

ACL " Code Red "をブロックするための Network-Based Application Recognition (NBAR) 使用は徐々に引出し、

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[" Code Red " ワームをブロックする方法](#)

[サポート対象プラットフォーム](#)

[IIS Web ログの感染試みを検出して下さい](#)

[IOS クラスベース マーキング機能を使用して受信 " Code Red "刻み目をマークして下さい](#)

[方式 A: ACLの使用](#)

[方式 B: ポリシーベース ルーティング \(PBR\)の使用](#)

[方式 C: クラスベース ポリシングの使用](#)

[NBAR 制限](#)

[既知の問題](#)

[関連情報](#)

[はじめに](#)

この資料は Network-Based Application Recognition (NBAR) によってネットワーク入力ポイントで" Code Red " ワームおよび Cisco IOS® ソフトウェア on Cisco ブロックするために方式をルータ内のアクセス コントロール リスト (ACL) を提供したものです。この解決策は、Microsoft 製 IIS サーバ用推奨パッチと一緒に使用する必要があります。

注: この方式は 1600 シリーズ ルータを on Cisco はたらかせません。

注: 一部の P2P トラフィックは、その P2P プロトコルの特性のために完全にブロックされない場合があります。これらの P2P プロトコルは動的に完全にトラフィックをブロックを試みる解像度エンジンをバイパスするためにシグニチャを変更します。従って、ブロッキングそれらの代わりに帯域幅を完全に制限することを推奨します。このトラフィックのための帯域幅を絞って下さい。より少ない帯域幅を大いに与えて下さい; ただし、接続が行くようにして下さい。

[前提条件](#)

[要件](#)

次の項目に関する知識が推奨されます。

- [モジュラ QoS Command Line Interface \(CLI \)](#) のコマンドを使用するサービス品質 (QoS) サービス ポリシー。
- [NBAR](#)
- ACL
- ポリシ ベースのルーティング

[使用するコンポーネント](#)

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。この資料の設定は Cisco 3640 でテストされました Cisco IOSバージョン 12.2(24a) を実行する

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

[表記法](#)

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

[" Code Red " ワームをブロックする方法](#)

"Code Red "を戦うためにする必要がある最初の事柄は Microsoft から加えます利用可能なパッチをあります (セクション [方式 A](#) のリンクを参照して下さい; 下記の [ACL を使用して下さい](#))。これは脆弱 なシステムを保護し、感染させたシステムからワームを取除きます。ただし、サーバにパッチを加えることはワームがサーバに打撃を与えることからだけサーバを感染させることを、それ停止しない HTTP GET 要求を防ぎます。今でも感染試みのフラッドが殺到するサーバのための可能性があります。

このアドバイザリで詳述されるソリューションは Microsoft パッチと共にはたらくようにネットワーク入力ポイントで " Code Red " HTTP GET 要求をブロックするために設計されています。

このソリューションは HTTP GET 要求の内容を分析する唯一の方法が TCP 接続の確立を次ので多数の Cache エントリ、隣接関係および NAT/PAT エントリの集結によって引き起こされた問題を治さないどんなに感染をブロックするように試みます。次のプロシージャはネットワークのスキャンから保護を助けません。ただし、それは外部ネットワークからの蔓延からサイトを保護するか、または保守するマシンが必要がある感染試みの数を減らします。受信 フィルタリングと組み合わせて、送信フィルタリングは感染させたクライアントがグローバル な インターネットに " Code Red " ワームを広げること防ぐ。

[サポート対象プラットフォーム](#)

この資料に説明があるソリューションは Cisco IOS ソフトウェア内のクラスベース マーキング機能を必要とします。特に、マッチング機能では、NBAR 内の HTTP サポートクラシフィケーション機能を使用します。サポートされているプラットフォームおよび IOS ソフトウェア最低必要条件を次に要約します。

プラットフォーム	最低限の Cisco IOS ソフトウェア
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

注: NBAR を使用することを Cisco Express Forwarding (CEF) が可能にする必要があります。

クラスベース マーキングおよび Distributed NBAR (DNBAR) は次のプラットフォームでも使用できます。

プラットフォーム	最低限の Cisco IOS ソフトウェア
7500	12.1(6)E
FlexWAN	12.1(6)E

[IIS Web ログの感染試みを検出して下さい](#)

