Как мы создавали NGFW: межсетевой экран с использованием DPI

Алексей Оладько

История развития межсетевых экранов

- Packet filters
- Stateful firewall

```
iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -p tcp -m multiport --dports 22,53,80,443 -j ACCEPT
iptables -A FORWARD -p udp -m multiport --dports 53,123,138 -j ACCEPT
iptables -A FORWARD -p icmp --icmp-type 8 -j ACCEPT
iptables -A FORWARD -j DROP
```

Настройка межсетевого экрана

- Разрешить пользователям доступ к web
- Разрешить директору все

```
iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -p tcp -m multiport --dports 80,443 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -s 192.168.10.10 -j ACCEPT
iptables -A FORWARD -j DROP
```

Настройка межсетевого экрана

- Разрешить пользователям доступ к web
- **Запретить вконтакте и одноклассники**
- Разрешить директору все

```
iptables -A PREROUTING –t nat –p tcp --dport 80 –j DNAT --to-port 8080

iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -s 192.168.10.10 -j ACCEPT
iptables -A FORWARD -j DROP
```

```
block.acl
    vk\.com
    odnoklassniki\.ru

squid.conf
    acl block dstdomain "/etc/squid/block.acl"
    http_access deny block
```

Настройка межсетевого экрана

- Разрешить пользователям доступ к web
- Запретить вконтакте и одноклассники
- **Разрешить техподдержке TeamViewer**
- **Разрешить отделу продаж Skype for Business**
- Разрешить директору все

TeamViewer's Ports

These are the ports which TeamViewer needs to use:
TCP/UDP Port 5938
TCP Port 443
TCP Port 80

Порты для Skype for Business

Все серверы	Браузер SQL	1434	UDP
Серверы переднего плана	Служба переднего плана Skype для бизнеса Server	5060	TCP
Серверы переднего плана	Служба переднего плана Skype для бизнеса Server	5061	TCP (TLS)
Серверы переднего плана	Служба переднего плана Skype для бизнеса Server	444	HTTPS TCP
Серверы переднего плана	Служба переднего плана Skype для бизнеса Server	135	DCOM и удаленный вызов процедур (RPC)
Серверы переднего плана	Служба конференц-связи с обменом мгновенными сообщениями Skype для бизнеса Server	5062	TCP
Серверы переднего плана	Служба веб-конференций Skype для бизнеса Server	8057	TCP (TLS)
Серверы переднего плана	Служба веб-совместимости конференций Skype для бизнеса Server	8058	TCP (TLS)
Серверы переднего плана	Служба аудио- и видеоконференций Skype для бизнеса Server	5063	TCP
Серверы переднего плана	Служба аудио- и видеоконференций Skype для бизнеса Server	57501-65535	TCP/UDP
Серверы переднего плана	Служба веб-совместимости Skype для бизнеса Server	80	HTTP
Серверы переднего плана	Служба веб-совместимости Skype для бизнеса Server	443	HTTPS

Настройка межсетевого экрана

- Разрешить пользователям доступ к web
- Запретить вконтакте и одноклассники
- **Разрешить отделу продаж Skype for Business**
- **Разрешить техподдержке TeamViewer**
- Разрешить директору все

```
iptables -A FORWARD -j ACCEPT
```

Настройка межсетевого экрана

- Разрешить пользователям доступ к web
- Запретить вконтакте и одноклассники
- **Разрешить отделу продаж Skype for Business**
- **Разрешить техподдержке TeamViewer**
- Разрешить директору все

```
-m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
-dpi-application VK,Odnoklassniki DROP
-dpi-protocol HTTP ACCEPT
-user-group Sales.Dep -dpi-application “Skype for Business” ACCEPT
-user-group Support.Dep –dpi-application TeamViewer ACCEPT
-user Ivanov.A ACCEPT
any to any DROP
```

Deep packet inspection

Deep packet inspection – осуществляет анализ содержимого трафика на 4-7 уровнях модели OSI.

