PIX 및 ASA를 통한 연결 문제 해결

목차

소개

이 문서에서는 Cisco ASA 5500 Series ASA(Adaptive Security Appliance) 및 Cisco PIX 500 Series Security Appliance를 사용하는 경우에 대한 문제 해결 아이디어와 제안을 제공합니다.애플리케이션 또는 네트워크 소스가 중단되거나 사용할 수 없는 경우, 방화벽(PIX 또는 ASA)이 주요 타겟이 되는 경우가 많으며 중단의 원인으로 인한 영향이 가장 많습니다.관리자는 ASA 또는 PIX에서 일부 테스트를 수행하여 ASA/PIX가 문제를 일으키는지 여부를 결정할 수 있습니다.

PIX/ASA 참조:Cisco 보안 어플라이언스의 인터페이스 관련 문제 해결에 대해 자세히 알아보려면

Cisco Security Appliance를 통해 연결을 설정하고 문제를 해결하십시오.

참고: 이 문서에서는 ASA 및 PIX에 초점을 맞춥니다.ASA 또는 PIX에서 트러블슈팅이 완료되면 다른 디바이스(라우터, 스위치, 서버 등)에 추가 트러블슈팅이 필요할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco ASA 5510(OS 7.2.1 및 8.3 포함)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.

관련 제품

이 문서는 다음과 같은 하드웨어 및 소프트웨어 버전과 함께 사용할 수도 있습니다.

- ASA 및 PIX OS 7.0, 7.1, 8.3 이상
- FWSM(Firewall Services Module) 2.2, 2.3 및 3.1

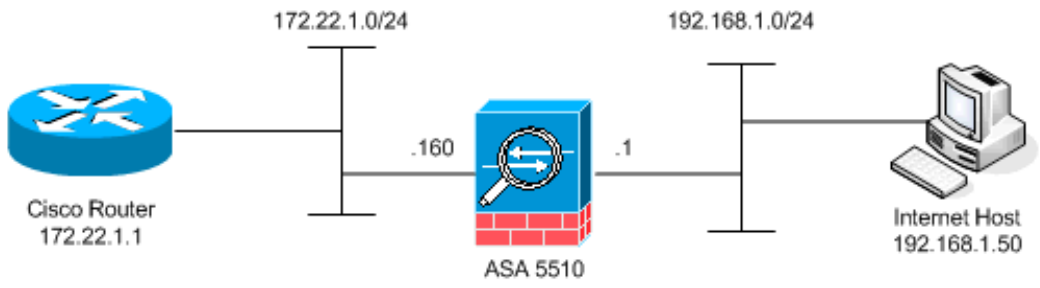
참고: 특정 명령과 구문은 소프트웨어 버전에 따라 다를 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

이 예에서는 ASA 또는 PIX가 프로덕션 중이라고 가정합니다.ASA/PIX 컨피그레이션은 비교적 간단하거나(50개의 컨피그레이션 라인만 해당) 복잡할 수 있습니다(수백 개에서 수천 개의 컨피그레이션 라인). 사용자(클라이언트) 또는 서버는 보안 네트워크(내부) 또는 비보안 네트워크(DMZ 또는 외부)에 있을 수 있습니다.



ASA는 이 컨피그레이션으로 시작합니다.이 컨피그레이션은 Lab에 참조 지점을 제공하기 위한 것

입니다.

ASA 초기 컨피그레이션

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 10.1.1.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list outside_acl extended permit tcp any host
172.22.1.254 eq www
access-list inside_acl extended permit icmp 192.168.1.0
255.255.255.0 any
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq www
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq telnet
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no asdm history enable
arp timeout 14400
global (outside) 1 172.22.1.253
nat (inside) 1 192.168.1.0 255.255.255.0


!--- The above NAT statements are replaced by the
following statements !--- for ASA 8.3 and later. object
network obj-192.168.1.0 subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic 172.22.1.253 static
(inside,outside) 192.168.1.100 172.22.1.254 netmask
255.255.255.255 !--- The above Static NAT statement is
replaced by the following statements !--- for ASA 8.3
and later. object network obj-172.22.1.254 host
```

