アプリケーション認識型ファイアウォール

このドキュメントでは、NBAR が検出してゾーンベース ファイアウォール アプリケーションを認識させることができるアプリケーションに基づいて、ゾーンベース ファイアウォール ポリシーを定義する方法について説明します。アプリケーションファイアウォールは、トラフィックを検査し、アプリケーション、カテゴリ、アプリケーションファミリ、またはアプリケーショングループに基づいてトラフィックをブロックします。このアプリケーション認識型ファイアウォールの機能には、次の利点があります。

- アプリケーションの可視性ときめ細かな制御
- 1400 以上のレイヤ 7 アプリケーションの分類
- アプリケーション、カテゴリ、アプリケーションファミリ、またはアプリケーショングループごとのトラフィックの許可またはブロック

アプリケーション認識型ファイアウォールに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

機能名	リリース	機能情報
アプリケーション認識型ゾーンベースFW	Cisco IOS XE Fuji 16.9.1	このドキュメントでは、NBARが検出してゾーンベース ファイアウォール アプリケーションを認識させることができるアプリケーションに基づいて、ゾーンベース ファイアウォール ポリシーを定義する方法について説明します。アプリケーション ファイアウォールは、トラフィックを検査し、アプリケーション、カテゴリ、アプリケーションファミリ、またはアプリケーショングループに基づいてトラフィックをブロックします。 次のコマンドが導入または変更されました： **show class-map***avc-classmap-name* **show policy-map type inspect zone-pair** **show policy-map type inspect zone-pair sessions** **show policy-map type inspect avc** **show platform hardware qfpactive feature firewall drop**

ゾーンベース FW でのアプリケーション認識に関する情報

アプリケーション認識型ファイアウォールの前提条件

- トラフィックがレイヤ3/レイヤ4検査クラスマップと一致していることを確認します。トラフィックがファイアウォール検査に一致しない場合、AVC ポリシーはトラフィックを認識できません。
- AVC サービスポリシーが適用されている同じクラスマップの DNS を検査します。

アプリケーション認識型ゾーンベース FW に関する制約事項

- セルフゾーンへのトラフィックはサポートされません。
- AVC 検査ポリシーは、すべてのアプリケーションを許可し、特定のアプリケーションのみを拒否する必要があります。これは、多くのアプリケーションが相互に依存しているため、あるアプリケーションを許可し、他のすべてのアプリケーションを拒否することは常に機能するわけではないためです。

- 各アプリケーション クラスマップは、最大 16 のフィルタ（各一致がフィルタと見なされます）を持つことができます。
- AVC ポリシーマップは、最大 32 のクラスマップ（class-default を含む）を持つことができます。
- **match protocol attribute category** コマンドを使用してカテゴリを指定する場合は、**match protocol attribute application-family** または **match protocol attribute application-group** を設定できません。

クラスマップやポリシーマップを設定する前に、**parameter-map type inspect** を使用して、ドロップされたパケットをログに記録するようにパラメータマップタイプを設定してください。

```
Device (config)# parameter-map type inspect
Device (config-map)# log dropped-packets
```

ネットワークレイヤ L3/L4 に基づくポリシー

ゾーンベース ファイアウォールは、ネットワークレイヤ L3/L4 に基づくポリシーを使用します。たとえば、クラスマップは、ACL と L4 プロトコル TCP/UDP/ICMP または L7 プロトコル FTP および SIP に基づいています。L7 プロトコルを使用して定義されたポリシーは、プロトコルの宛先ポートを使用してパケットを分類します。ZBF にはアプリケーションの可視性がなく、FTP ALG を介した FTP 検査をサポートし、ポート 21 に基づくプロトコルのみを識別します。

（注） FTP 制御フローがランダムなポートで開かれると、ゾーンベース ファイアウォールはアプリケーションを識別できません。

ZBFW での NBAR ベースアプリケーション認識の設定方法

レイヤ 4 ゾーンベース ファイアウォールの設定

```
Device(config-profile)#class-map type inspect match-any cm1
Device(config-cmap)#match protocol http
Device(config-cmap)#match protocol https
Device(config-cmap)#match protocol dns
Device(config-cmap)#match protocol tcp
Device(config-cmap)#match protocol udp
Device(config-cmap)#match protocol icmp
Device(config-cmap)#exit
Device(config)#class-map match-any nbar-class1
Device(config-cmap)#match protocol yahoo-mail
Device(config-cmap)#match protocol amazon
```

```
Device(config-cmap)#match protocol attribute category consumer-internet
Device(config-cmap)#exit
```

アプリケーション認識型ファイアウォールの L7 サービスポリシー

手順

	コマンドまたはアクション	目的

ステップ 1	検査用のクラスマップを設定します。
	例：
	`class-map type inspect match-any cm1`
	` match protocol http`
	` match protocol https`
	` match protocol dns`
	` match protocol tcp`
	` match protocol udp`
	` match protocol icmp`
		class-map type inspect コマンドと **match protocol** コマンドを使用して、プロトコルとカテゴリを定義します。

