NBAR 및 ACL을 사용하여 "코드 레드" WORM 차단

목차

소개

이 문서에서는 Cisco 라우터의 Cisco IOS® Software에서 NBAR(Network-Based Application Recognition) 및 ACL(Access Control Lists)을 통해 네트워크 인그레스 포인트에서 "코드 레드(Code Red)" WORM을 차단하는 방법을 제공합니다. 이 솔루션은 Microsoft의 IIS 서버에 권장되는 패치와 함께 사용해야 합니다.

참고: 이 방법은 Cisco 1600 Series 라우터에서 작동하지 않습니다.

참고: P2P 프로토콜의 특성 때문에 일부 P2P 트래픽을 완전히 차단할 수 없습니다. 이러한 P2P 프로토콜은 트래픽을 완전히 차단하려는 DPI 엔진을 우회하도록 동적으로 시그니처를 변경합니다. 따라서 대역폭을 완전히 차단하지 않고 제한하는 것이 좋습니다. 이 트래픽의 대역폭을 조절합니다. 훨씬 적은 대역폭을 제공합니다. 그러나 연결이 끊어집니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 모듈형 QoS CLI(Command Line Interface)의 명령을 사용하여 QoS(Quality of Service) 서비스

정책을 생성합니다.
- NBAR
- ACL
- 정책 기반 라우팅

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다. 이 문서의 컨피그레이션은 Cisco IOS 버전 12.2(24a)를 실행하는 Cisco 3640에서 테스트되었습니다.

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.

표기 규칙

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

"코드 레드" WORM 차단 방법

"코드 레드"를 방지하기 위해 가장 먼저 해야 할 일은 Microsoft에서 제공하는 패치를 적용하는 것입니다(방법 A: 아래에 ACL을 사용하십시오. 그러면 취약한 시스템이 보호되고 감염된 시스템에서 WORM이 제거됩니다. 그러나 서버에 패치를 적용하면 worm이 서버를 감염시키는 것을 방지하지만 HTTP GET 요청이 서버에 도달하는 것을 막지 않습니다. 서버가 많은 감염 시도를 퍼부을 가능성이 여전히 있다.

이 권고 사항에 대한 솔루션은 Microsoft 패치와 함께 작동하여 네트워크 인그레스 포인트에서 "Code Red" HTTP GET 요청을 차단하도록 설계되었습니다.

이 솔루션은 감염을 차단하려고 시도하지만 HTTP GET 요청의 내용을 분석하는 유일한 방법은 TCP 연결을 설정한 후에 HTTP GET 요청의 내용을 분석하는 것이기 때문에 많은 수의 캐시 항목, 인접성 및 NAT/PAT 항목의 증가로 인한 문제를 치료하지 않습니다. 다음 절차는 네트워크 스캔을 방지하는 데 도움이 되지 않습니다. 그러나 외부 네트워크로부터 사이트를 보호하거나 시스템이 서비스해야 하는 감염 횟수를 줄입니다. 인바운드 필터링과 함께 아웃바운드 필터링은 감염된 클라이언트가 "Code Red(코드 레드)" WORM을 전역 인터넷으로 전파하지 못하도록 합니다.

지원되는 플랫폼

이 문서에서 설명하는 솔루션에는 Cisco IOS 소프트웨어 내의 클래스 기반 마킹 기능이 필요합니다. 특히 HTTP URL의 모든 부분에서 매칭하는 기능은 NBAR 내의 HTTP 하위 포트 분류 기능을 사용합니다. 지원되는 플랫폼 및 최소 Cisco IOS 소프트웨어 요구 사항은 아래에 요약되어 있습니다.

플랫폼	최소 Cisco IOS 소프트웨어
7200	12.1(5)T
7100	12.1(5)T
3745	12.2(8)T
3725	12.2(8)T
3660	12.1(5)T

3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(2)T

참고: NBAR를 사용하려면 Cisco CEF(Express Forwarding)를 활성화해야 합니다.

