使用NBAR和ACL阻止「紅色代碼」蠕蟲

目錄

簡介

本文提供在Cisco路由器的Cisco IOS®軟體中，透過網路型應用程式辨識(NBAR)和存取控制清單(ACL)，在網路輸入點封鎖「Code Red」蠕蟲的方法。此解決方案應與Microsoft為IIS伺服器推薦的修補程式結合使用。

注意：此方法在Cisco 1600系列路由器上不起作用。

注意：某些P2P流量因其P2P協定的性質而無法完全阻止。這些P2P協定動態更改其簽名，以繞過嘗試完全阻止其流量的任何DPI引擎。因此，建議限制頻寬，而不是完全阻塞頻寬。限制此流量的頻寬。提供少得多的頻寬；但是，讓連線通過。

必要條件

需求

思科建議您瞭解以下主題：

- 使用模組化QoS命令列介面(CLI)的命令[的服務品質](#)(QoS)服務策略。
- NBAR
- ACL

- 基於策略的路由

採用元件

本文件所述內容不限於特定軟體和硬體版本。本檔案中的組態已在執行Cisco IOS版本12.2(24a)的Cisco 3640上測試

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

如何阻止「紅色代碼」蠕蟲

要對抗「紅色代碼」，您首先應該做的就是應用Microsoft提供的補丁程式(請參閱下面的方法A：使用ACL一節中的連結)。這樣可以保護易受攻擊的系統，並從受感染的系統刪除蠕蟲。但是，將該修補程式應用到伺服器只能防止蠕蟲感染伺服器，並不會阻止HTTP GET請求進入伺服器。伺服器仍有可能遭受大量感染嘗試的攻擊。

本建議中詳述的解決方案旨在與Microsoft補丁結合使用，在網路入口點阻止「Code Red」 HTTP GET請求。

此解決方案嘗試阻止感染，但它無法解決由於大量快取條目、鄰接關係和NAT/PAT條目累積而導致的問題，因為分析HTTP GET請求內容的唯一方法是建立TCP連線。以下步驟無助於防止網路掃描。但是，它將保護站點免受外部網路感染，或者減少電腦必須服務的感染嘗試次數。與入站過濾結合使用時，出站過濾可防止受感染的客戶端將「紅色代碼」蠕蟲傳播到全球網際網路。

支援的平台

本檔案所述的解決方案需要Cisco IOS軟體中的類別型標籤功能。具體而言，在HTTP URL的任何部分上進行匹配的功能會使用NBAR中的HTTP子埠分類功能。支援的平台和最低Cisco IOS軟體要求概述如下：

平台	最低Cisco IOS軟體
7200	12.1(5)公噸
7100	12.1(5)公噸
3745	12.2(8)公噸
3725	12.2(8)公噸
3660	12.1(5)公噸
3640	12.1(5)公噸
3620	12.1(5)公噸

2600	12.1(5)公噸
1700	12.2(2)公噸

注意：您需要啟用Cisco Express Forwarding(CEF)才能使用NBAR。

以下平台上還提供了基於類的標籤和分散式NBAR(DNBAR):

平台	最低Cisco IOS軟體
7500	12.1(6)E
FlexWAN	12.1(6)E

在IIS Web日誌中檢測感染嘗試

初始感染嘗試向目標IIS伺服器傳送一個大型HTTP GET請求。最初的「紅色代碼」印跡顯示如下：

```
2001-08-04 16:32:23 10.101.17.216 - 10.1.1.75 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
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
```

「紅色代碼」II的足跡顯示如下：

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%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 -
```

請注意，GET請求始終查詢副檔名為.ida的檔案。這是所有感染嘗試中的常見字串，因此可以在IOS中用作具有基於類的標籤的匹配條件。GET請求的其餘部分不一定一致，因為它只是嘗試建立緩衝區溢位。通過比較上面的兩個條目可以看到這一點。

現在有報導稱，這兩個特徵碼之間的差別是由於新的「Code Red」蠕蟲病毒株，稱為CodeRed.v3或CodeRed.C。原始的「紅色代碼」變種在GET請求中包含「NNNNNNN」字串，而新變種包含「XXXXXXXX」。有關詳細資訊，請參閱Symantec建議。

2001年8月6日，美國東部時間下午6:24，我們錄得新的足跡。我們後來瞭解到，這是eEye漏洞掃描器留下的足跡。

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

此建議中提供的阻止「Code Red」的技術還可以通過收緊類對映定義（如下一部分所示）來阻止這些掃描嘗試。

使用IOS類別型標籤功能標籤入站「紅色代碼」攻擊

要阻止「紅色代碼」蠕蟲，請使用以下三種方法之一。這三種方法都使用Cisco IOS MQC功能對惡意流量進行分類。然後按照以下說明丟棄此流量。

方法A：使用ACL

此方法使用輸出介面上的ACL來捨棄標籤為「Code Red」的封包。讓我們使用以下網路圖說明此方法的步驟：

以下是設定此方法的步驟：

1. 使用Cisco IOS軟體中基於類的標籤功能對入站「紅色代碼」駭客進行分類，如下所示：