```
172.22.1.254 nat (inside,outside) static 192.168.1.100
access-group outside_acl in interface outside access-
group inside_acl in interface inside timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

문제

사용자는 IT 부서에 연락하여 애플리케이션 X가 더 이상 작동하지 않는다고 보고합니다.인시던트가 ASA/PIX 관리자로 에스컬레이션됩니다.관리자는 이 특정 애플리케이션에 대해 거의 알지 못합니다.관리자는 ASA/PIX를 사용하여 애플리케이션 X에서 사용하는 포트 및 프로토콜과 문제의 원인을 검색합니다.

솔루션

ASA/PIX 관리자는 최대한 많은 정보를 사용자로부터 수집해야 합니다.다음과 같은 유용한 정보를 제공합니다.

- Source IP address(소스 IP 주소) - 일반적으로 사용자의 워크스테이션 또는 컴퓨터입니다.
- Destination IP address(대상 IP 주소) - 사용자 또는 애플리케이션이 연결하려고 시도하는 서버 IP 주소입니다.
- 애플리케이션이 사용하는 포트 및 프로토콜

이러한 질문 중 하나에 대한 답을 얻을 수 있다면 관리자는 운이 좋은 경우가 많습니다.이 예에서는 관리자가 정보를 수집할 수 없습니다.ASA/PIX syslog 메시지를 검토하는 것이 좋지만 관리자가 찾을 내용을 모르는 경우 문제를 찾기가 어렵습니다.

1단계 - 사용자의 IP 주소 검색

사용자의 IP 주소를 검색하는 방법에는 여러 가지가 있습니다.이 문서는 ASA와 PIX에 대한 것이므로 이 예에서는 ASA와 PIX를 사용하여 IP 주소를 검색합니다.

사용자는 ASA/PIX와 통신을 시도합니다.이 통신은 ICMP, 텔넷, SSH 또는 HTTP일 수 있습니다.선택한 프로토콜은 ASA/PIX에서 제한된 활동을 가져야 합니다.이 특정 예에서는 사용자가 ASA의 내부 인터페이스를 ping합니다.

관리자는 이러한 옵션 중 하나 이상을 설정한 다음 사용자가 ASA의 내부 인터페이스를 ping하도록 해야 합니다.

- **Syslog**로깅이 활성화되어 있는지 확인합니다.로깅 수준을 **디버그**로 설정해야 합니다.로깅은 다양한 위치로 전송할 수 있습니다.이 예에서는 ASA 로그 버퍼를 사용합니다.프로덕션 환경에 외부 로깅 서버가 필요할 수 있습니다.

```
ciscoasa(config)#logging enable
ciscoasa(config)#logging buffered debugging
```

사용자는 ASA의 내부 인터페이스(ping 192.168.1.1)을 ping합니다. 이 출력이 표시됩니다.

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-6-302020: Built ICMP connection for faddr 192.168.1.50/512
gaddr 192.168.1.1/0 laddr 192.168.1.1/0
%ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.50/512
gaddr 192.168.1.1/0 laddr 192.168.1.1/0
!--- The user IP address is 192.168.1.50.
```

- **ASA 캡처 기능**관리자는 ASA에서 캡처해야 하는 트래픽을 정의하는 액세스 목록을 생성해야 합니다.access-list가 정의되면 **capture** 명령은 access-list를 통합하여 인터페이스에 적용합니다.

```
ciscoasa(config)#access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#capture inside_interface access-list inside_test interface inside
```

사용자는 ASA의 내부 인터페이스(ping 192.168.1.1)을 ping합니다. 이 출력이 표시됩니다.

```
ciscoasa#show capture inside_interface
   1: 13:04:06.284897 192.168.1.50 > 192.168.1.1: icmp: echo request
 !--- The user IP address is 192.168.1.50.
```

참고: 캡처 파일을 ethereal과 같은 시스템에 다운로드하려면 이 출력에 표시된 대로 할 수 있습니다.