클래스 기반 마킹 및 DNBAR(Distributed NBAR)는 다음 플랫폼에서도 사용할 수 있습니다.

플랫폼	최소 Cisco IOS 소프트웨어
7500	12.1(6)E
FlexWAN	12.1(6)E

IIS 웹 로그에서 감염 시도 탐지

초기 감염 시도에서는 큰 HTTP GET 요청을 대상 IIS 서버로 보냅니다. 원래 "코드 레드" 설치 공간은 다음과 같습니다.

```
2001-08-04 16:32:23 10.101.17.216 - 10.1.1.75 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u
7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403
```

"Code Red(코드 레드)" II 설치 공간은 다음과 같습니다.

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090
%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%
u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403 -
```

GET 요청은 항상 확장명이 .ida인 파일을 찾습니다. 이는 모든 감염 시도에서 일반적인 문자열이므로 IOS에서 클래스 기반 표시를 사용하는 일치 조건으로 사용할 수 있습니다. GET 요청의 나머지 부분은 버퍼 오버플로를 만들려고 하는 것이므로 반드시 일치하지는 않습니다. 위의 두 항목을 비교하여 볼 수 있습니다.

이 두 서명 사이의 차이는 CodeRed.v3 또는 CodeRed.C라는 "Code Red" worm의 새로운 변종 때문에 보고되고 있습니다. 원래 "Code Red(코드 빨간색)" 변형에는 GET 요청에 "NNNNNNNNNN" 문자열이 포함되며, 새 변형에는 "XXXXXXXX"가 포함됩니다. 자세한 내용은 Symantec 자문을 참조하십시오.

2001년 8월 6일 오후 6시 24분 EDT에서 새로운 공간을 기록했습니다. 그 후 eEye 취약성 스캐너에 의해 남겨진 공간이 있습니다.

```
2001-08-06 22:24:02 10.30.203.202 - 10.1.1.9 80 GET /x.ida AAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X 403 HTTP/1.1 -
```

이 권고 사항에 제공된 "코드 레드"를 차단하는 기술은 다음 단원에 표시된 대로 클래스 맵 정의를

강화하여 이러한 스캐닝 시도를 차단할 수도 있습니다.

IOS 클래스 기반 마킹 기능을 사용하여 인바운드 "코드 빨간색" 해킹으로 표시

"코드 레드" 벌레를 차단하려면 아래에 설명된 세 가지 방법 중 하나를 사용합니다. 세 가지 방법 모두 Cisco IOS MQC 기능을 사용하여 악성 트래픽을 분류합니다. 그런 다음 아래 설명된 대로 이 트래픽이 삭제됩니다.

방법 A: ACL 사용

이 메서드는 출력 인터페이스에서 ACL을 사용하여 표시된 "Code Red" 패킷을 삭제합니다. 다음 네트워크 다이어그램을 사용하여 이 방법의 단계를 설명하겠습니다.

이 방법을 구성하는 단계는 다음과 같습니다.

1. 아래와 같이 Cisco IOS 소프트웨어의 클래스 기반 마킹 기능으로 인바운드 "코드 레드" 해킹을 분류합니다.
   ```
   Router(config)#class-map match-any http-hacks
   Router(config-cmap)#match protocol http url "*default.ida*"
   Router(config-cmap)#match protocol http url "*cmd.exe*"
   Router(config-cmap)#match protocol http url "*root.exe*"
   ```

   위의 클래스 맵은 HTTP URL의 내부에서 검색되며 지정된 모든 문자열과 일치합니다. "코드 레드"의 default.ida 외에 다른 파일 이름이 포함되어 있습니다. 다음 문서에서 설명하는 Sadmind 바이러스와 같은 유사한 해킹 시도를 차단하는 데 이 기술을 사용할 수 있습니다 .http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.html
2. 정책을 구축하고 **set** 명령을 사용하여 인바운드 "Code Red" 해킹을 정책 맵으로 표시합니다. 이 문서에서는 다른 네트워크 트래픽이 이 값을 전달하지 않을 가능성이 있으므로 DSCP 값 1(10진수)을 사용합니다.여기서는 인바운드 "Code Red" 해킹을 "mark-inbound-http-hacks"라는 정책 맵으로 표시합니다.
   ```
   Router(config)#policy-map mark-inbound-http-hacks
   Router(config-pmap)#class http-hacks
   Router(config-pmap-c)#set ip dscp 1
   ```

3. 수신 "Code Red" 패킷을 표시하려면 입력 인터페이스에서 인바운드 정책으로 정책을 적용합니다.
   ```
   Router(config)#interface serial 0/0
   Router(config-if)#service-policy input mark-inbound-http-hacks
   ```

4. 서비스 정책에 의해 설정된 대로 DSCP 값 1에서 일치하는 ACL을 구성합니다.
   ```
   Router(config)#access-list 105 deny ip any any dscp 1
   Router(config)#access-list 105 permit ip any any
   ```

참고: Cisco IOS Software Releases 12.2(11) 및 12.2(11)NBAR(CSCdv48172)와 함께 사용할 클래스 맵에서 정의하는 ACL의 **log** 키워드를 지원합니다. 이전 릴리스를 사용하는 경우 ACL에서 **log** 키워드를 사용하지 마십시오. 이렇게 하면 모든 패킷이 CEF-switched 대신 프로세스 스위칭이 되고 NBAR는 CEF가 필요하므로 작동하지 않습니다.

5. 대상 웹 서버에 연결하는 출력 인터페이스에 ACL 아웃바운드를 적용합니다.
```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```