Результат анализа:

- Протокол прикладного уровня. Например, HTTP, Skype
- Приложение. Например, VK, Skype
- Метаданные. Например, поле Host заголовка HTTP

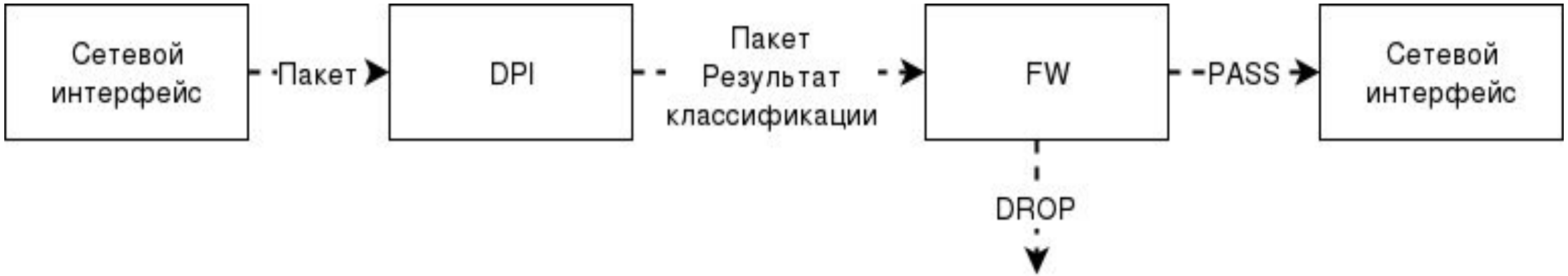
Deep packet inspection

Приложение Skype – бесплатное проприетарное программное обеспечение с закрытым кодом, обеспечивающее текстовую, голосовую и видеосвязь через Интернет.

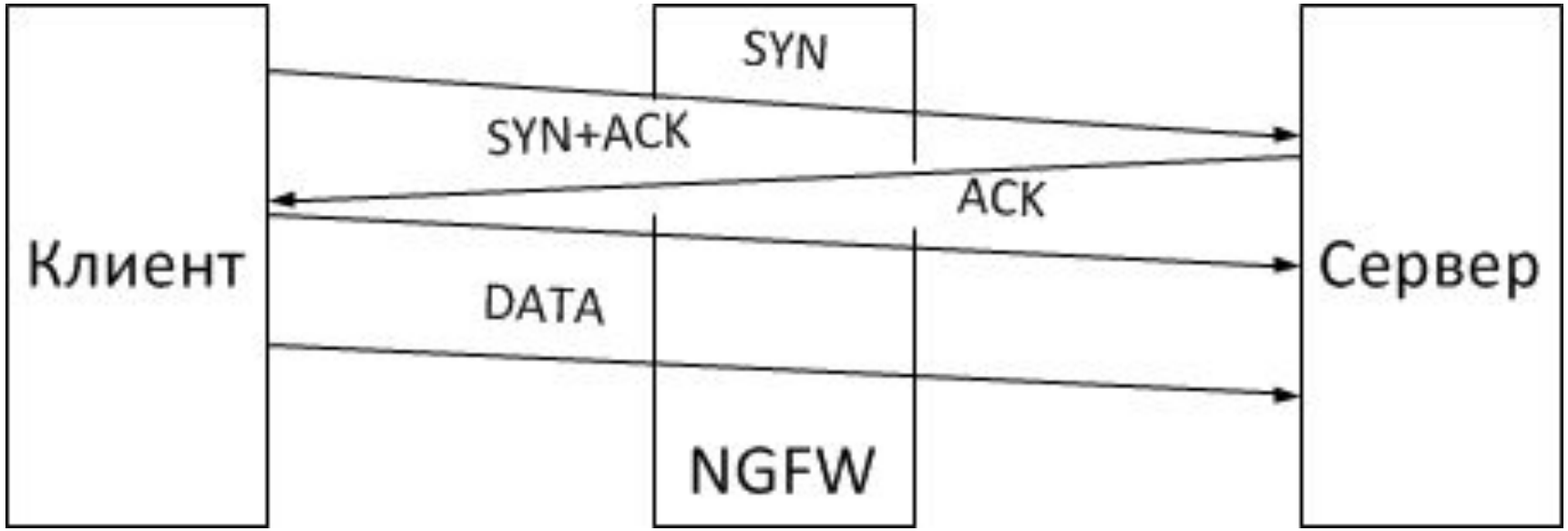
Одно приложение может работать по разным прикладным протоколам:

- Skype
- SSL

Интеграция DPI в межсетевой экран



Проблема: концепция работы протокола TCP



Как устроен DPI

Детекторы

DNS	HTTP	FTP	Skype	SSL	SSH	IMAP	....

Решения детектора:

- EXCLUDE
- MATCH
- NEED NEXT PACKET

Результат классификации:

1. Текущий классифицированный движком протокол.
2. Битовая маска исключенных из классификации протоколов.
3. Флаг окончания классификации сетевого потока (сигнализирует, что данные из пунктов 1 и 2 для данного потока далее изменяться не будут).

Изменена общая структура правил

Было

```
-m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
Список правил
Default rule (PASS/DROP)
```

Стало

1. Если сетевой поток был уже заблокирован, то пакет тоже блокируется.

```
-dpi-drop-mark DROP
```

2. Если сетевой поток ранее был разрешен и результат классификации не был изменен, то пакет пропускается.

```
! -dpi-result-change -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

3. Правила межсетевого экрана. Запрещающие правила ведут устанавливают флаг блокировки в дескрипторе сетевого потока. Правило по умолчанию

```
Список правил
Default rule (PASS/DROP)
```

Правила по классифицированным протоколам

Логика работы разрешающих определенный протокол правил:

1. Если классифицированный движком DPI протокол для текущего пакета совпадает с заданным – применить правило.
2. Если флаг окончания классификации сетевого потока установлен – не применять правило.
3. Если заданный протокол не исключен из классификации – применить правило.
4. Не применять правило.

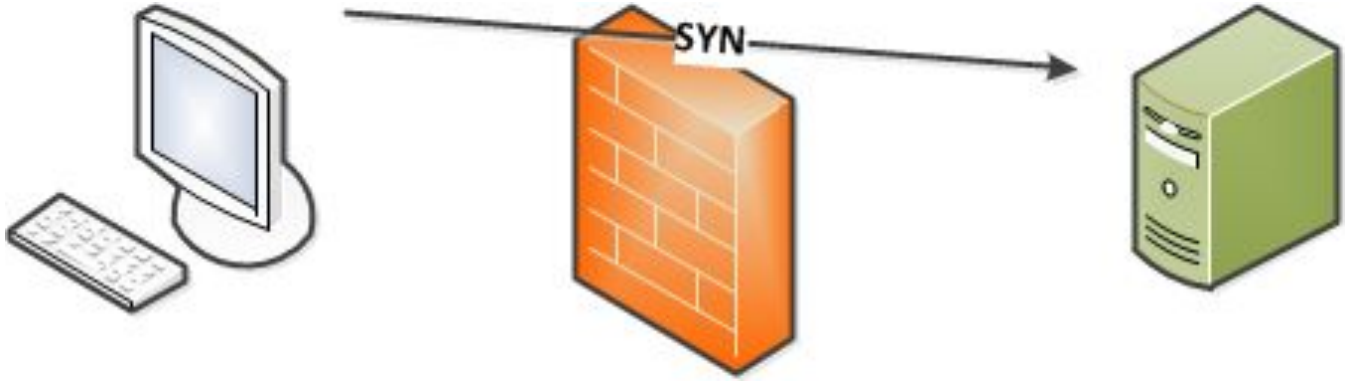
Пошаговая логика работы запрещающих определенный протокол правил:

1. Если классифицированный движком DPI протокол для текущего пакета совпадает с заданным – применить правило.
2. Не применять правило.

Таблица истинности для правил

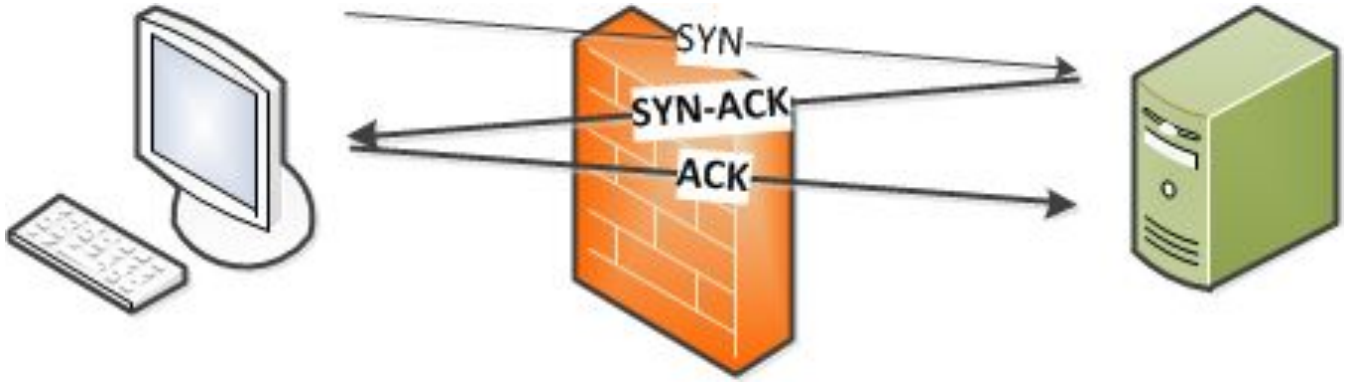
Результат классификации			Цель правила	
Классифицированный протокол совпадает с заданным	Флаг окончания классификации сетевого потока установлен	Протокол не исключен из классификации	ACCEPT	DROP
–	–	+	+	–
–	+	–	–	–
–	+	+	–	–
+	+/–	+/–	+	+

Пример работы разрешающих правил



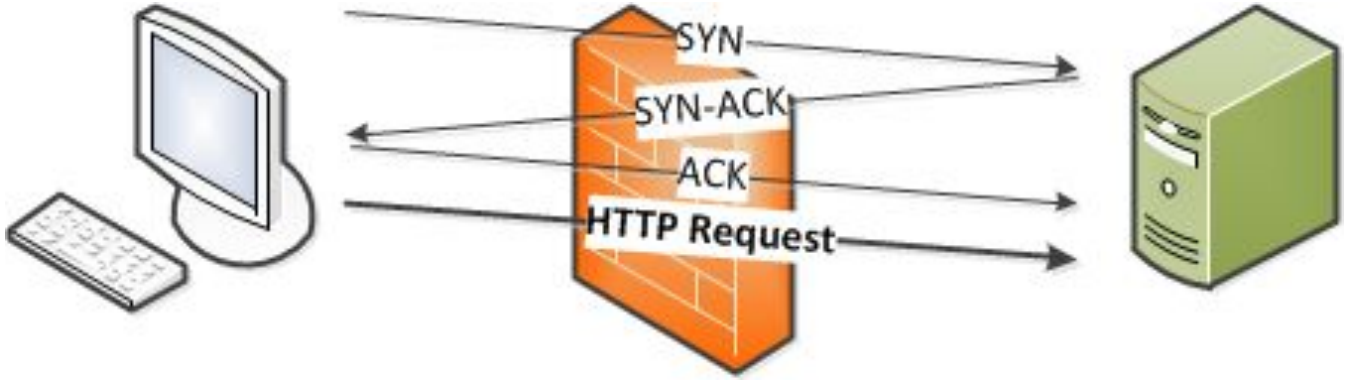