```
!--- Open an Internet Explorer and browse with this https link format: https://[
```

ASA/PIX 참조:ASA에서 패킷 캡처에 대한 자세한 정보를 보려면 CLI 및 ASDM 컨피그레이션을 사용하여 패킷 캡처 예

- **디버그**debug **icmp trace** 명령은 사용자의 ICMP 트래픽을 캡처하는 데 사용됩니다.

```
ciscoasa#debug icmp trace
```

사용자는 ASA의 내부 인터페이스(ping 192.168.1.1)을 ping합니다. 이 출력은 콘솔에 표시됩니다.

```
ciscoasa#
!--- Output is suppressed. ICMP echo request from 192.168.1.50 to 192.168.1.1 ID=512
seq=5120 len=32
ICMP echo reply from 192.168.1.1 to 192.168.1.50 ID=512 seq=5120 len=32
!--- The user IP address is 192.168.1.50.
```

debug icmp 추적을 비활성화하려면 다음 명령 중 하나를 사용합니다.**디버그 icmp 추적 없음** **undebug icmp 추적모두 디버그 해제**, **모두 디버그** 해제 또는 **모두 실행**

이 세 가지 옵션 각각은 관리자가 소스 IP 주소를 결정하는 데 도움이 됩니다.이 예에서는 사용자의 소스 IP 주소가 192.168.1.50입니다. 관리자는 애플리케이션 X에 대해 자세히 알아보고 문제의 원인을 확인할 수 있습니다.

2단계 - 문제의 원인 찾기

이 문서의 1단계 섹션에 나열된 정보에 대한 참조를 통해 관리자는 애플리케이션 X 세션의 소스를

파악합니다.관리자는 애플리케이션 X에 대해 자세히 알아보고 문제가 발생할 수 있는 위치를 찾을 준비가 되었습니다.

ASA/PIX 관리자는 나열된 제안 중 하나 이상에 대해 ASA를 준비해야 합니다.관리자가 준비되면 사용자는 애플리케이션 X를 시작하고 다른 모든 활동을 제한합니다. 추가 사용자 활동으로 인해 혼란이 발생하거나 ASA/PIX 관리자가 잘못 사용될 수 있기 때문입니다.

- **syslog 메시지를 모니터링합니다.**1단계에 위치한 사용자의 소스 IP 주소를 검색합니다. 사용자는 애플리케이션 X를 시작합니다. ASA 관리자는 **show logging** 명령을 실행하고 출력을 봅니다.

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-6-
305011: Built dynamic TCP translation from inside:192.168.1.50/1107 to
outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP connection 90 for
outside:172.22.1.1/80
(172.22.1.1/80) to inside:192.168.1.50/1107 (172.22.1.254/1025)
```

로그는 목적지 IP 주소가 172.22.1.1, 프로토콜은 TCP, 목적지 포트는 HTTP/80, 트래픽은 외부 인터페이스로 전송됨을 나타냅니다.

- **캡처 필터를 수정합니다.**access-list inside_test 명령은 이전에 사용되었으며 여기에서 사용됩니다.

```
ciscoasa(config)#access-list inside_test permit ip host 192.168.1.50 any
!--- This ACL line captures all traffic from 192.168.1.50 !--- that goes to or through the
ASA. ciscoasa(config)#access-list inside_test permit ip any host 192.168.1.50 any
!--- This ACL line captures all traffic that leaves !--- the ASA and goes to 192.168.1.50.
ciscoasa(config)#no access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#clear capture inside_interface
!--- Clears the previously logged data. !--- The no capture inside_interface removes/deletes
the capture.
```

사용자가 애플리케이션 X를 시작합니다. 그러면 ASA 관리자가 **show capture inside_interface** 명령을 실행하고 출력을 봅니다.

```
ciscoasa(config)#show capture inside_interface
1: 15:59:42.749152 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
2: 15:59:45.659145 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
3: 15:59:51.668742 192.168.1.50.1107 > 172.22.1.1.80:
S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK>
```