```
<#root>
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*"
```

上面的類對映檢視HTTP URL的內部並與任何指定的字串匹配。請注意，除了「Code Red」的default.ida之外，我們還包含其他檔名。您可以使用此技術阻止類似的入侵嘗試，如Sadmind病毒，將在以下文檔中說明：

- http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp
- http://www.sophos.com/virusinfo/analyses/unixsadmind.html

2. 構建策略並使用set命令將入站「紅色代碼」駭客與策略對映進行標籤。本檔案使用DSCP值1（十進位制），因為不可能有任何其他網路流量攜帶此值。

   此處我們使用名為「mark-inbound-http-hacks」的策略對映來標籤入站「紅色代碼」駭客。

```
<#root>

Router(config)#

policy-map mark-inbound-http-hacks

Router(config-pmap)#

class http-hacks

Router(config-pmap-c)#

set ip dscp 1
```

3. 將該策略作為入站策略應用於輸入介面，以標籤到達的「紅色代碼」資料包。

```
<#root>

Router(config)#

interface serial 0/0

Router(config-if)#

service-policy input mark-inbound-http-hacks
```

4. 根據服務策略設定，在DSCP值1上配置匹配的ACL。

```
<#root>

Router(config)#

access-list 105 deny ip any any dscp 1

Router(config)#

access-list 105 permit ip any any
```

註：Cisco IOS軟體版本12.2(11)和12.2(11)T在定義類對映以與NBAR(CSCdv48172)一起使用時引入了對ACL上log關鍵字的支援。如果使用的是早期版本，請不要在ACL上使用log關鍵字。這麼做會強制所有封包進行程式交換而不是CEF交換，且NBAR無法運作，因為它需要CEF。

5. 在連線到目標Web伺服器的輸出介面上應用出站ACL。

```
<#root>

Router(config)#

interface ethernet 0/1


Router(config-if)#

ip access-group 105 out
```

6. 驗證您的解決方案是否按預期工作。執行show access-list命令，並確保deny語句的「matches」值遞增。

```
<#root>

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)
```

在設定步驟中，您還可以使用no ip unreachable介面層級指令停用傳送IP無法連線訊息，以避免導致路由器消耗過多資源。

如果可以策略性地將DSCP=1流量路由到Null 0（如方法B部分所述），則不建議使用此方法。

方法B：使用基於策略的路由(PBR)

此方法使用基於策略的路由來阻止標籤為「紅色代碼」的資料包。如果已配置方法A或C，則無需應用此方法中的命令。

以下是實施此方法的步驟：

1. 對流量進行分類並標籤。使用方法A中顯示的class-map和policy-map命令。
2. 使用service-policy命令將該策略作為入站策略應用於輸入介面，以標籤到達的「紅色代碼」資料包。參見方法A。
3. 建立與標籤的「紅色代碼」資料包匹配的擴展IP ACL。

```
<#root>

Router(config)#

access-list 106 permit ip any any dscp 1
```

4. 使用route-map命令構建路由策略。

```
<#root>

Router(config)#

route-map null_policy_route 10

Router(config-route-map)#

match ip address 106

Router(config-route-map)#

set interface Null0
```

5. 將路由對映應用於輸入介面。

```
<#root>

Router(config)#

interface serial 0/0

Router(config-if)#
```

```
ip policy route-map null_policy_route
```

6. 使用show access-list命令驗證您的解決方案是否按預期運作。如果使用輸出ACL並啟用了ACL日誌記錄，您還可以使用show log命令，如下所示：

```
<#root>

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
```

我們能夠在路由器的輸入介面做出丟棄決定，而不是在每個輸出介面上都需要一個輸出ACL。同樣地，我們建議使用no ip unreachables指令停用傳送IP無法到達訊息。

方法C：使用基於類的策略

此方法通常具有最高的可擴充性，因為它不依賴PBR或輸出ACL。

1. 使用方法A中所示的class-map命令對流量進行分類。
2. 使用policy-map命令構建策略，並使用police命令為此流量指定丟棄操作。

```
<#root>

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. 使用service-policy命令將該策略作為入站策略應用於輸入介面，以丟棄「紅色代碼」資料包。

```
<#root>

Router(config)#

interface serial 0/0


Router(config-if)#

service-policy input drop-inbound-http-hacks
```

4. 使用show policy-map interface命令驗證您的解決方案是否按預期工作。確保看到類和單個匹配條件的遞增值。

```
<#root>

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限制

將NBAR與本文檔中的方法一起使用時，請注意NBAR不支援以下功能：

- 超過24個併發URL、主機或MIME型別匹配
- 在URL中的前400位元組之外進行比對
- 非IP流量
- 組播和其他非CEF交換模式
- 分段的資料包
- 流水線化的持久HTTP請求
- 使用安全HTTP的URL/主機/MIME/分類
- 使用有狀態協定的非對稱流
- 來自運行NBAR的路由器或發往路由器的資料包

您無法在以下邏輯介面上配置NBAR:

- 快速乙太通道
- 使用通道或加密的介面
- VLAN
- 撥號器介面
- 多重連結PPP

注意：自Cisco IOS版本12.1(13)E起，NBAR可在VLAN上配置，但僅在軟體交換路徑中受支援。

由於NBAR不能用於對使用隧道或加密的WAN鏈路上的輸出流量進行分類，因此請將其應用於路由器上的其他介面（如LAN介面），以便在流量切換到WAN鏈路進行輸出之前執行輸入分類。

有關NBAR的詳細資訊，請參閱相關資訊中的連結

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）。