6. 솔루션이 예상대로 작동하는지 확인합니다. show access-**list** 명령을 실행하고 deny 문의 "matches" 값이 증가하는지 확인합니다.
```
Router#show access-list 105
Extended IP access list 105
 deny ip any any dscp 1 log (2406 matches)
 permit ip any any (731764 matches)
```
컨피그레이션 단계에서 **no ip unreachable** interface-level 명령을 사용하여 IP 연결 불가 메시지 전송을 비활성화하여 라우터가 과도한 리소스를 확장하도록 할 수도 있습니다.Method B 섹션에 설명된 대로 DSCP=1 트래픽을 Null 0으로 정책 라우팅할 수 있는 경우에는 이 방법을 사용하지 않는 것이 좋습니다.

방법 B: PBR(Policy-Based Routing) 사용

이 방법은 정책 기반 라우팅을 사용하여 표시된 "Code Red" 패킷을 차단합니다. 메서드 A 또는 C가 이미 구성된 경우 이 메서드의 명령을 적용할 필요가 없습니다.

이 방법을 구현하는 단계는 다음과 같습니다.

1. 트래픽을 분류하고 표시합니다. 메서드 A에 표시된 **class-map** 및 **policy-map** 명령을 사용합니다.
2. **service-policy** 명령을 사용하여 정책을 입력 인터페이스에서 인바운드 정책으로 적용하여 도착하는 "Code Red" 패킷을 표시합니다. 방법 A를 참조하십시오.
3. 표시된 "Code Red" 패킷에서 일치하는 확장 IP ACL을 생성합니다.
```
Router(config)#access-list 106 permit ip any any dscp 1
```

4. 라우팅 정책을 **작성하려면 route-map** 명령을 사용합니다.
```
Router(config)#route-map null_policy_route 10
Router(config-route-map)#match ip address 106
Router(config-route-map)#set interface Null0
```
5. 경로 맵을 입력 인터페이스에 적용합니다.
```
Router(config)#interface serial 0/0
Router(config-if)#ip policy route-map null_policy_route
```