캡처된 트래픽은 관리자에게 몇 가지 중요한 정보를 제공합니다.대상 주소 - 172.22.1.1포트 번호 - 80/httpProtocol(프로토콜) - TCP("S" 또는 syn 플래그 알림)또한 관리자는 애플리케이션 X의 데이터 트래픽이 ASA에 도착한다는 것도 알고 있습니다.출력이 show capture **inside_interface** 명령 출력인 경우 애플리케이션 트래픽이 ASA에 도달하지 않았거나 캡처 필터가 트래픽을 캡처하도록 설정되지 않은 것입니다.

```
ciscoasa#show capture inside_interface
0 packet captured
0 packet shown
```

이 경우 관리자는 사용자 컴퓨터와 ASA 사이의 경로에 있는 사용자 컴퓨터 및 라우터 또는 기타 네트워크 장치를 조사하는 것을 고려해야 합니다.**참고:** 트래픽이 인터페이스에 도달하면 **capture** 명령은 ASA 보안 정책이 트래픽을 분석하기 전에 데이터를 기록합니다.예를 들어 access-list는 인터페이스에서 들어오는 모든 트래픽을 거부합니다.capture 명령은 여전히 트래픽을 기록합니다.그런 다음 ASA 보안 정책이 트래픽을 분석합니다.

- **디버그**관리자는 응용 프로그램 X에 익숙하지 않으므로 응용 프로그램 X 조사에 사용할 디버그 서비스 중 어떤 서비스를 사용할 것인지 알지 못합니다.디버그가 이 시점에서 최적의 문제 해결 옵션이 아닐 수 있습니다.

2단계에서 수집한 정보를 통해 ASA 관리자는 몇 가지 유용한 정보를 얻을 수 있습니다.관리자는 트래픽이 ASA의 내부 인터페이스, 소스 IP 주소, 대상 IP 주소 및 X가 사용하는 서비스 애플리케이션(TCP/80)에 도착한다는 사실을 알고 있습니다. syslogs에서 관리자는 통신이 처음에 허용되었음을 알고 있습니다.

3단계 - 애플리케이션 트래픽 확인 및 모니터링

ASA 관리자는 애플리케이션 X 트래픽이 ASA에서 나갔음을 확인하고 애플리케이션 X 서버의 반환 트래픽을 모니터링합니다.

- **syslog 메시지를 모니터링합니다.**소스 IP 주소(192.168.1.50) 또는 대상 IP 주소(172.22.1.1)에 대한 syslog 메시지를 필터링합니다. 명령줄에서 syslog 메시지를 필터링하면 **show logging**과 같습니다. **| 192.168.1.50 포함** 또는 **show logging |에는 172.22.1.1이 포함됩니다**. 이 예에서 **show logging** 명령은 필터 없이 사용됩니다.쉽게 읽을 수 있도록 출력이 억제됩니다.

```
ciscoasa#show logging
!--- Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-7-
609001: Built local-host outside:172.22.1.1 %ASA-6-305011: Built dynamic TCP translation
from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP
connection 90 for outside:172.22.1.1/80 (172.22.1.1/80) to inside:192.168.1.50/1107
(172.22.1.254/1025) %ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80
to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout
%ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30
%ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107
to outside:172.22.1.254/1025 duration 0:01:00
%ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00
```

  syslog 메시지는 SYN 시간 초과 때문에 연결이 닫혔음을 나타냅니다.그러면 관리자가 ASA에서 애플리케이션 X 서버 응답을 수신하지 않았음을 알 수 있습니다.Syslog 메시지 종료 이유는 다를 수 있습니다.3방향 핸드셰이크 완료 후 30초 후에 발생한 강제 연결 종료 때문에 SYN 시간 제한이 로깅됩니다.이 문제는 일반적으로 서버가 연결 요청에 응답하지 못하고 대부분의 경우 PIX/ASA의 컨피그레이션과 관련이 없는 경우에 발생합니다.이 문제를 해결하려면 다음 체크리스트를 참조하십시오.static 명령을 올바르게 입력했는지, 다른 정적 명령과 겹치지 않는지 확인합니다. 예를 들면 다음과 같습니다.

```
static (inside,outside) x.x.x.x  y.y.y.y netmask 255.255.255.255
```

