나타냅니다**.서로 다른 NAT 컨피그레이션에 대한 자세한 내용은 NAT 정보를 참조하십시오.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

ASA는 연결 문제를 해결할 수 있는 여러 툴을 제공합니다.컨피그레이션을 확인하고 이전에 나열된 출력을 확인한 후에도 문제가 계속되면 이러한 툴 및 기술을 통해 연결 오류의 원인을 확인할 수 있습니다.

패킷 추적기

```
ASA(config)# packet-tracer input inside tcp 10.2.1.124 1234 198.51.100.100 80


--Omitted--

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

ASA의 패킷 추적기 기능을 사용하면 시뮬레이션된 패킷을 지정하고, 트래픽이 처리될 때 방화벽이 거치는 다양한 단계, 검사 및 기능을 모두 볼 수 있습니다.이 툴을 사용하면 방화벽을 통과하도록 허용되어야 하는 트래픽의 예를 식별하고 트래픽을 시뮬레이션하기 위해 5-튜플을 사용하는 것이 좋습니다.이전 예에서 패킷 추적기는 다음 조건을 충족하는 연결 시도를 시뮬레이션하기 위해 사용됩니다.

- 시뮬레이션된 패킷이 **내부**에 **도착합니다**.
- 사용되는 프로토콜은 **TCP입니다**.
- 시뮬레이션된 클라이언트 IP 주소는 **10.2.1.124입니다**.
- 클라이언트는 포트 **1234**에서 소싱된 트래픽을 **전송합니다**.
- 트래픽은 IP 주소 **198.51.100.100**의 서버로 **전송됩니다**.
- 트래픽은 포트 **80**으로 **이동합니다**.

명령 **밖**에 인터페이스에 대한 언급이 없습니다.이는 패킷 추적기 설계에 의한 것입니다.이 툴은 방화벽이 어떤 유형의 연결 시도를 어떻게 처리하는지, 여기에는 라우팅 방법과 어떤 인터페이스 밖으로 처리되는지 알려줍니다.패킷 추적기에 대한 자세한 내용은 Tracing Packets with Packet Tracer를 참조하십시오.

캡처

```
ASA# capture capin interface inside match tcp host 10.2.1.124 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#   show capture capin

3 packets captured

  1: 11:31:23.432655       10.2.1.124.18711 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712518       198.51.100.100.80 > 10.2.1.124.18711: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.2.1.124.18711 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       203.0.113.2.18711 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712472       198.51.100.100.80 > 203.0.113.2.18711: S 95714629:
```

```
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       203.0.113.2.18711 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

ASA 방화벽은 인터페이스를 드나드는 트래픽을 캡처할 수 있습니다.이 캡처 기능은 트래픽이 방화벽에 도달하거나 방화벽에서 출발하는지 여부를 명확히 확인할 수 있으므로 환상적인 기능입니다 .앞의 예에서는 내부 및 외부 인터페이스에서 capin과 capout이라는 두 **캡처**의 컨피그레이션을 각각 보여 줍니다.capture 명령은 **match** 키워드를 사용했으며, 이를 통해 캡처할 트래픽에 대해 구체적으로 지정할 수 있습니다.

캡처 **캡처**의 경우 **tcp 호스트 10.2.1.124 호스트 198.51.100.100과** 일치하는 내부 인터페이스(인그레스 또는 이그레스)에서 보이는 트래픽을 매칭하려고 했습니다. 즉, **호스트 10.2.1.124**에서 **호스트 198.51.100.100**에서 전송되는 모든 TCP 트래픽을 캡처하고자 합니다10 0 **또는 그 반대입니다** .match 키워드를 사용하면 방화벽에서 해당 트래픽을 양방향으로 캡처할 수 있습니다.외부 인터페이스에 대해 정의된 capture 명령은 내부 클라이언트 IP 주소를 참조하지 않습니다. 방화벽이 해당 클라이언트 IP 주소에서 PAT를 수행하기 때문입니다.따라서 해당 클라이언트 IP 주소**와 일치시킬** 수 없습니다.대신 이 예에서는 **any를 사용하여** 가능한 모든 IP 주소가 해당 조건과 일치함을 나타냅니다.

캡처를 구성한 후 연결을 다시 설정하려고 시도한 다음 **show capture *<capture_name>*** 명령을 사용하여 캡처를 계속 볼 수 있습니다.이 예에서는 클라이언트가 캡처에 표시된 TCP 3-Way 핸드셰이크를 통해 분명하게 서버에 연결할 수 있음을 확인할 수 있습니다.