最初の感染試みはターゲット IIS サーバに大きい HTTP GET 要求を送信 します。 オリジナル " Code Red " フットプリントは下記のように示されています:

```
2001-08-04 16:32:23 10.101.17.216 - 10.1.1.75 80 GET /default.ida
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNN%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 " II フットプリントは下記のように示されています:

```
2001-08-04 15:57:35 10.7.35.92 - 10.1.1.75 80 GET /default.ida XXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%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 要求が .ida 拡張を用いるファイルを常に探していることに注意して下さい。 従ってこれは 全ての感染試みのよくあるストリングで、としてクラスベース マーキングと IOS で一致条件使 用することが出来ます。 GET 要求の残りは必ずしもちょうどバッファオーバフローを作成す るように試みているように一貫していません。 これは上記の 2 つのエントリの比較によって見ら れる場合があります。

これら二つのシグニチャ間の違いが新しい種類がの " Code Red " ワーム、ダビングされた

CodeRed.v3 または CodeRed.C.原因であることが今報告されています。 オリジナル" Code Red "種は GET 要求で新しい種類は「」が含まれているが、「NNNNNNNN」字符串を示します。
。 [Symantec Advisory](#) を詳細については 参照して下さい。

6:24PM EDT 8月6日 2001 で、新しいフットプリントを記録しました。これが [eEye 脆弱性スキャナー](#)によって置き去りになるフットプリントであることをその後学んでいました。

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

このアドバイザリで提供される" Code Red "をブロックするための手法はまた次のセクションに示すようにクラスマップ定義をきつく締めることによってこれらをスキャン済み単にブロックできます。

[IOS クラスベース マーキング機能を使用して受信 " Code Red "刻み目をマークして下さい](#)

"Code Red "ワームをブロックするために、下記の3つのメソッドの1つを使用して下さい。3つのメソッドはすべて Cisco IOS MQC 機能を使用して悪意のあるトラフィックを分類します。このトラフィックはそれから下記のように廃棄されます。

[方式 A: ACLの使用](#)

この方式はマーク付き" Code Red "パケットを廃棄するのに出カインターフェイスの ACL を使用します。次のネットワーク図をこの方式のステップを説明するのに使用しよう:



ステップはこの方式の設定にここにあります:

1. 下記に示されているように Cisco IOS ソフトウェアのクラスベース マーキング機能が付いている受信 " Code Red "刻み目を、分類して下さい:

```
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*"
```

HTTP URL のの中の上記のクラスマップ外観はの特定の文字列一致し。" Code Red "の default.ida のほかの他のファイル名を含んでいたことに注意して下さい。同じような刻み目試みを、次に挙げるドキュメントで説明される Sadmin ウイルスのようなブロックするこの手法を使用できます

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

2. ポリシーを構築し、ポリシー マップで受信 " Code Red "刻み目をマークする set コマンドを

使用して下さい。この資料は他のどのネットワークトラフィックもこの値を運んでいることとはまずないので 1 という DSCP 値を使用します (小数点で)。ここに「mark-inbound-http-hacks」と指名されるポリシー マップで受信 " Code Red "刻み目をマークします。

```
Router(config)#policy-map mark-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#set ip dscp 1
```

3. 到着 " Code Red "パケットをマークするために入インターフェイスの受信 ポリシーとしてポリシーを適用して下さい。

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

4. 1 という DSCP 値で一致するサービス ポリシーによってセットで ACL を設定して下さい。

```
Router(config)#access-list 105 deny ip any any dscp 1
Router(config)#access-list 105 permit ip any any
```

注: Cisco IOS ソフトウェア リリース 12.2(11) および 12.2(11)T は NBAR

(CSCdv48172) と併用するためのクラスマップの定義の ACL の Log キーワードのサポートを導入します。以前のリリースを使用している場合、ACL の Log キーワードを使用しないで下さい。することはそうすべてのパケットを CEF スイッチの代わりにプロセス交換されるために強制し CEF を必要とするので NBAR ははたらきません。

5. ターゲットの Web サーバに接続する出インターフェイスで送信 ACL を適用して下さい。

```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```

6. ソリューションが予想通りはたらくことを確認して下さい。 show access-list コマンドを実行し、否定文のための " matches " 値が増分していることを確認して下さい。