  ASA 8.3 이상의 고정 NAT는 다음과 같이 구성할 수 있습니다.

```
object network obj-y.y.y.y
 host y.y.y.y
 nat (inside,outside) static x.x.x.x
```

  외부에서 전역 IP 주소에 대한 액세스를 허용하기 위해 액세스 목록이 있고 인터페이스에 바인딩되어 있는지 확인합니다.

```
access-list OUTSIDE_IN extended permit tcp any host x.x.x.x eq www
access-group OUTSIDE_IN in interface outside
```

  서버에 성공적으로 연결하려면 서버의 기본 게이트웨이가 PIX/ASA의 DMZ 인터페이스를 가리켜야 합니다.syslog 메시지에 대한 자세한 내용은 ASA 시스템 메시지를 참조하십시오.
- **새 캡처 필터를 만듭니다.**이전에 캡처된 트래픽 및 syslog 메시지에서 관리자는 애플리케이션 X가 외부 인터페이스를 통해 ASA를 남겨야 한다는 사실을 알고 있습니다.

```
ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80
!--- When you leave the source as 'any', it allows !--- the administrator to monitor any
network address translation (NAT). ciscoasa(config)#access-list outside_test permit tcp host
172.22.1.1 eq 80 any
!--- When you reverse the source and destination information, !--- it allows return traffic
to be captured. ciscoasa(config)#capture outside_interface access-list outside_test
```

```
interface outside
```

사용자는 애플리케이션 X로 새 세션을 시작해야 합니다. 사용자가 새 애플리케이션 X 세션을 시작한 후 ASA 관리자는 ASA에서 **show capture outside_interface** 명령을 실행해야 합니다.

```
ciscoasa(config)#show capture outside_interface
3 packets captured
   1: 16:15:34.278870 172.22.1.254.1026 > 172.22.1.1.80:
S 1676965539:1676965539(0) win 65535 <mss 1380,nop,nop,sackOK>
   2: 16:15:44.969630 172.22.1.254.1027 > 172.22.1.1.80:
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
   3: 16:15:47.898619 172.22.1.254.1027 > 172.22.1.1.80:
S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK>
3 packets shown
```

캡처는 외부 인터페이스에서 나가는 트래픽을 보여주지만 172.22.1.1 서버의 응답 트래픽은 표시하지 않습니다.이 캡처는 ASA에서 나가는 데이터를 보여줍니다.

- **packet-tracer 옵션을 사용합니다.**이전 섹션에서 ASA 관리자는 ASA에서 **packet-tracer** 옵션을 사용할 수 있는 충분한 정보를 학습했습니다.**참고:** ASA는 버전 7.2에서 시작하는 **packet-tracer** 명령을 지원합니다.

```
ciscoasa#packet-tracer input inside tcp 192.168.1.50 1025 172.22.1.1 http
!--- This line indicates a source port of 1025. If the source !--- port is not known, any
number can be used. !--- More common source ports typically range !--- between 1025 and
65535. Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC
Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule
Additional Information: MAC Access list Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW
Config: Additional Information: Found no matching flow, creating a new flow Phase: 4 Type:
ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.22.1.0
255.255.255.0 outside Phase: 5 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-
group inside_acl in interface inside
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
  match ip inside 192.168.1.0 255.255.255.0 outside any
    dynamic translation to pool 1 (172.22.1.254)
    translate_hits = 6, untranslate_hits = 0
Additional Information:
Dynamic translate 192.168.1.50/1025 to 172.22.1.254/1028
using netmask 255.255.255.255

Phase: 9
Type: NAT
Subtype: host-limits
```

```
Result: ALLOW
Config:
nat (inside) 1 192.168.1.0 255.255.255.0
  match ip inside 192.168.1.0 255.255.255.0 outside any
    dynamic translation to pool 1 (172.22.1.254)
    translate_hits = 6, untranslate_hits = 0
Additional Information:

Phase: 10
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 94, packet dispatched to next module

Phase: 15
Type: ROUTE-LOOKUP
Subtype: output and adjacency
Result: ALLOW
Config:
Additional Information:
found next-hop 172.22.1.1 using egress ifc outside
adjacency Active
next-hop mac address 0030.a377.f854 hits 11
!--- The MAC address is at Layer 2 of the OSI model. !--- This tells the administrator the
next host !--- that should receive the data packet. Result: input-interface: inside input-
status: up input-line-status: up output-interface: outside output-status: up output-line-
status: up Action: allow
```