ステップ 2	アプリケーション ファイアウォール ポリシーを使用して、アクション（この場合はAVC）を定義します。
	例：
	`policy-map type inspect avc nbar-policy1`
	`class nbar-class1`
	`deny`
	`class class-default`
	`allow`
		deny コマンドを使用して、`nbar-class1` クラスマップにリストされているリモートネットワーク管理プロトコルを拒否します。

ステップ 3	アプリケーション ファイアウォール ポリシーを使用して、ドロップされたパケットをログに記録します。
	例：
	`policy-map type inspect pm1`
	`class type inspect cm1`
	`  inspect`
	`  service-policy avc nbar-policy1`
	`class class-default`
	`  drop log`
	nbar-class1 での Amazon からのトラフィックは、ポリシーによって拒否されます。たとえば、ドロップされたパケットは、次のドロップログメッセージに示されます。
	`Oct 17 12:44:08.101: %IOSXE-6-PLATFORM: R0/0:`
	`cpp_cp:`
	`QFP:0.0 Thread:000 TS:00000002517650404876`
	`%FW-6-DROP_PKT:`
	`Dropping dns/amazon pkt from GigabitEthernet3`
	`171.70.168.183:53 =>`
	`171.10.1.101:50877(target:class)`	

	コマンドまたはアクション	目的
	-(in_to_out:cm1) due to AVC Policy drop:classify result with ip ident 65434	

次のタスク

入力インターフェイスに **ip nbar protocol-discovery ipv4** コマンドを追加します。その後、**show ip nbar protocol-discovery interface** [**intf-name**] コマンドを使用して、アプリケーションの分類を確認します。

例：アプリケーション認識型 show コマンド

この例では、**show policy-map type inspect zone-pair** コマンドにより、ポリシーマップの統計とその他の情報（指定されたゾーンペアに存在するセッションに関する情報など）が表示されます。`Class-map: nbar-class1 (match-any)` に続く行には、トラフィックが nbar-class1 クラスと一致するたびに増加するパケットカウンタ値（`7 packets`）が含まれています。

```
Device# show policy-map type inspect zone-pair

Zone-pair: in_to_out
Service-policy inspect : pm1

Class-map: cm1 (match-any)
Match: protocol http
Match: protocol https
Match: protocol dns
Match: protocol tcp
Match: protocol udp
Match: protocol icmp
Inspect
Packet inspection statistics [process switch:fast switch]
tcp packets: [0:485]
dns packets: [0:51]

Session creations since subsystem startup or last reset 21
Current session counts (estab/half-open/terminating) [13:0:0]
Maxever session counts (estab/half-open/terminating) [13:2:0]
Last session created 00:00:00
Last statistic reset 00:00:19
Last session creation rate 151
Last half-open session total 0

Service-policy inspect avc : nbar-policy1

Class-map: nbar-class1 (match-any)
7 packets, 1449 bytes
30 second offered rate 1000 bps, drop rate 0000 bps
Match: protocol amazon
Match: protocol yahoo-mail
Match: protocol attribute category consumer-internet
Deny

Class-map: class-default (match-any)
211 packets, 94091 bytes
30 second offered rate 27000 bps, drop rate 0000 bps
```

```
Match: any
Allow

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

```
Device# show platform hardware qfp active feature firewall drop
-------------------------------------------------------------------------------
Drop Reason                                                             Packets
-------------------------------------------------------------------------------
AVC Policy drop:classify result                                              38
```

```
Device# show platform hardware qfp active feature firewal datapath scb
[s=session  i=imprecise channel c=control channel  d=data channel A/D=appfw action
allow/deny]
Session ID:0x0000DA5B  171.10.1.101 64204 171.70.168.183 53 proto 17 (0:0) (1456:0xd000208)
 [scA]
Session ID:0x0000DA18  171.10.1.101 58836 74.125.199.103 443 proto 6 (0:0) (1456:0xd000208)
 [sdA]
Session ID:0x0000DA5A  171.10.1.101 64206 8.8.8.8 53 proto 17 (0:0) (0:0xd000001) [sc]
Session ID:0x0000DA11  171.10.1.101 58833 74.125.199.84 443 proto 6 (0:0) (1440:0xd000210)
 [sdA]
Session ID:0x0000DA57  171.10.1.101 64205 173.36.131.10 53 proto 17 (0:0) (1761:0xd00033f)
 [scD]
Session ID:0x0000DA2C  171.10.1.101 58839 74.125.199.94 443 proto 6 (0:0) (1456:0xd000208)
 [sdA]
Session ID:0x0000DA59  171.10.1.101 64203 173.36.131.10 53 proto 17 (0:0) (1761:0xd00033f)
 [scD]
Session ID:0x0000DA0B  171.10.1.101 58831 74.125.199.94 443 proto 6 (0:0) (1456:0xd000208)
 [sdA]
Session ID:0x0000DA5C  171.10.1.101 64207 8.8.4.4 53 proto 17 (0:0) (0:0xd000001) [sc]
Session ID:0x0000DA58  171.10.1.101 64203 171.70.168.183 53 proto 17 (0:0) (1761:0xd00033f)
 [scD]
```

ファイアウォール ステートフル シャーシ間冗長性に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。