```
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)
```

コンフィギュレーションのステップでは、またルータを余分なリソースを費やすために引き起こすことを避ける no ip unreachable interface-level コマンドで IP 到達不可能なメッセージを送信することを無効にすることができます。この方式は方式 B セクションに記述されているように 0 を無効にするポリシー ルート DSCP=1 トラフィックことができれば推奨されません。

方式 B: ポリシーベース ルーティング (PBR) の使用

この方式はマーク付き " Code Red "パケットをブロックするのにポリシーベースのルーティングを使用します。メソッド A か C が既に設定されている場合この方式のコマンドを適用する必要はありません。

ステップはこの方式の設定にここにあります:



1. トラフィックを分類し、それをマークして下さい。方式 A.で示されている **class-map** および **policy-map** コマンドを使用して下さい。
2. 入力インターフェイスの受信 ポリシーとしてポリシーを到着" Code Red "パケットをマークするために適用する **service-policy** コマンドを使用して下さい。方式 A.を参照して下さい。
3. マーク付き" Code Red "パケットで一一致する拡張 IP ACL を作成して下さい。

```
Router(config)#access-list 106 permit ip any any dscp 1
```

4. ルーティングポリシーを構築する **route-map** コマンドを使用して下さい。

```
Router(config)#route-map null_policy_route 10
Router(config-route-map)#match ip address 106
Router(config-route-map)#set interface Null0
```

5. 入力インターフェイスにルート マップを加えて下さい。

```
Router(config)#interface serial 0/0
Router(config-if)#ip policy route-map null_policy_route
```

6. **show access-list** コマンドをソリューション使用を期待どおりに確認して下さい。出力 ACL を使用していて、ACLロギングを有効にする場合、また下記に示されているように **show log** コマンドを、使用できます:

```
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
```

各出力インターフェイスの出力 ACL を作れます必要としますよりもむしろルータの入力インターフェイスで廃棄デジジョンを。再度、コマンド **no ip unreachable** コマンドで送信 IP 到達不可能なメッセージを無効にすることを推奨します。

方式 C: クラスベース ポリシングの使用

この方式は一般に PBR か出力 ACL に左右されないのが最も拡張が容易です。

1. 方式 A.で示されている **class-map** コマンドを使用してトラフィックを分類して下さい。
2. ポリシーを **policy-map** コマンドを使用して構築し、このトラフィックのためのドロップするアクションを規定する **police** コマンドを使用して下さい。

```
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. 入力インターフェイスの受信 ポリシーとしてポリシーを" Code Red "パケットを廃棄するために適用する **service-policy** コマンドを使用して下さい。

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

4. ソリューションが **show policy-map interface** コマンドを期待どおりに使用することを確認して下さい。クラスおよび個々の一致条件については値を増分することを見るようにして下さい。

```
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 制限

NBAR をこの資料でメソッドと使用した場合、次の機能が NBAR によってサポートされないことに注目して下さい:

- 24 同時 URL 以上、ホストまたは MIME 型は一致しません
- URL の最初の 400 バイトを越えて一致
- 非 IP トラフィック
- マルチキャストおよび他の非 CEF 切り替えモード
- フラグメント化されたパケット
- 導管で送られた耐久性がある HTTP 要求
- セキュア HTTP の URL/HOST/MIME/分類
- ステートフルプロトコルの同期フロー
- から起きるパケットまたは NBAR を実行するルータに予定されて

次の論理的なインターフェイスの NBAR を設定できません:

- Fast EtherChannel (FEC)
- トンネリングか暗号化を使用するインターフェイス
- VLAN
- ダイアラ インターフェイス
- マルチリンク PPP

注: NBAR は Cisco IOS Release 12.1(13)E 現在で VLAN で設定可能、しかしソフトウェア・スイッチングパスだけでサポートされています。

NBAR がトンネル伝送するか、または暗号化が使用される WAN リンクのトラフィックを出力するために分類するのに使用することができないので、トラフィックが出力への WAN リンクに切り替えられる前に入力 分類を行うためにルータの他のインターフェイスにそれを、LAN インター

フェイスのような、代りに適用して下さい。

より多くの NBAR 情報に関しては、[関連情報](#)のリンクを参照して下さい