6. 솔루션이 예상대로 작동하는지 **show access-list** 명령에서 확인합니다. 출력 ACL을 사용 중이고 ACL 로깅을 활성화한 경우 아래와 같이 **show log** 명령을 사용할 수도 있습니다.
```
Router#show access-list 106
Extended IP access list 106
```

```
 permit ip any any dscp 1 (1506 matches)

Router#show log
Aug 4 13:25:20: %SEC-6-IPACCESSLOGP:
 list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
Aug 4 13:26:32: %SEC-6-IPACCESSLOGP:
 list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
```

모든 이그레스 인터페이스에서 출력 ACL이 필요 없이 라우터의 인그레스 인터페이스에서 폐기 결정을 내릴 수 있습니다. 다시 한 번, no ip unreachables 명령을 사용하여 전송 IP 도달 불가 메시지**를 비활성화하는 것이** 좋습니다.

방법 C: 클래스 기반 폴리싱 사용

이 방법은 PBR 또는 출력 ACL에 의존하지 않으므로 일반적으로 가장 확장성이 뛰어납니다.

1. 메소드 A에 표시된 class-map 명령을 사용하여 트래픽을 분류합니다.
2. policy-map 명령을 사용하여 정책을 구축하고 police 명령을 사용하여 이 트래픽에 대한 삭제 작업을 지정합니다.

```
Router(config)#policy-map drop-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#police 1000000 31250 31250
 conform-action drop exceed-action drop violate-action drop
```

3. 입력 인터페이스에서 정책을 인바운드 정책으로 적용하여 "Code Red" 패킷을 삭제하려면 service-policy 명령을 사용합니다.

```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input drop-inbound-http-hacks
```

4. 솔루션이 show policy-map interface 명령에서 예상대로 작동하는지 확인합니다. 클래스 및 개별 일치 조건에 대한 값이 증가하는지 확인합니다.

```
Router#show policy-map interface serial 0/0

Serial0/0

  Service-policy input: drop-inbound-http-hacks

    Class-map: http-hacks (match-any)
      5 packets, 300 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol http url "*default.ida*"
        5 packets, 300 bytes
        5 minute rate 0 bps
      Match: protocol http url "*cmd.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol http url "*root.exe*"
        0 packets, 0 bytes
        5 minute rate 0 bps
      police:
        1000000 bps, 31250 limit, 31250 extended limit
        conformed 5 packets, 300 bytes; action: drop
        exceeded 0 packets, 0 bytes; action: drop
        violated 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps

    Class-map: class-default (match-any)
      5 packets, 300 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
```

```
        Match: any
```

NBAR 제한 사항

이 문서의 메서드와 함께 NBAR를 사용하는 경우 NBAR에서는 다음 기능이 지원되지 않습니다.

- 24개 이상의 동시 URL, HOST 또는 MIME 유형 일치
- URL의 첫 400바이트를 초과하는 일치
- 비 IP 트래픽
- 멀티캐스트 및 기타 비CEF 스위칭 모드
- 단편화된 패킷
- 파이프라인된 영구 HTTP 요청
- 보안 HTTP를 통한 URL/HOST/MIME/분류
- 상태 저장 프로토콜이 있는 비대칭 흐름
- NBAR를 실행하는 라우터에서 시작하거나 라우터로 향하는 패킷

다음 논리적 인터페이스에서는 NBAR를 구성할 수 없습니다.

- Fast EtherChannel
- 터널링 또는 암호화를 사용하는 인터페이스
- VLAN
- 다이얼러 인터페이스
- 멀티링크 PPP

참고: NBAR는 Cisco IOS Release 12.1(13)E의 VLAN에서 구성할 수 있지만 소프트웨어 스위칭 경로에서만 지원됩니다.

NBAR는 터널링 또는 암호화가 사용되는 WAN 링크의 출력 트래픽을 분류하는 데 사용할 수 없으므로, 트래픽을 출력하기 위해 WAN 링크로 전환하기 전에 입력 분류를 수행하기 위해 LAN 인터페이스와 같은 라우터의 다른 인터페이스에 대신 적용합니다.

NBAR 정보에 대한 자세한 내용은 관련 정보의 링크를 참조하십시오.