packet-tracer 명령의 가장 중요한 출력은 마지막 줄이며, 이는 `Action:`.

각 3단계의 세 가지 옵션은 ASA가 애플리케이션 X 문제에 대해 책임이 없음을 관리자에게 보여줍니다.애플리케이션 X 트래픽은 ASA를 떠나고 ASA는 애플리케이션 X 서버로부터 응답을 받지 않습니다.

다음 단계는 무엇입니까?

응용 프로그램 X가 사용자에게 올바르게 작동할 수 있도록 하는 구성 요소가 많이 있습니다.구성 요소에는 사용자 컴퓨터, 애플리케이션 X 클라이언트, 라우팅, 액세스 정책 및 애플리케이션 X 서버가 포함됩니다.이전 예에서는 ASA가 애플리케이션 X 트래픽을 수신하고 전달한다는 것을 확인했습니다.이제 서버 및 애플리케이션 X 관리자가 참여해야 합니다.관리자는 애플리케이션 서비스가 실행 중인지 확인하고 서버의 로그를 검토하고 서버 및 애플리케이션 X에서 사용자의 트래픽을 수신했는지 확인해야 합니다.

문제/장애:TCP-Proxy 연결 종료 오류 메시지

다음 오류 메시지가 표시됩니다.

```
%PIX|ASA-5-507001: Terminating TCP-Proxy connection from
interface_inside:source_address/source_port to interface_outside:dest_address/dest_port -
reassembly limit of limit bytes exceeded
```

솔루션

설명:이 메시지는 TCP 세그먼트를 어셈블하는 동안 리어셈블리 버퍼 제한을 초과할 경우 표시됩니다.

- *source_address/source_port* - 연결을 시작하는 패킷의 소스 IP 주소 및 소스 포트입니다.
- *dest_address/dest_port* - 연결을 시작하는 패킷의 대상 IP 주소 및 목적지 포트입니다.
- *interface_inside* - 연결을 시작한 패킷이 도착하는 인터페이스의 이름입니다.
- *interface_outside* - 연결을 시작한 패킷이 종료되는 인터페이스의 이름입니다.
- *limit* - 트래픽 클래스에 대해 구성된 원시 연결 제한입니다.

이 문제의 해결 방법은 보안 어플라이언스에서 RTSP 검사를 비활성화하는 것입니다.

```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  no inspect rtsp
```

자세한 내용은 Cisco 버그 ID CSCsl15229(등록된 고객만 해당)를 참조하십시오.

문제/장애:"%ASA-6-110003:라우팅이 src 인터페이스에서 프로토콜에 대한 next-hop을 찾지 못했습니다." 오류 메시지

ASA에서 로 트래픽을 `.%ASA-6-110003: src interface:src IP/src port to dest interface:dest IP/dest port` 오류 메시지 `next-hop .`

솔루션

이 오류는 ASA가 인터페이스 라우팅 테이블에서 다음 홉을 찾으려고 할 때 발생합니다.일반적으로

이 메시지는 ASA가 하나의 인터페이스에 구축된 xlate(translation)와 다른 인터페이스를 가리키는 경로가 있을 때 수신됩니다.NAT 문에 잘못된 컨피그레이션이 있는지 확인합니다.컨피그레이션이 잘못되면 오류가 해결될 수 있습니다.

문제/장애:ASA에서 " %ASA-5-305013:전달 및 역방향 플로우에 대해 일치하는 비대칭 NAT 규칙" 오류 메시지

연결이 ASA에 의해 차단되고 이 오류 메시지가 수신됩니다.

```
%ASA-5-305013: Asymmetric NAT rules matched for forward
 and reverse flows; Connection protocol src
 interface_name:source_address/source_port dest
 interface_name:dest_address/dest_port denied due to NAT reverse path
 failure.
```

솔루션

NAT가 수행될 때 ASA는 패킷을 역방향으로 전환하려고 시도하고 이것이 어떤 변환에 도달하는지 확인합니다.NAT 변환이 전혀 또는 다른 경우 불일치가 발생합니다.소스와 대상이 동일한 아웃바운드 및 수신 트래픽에 대해 구성된 서로 다른 NAT 규칙이 있는 경우 이 오류 메시지가 가장 일반적으로 표시됩니다.관련 트래픽에 대한 NAT 문을 확인합니다.

문제/장애:수신 오류 - %ASA-5-321001:시스템에 대한 리소스 'conns' 제한 10000에 도달했습니다.

솔루션

이 오류는 ASA를 통해 위치한 서버의 연결이 최대 제한에 도달했음을 나타냅니다.이는 네트워크의 서버에 대한 DoS 공격을 나타내는 것일 수 있습니다.ASA에서 MPF를 사용하고 초기 연결 제한을 줄입니다.또한 DCD(Dead Connection Detection)를 활성화합니다. 다음 구성 조각을 참조하십시오.

```
class-map limit
 match access-list limit
!
policy-map global_policy
 class limit
  set connection embryonic-conn-max 50
  set connection timeout embryonic 0:00:10 dcd
!
access-list limit line 1 extended permit tcp any host x.x.x.x
```

문제/장애:오류 %PIX-1-106021 수신:인터페이스 int_name의 src_addr에서 dest_addr까지의 TCP/UDP 역방향 경로 확인 거부

솔루션

이 로그 메시지는 역방향 경로 검사가 활성화된 경우 수신됩니다.문제를 해결하고 역방향 경로 검사를 비활성화하려면 다음 명령을 실행합니다.

```
no ip verify reverse-path interface
```

문제/장애:위협 탐지로 인한 인터넷 연결 중단

이 오류 메시지는 ASA에서 수신됩니다.

```
%ASA-4-733100: [Miralix Licen 3000] drop rate-1 exceeded. Current burst
rate is 100 per second, max configured rate is 10; Current average rate is 4
per second, max configured rate is 5; Cumulative total count is 2526
```

솔루션

이 메시지는 비정상적인 트래픽 동작이 탐지될 때 기본 컨피그레이션으로 인해 위협 감지에 의해 생성됩니다.이 메시지는 TCP/UDP 포트인 Miralix Licen 3000에 중점을 둡니다.포트 3000을 사용하는 디바이스를 찾습니다.위협 탐지에 대한 ASDM 그래픽 통계를 확인하고 상위 공격을 확인하여 포트 3000 및 소스 IP 주소를 표시하는지 확인합니다.합법적인 디바이스인 경우 이 오류 메시지를 해결하기 위해 ASA의 기본 위협 탐지 속도를 높일 수 있습니다.

관련 정보

- Cisco ASA 명령 참조
- Cisco PIX 명령 참조
- Cisco ASA 오류 및 시스템 메시지
- Cisco PIX 오류 및 시스템 메시지
- Cisco ASA 5500 Series Adaptive Security Appliances 지원
- Cisco PIX 500 Series 보안 어플라이언스 지원
- 기술 지원 및 문서 – Cisco Systems