```
-dpi-drop-mark DROP
! -dpi-result-change -m conntrack --ctstate ESTABLISHED -j ACCEPT
-dpi-protocol-accept HTTP –j ACCEPT
Default rule –j DROP
```

Пример работы разрешающих правил



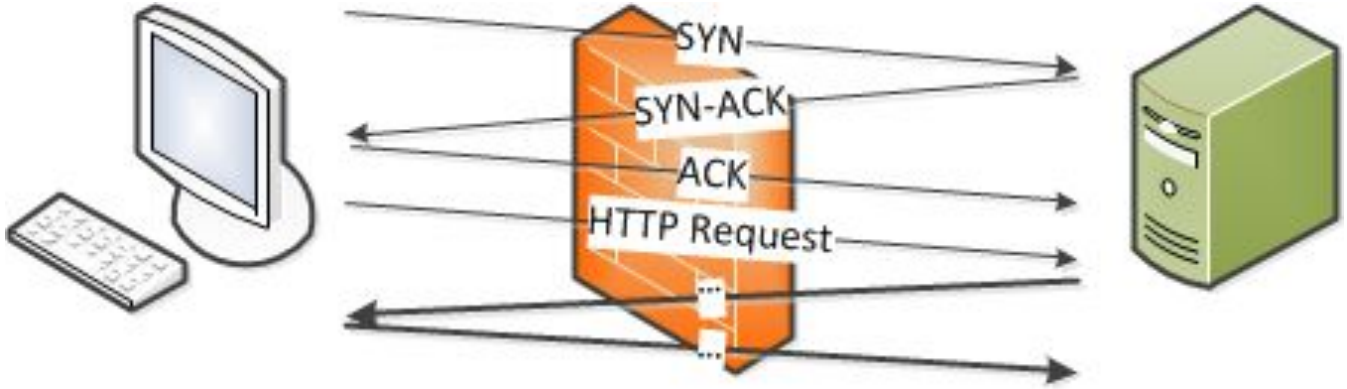

```
-dpi-drop-mark DROP
! -dpi-result-change -m conntrack --ctstate ESTABLISHED -j ACCEPT
-dpi-protocol-accept HTTP –j ACCEPT
Default rule –j DROP
```

Пример работы разрешающих правил



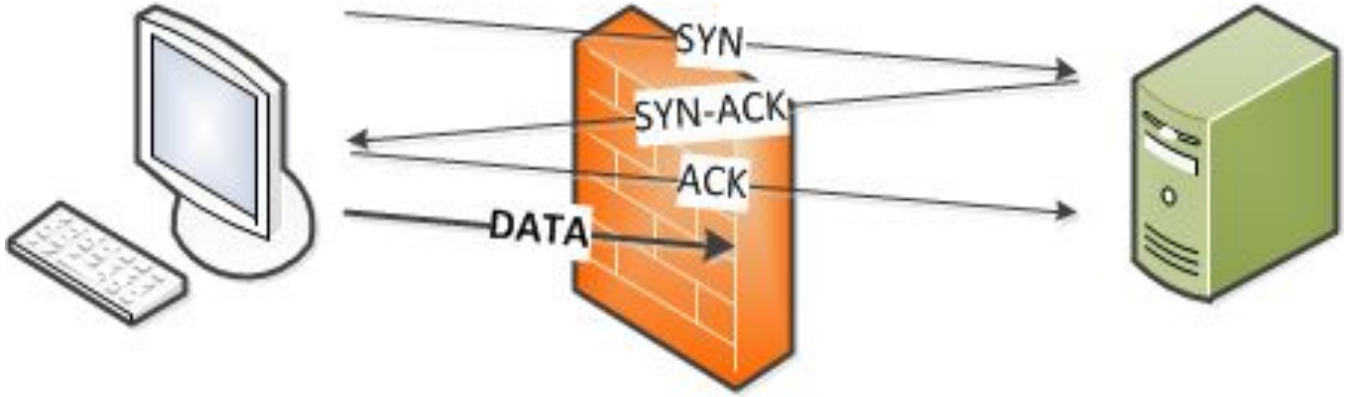

```
-dpi-drop-mark DROP
! -dpi-result-change -m conntrack --ctstate ESTABLISHED -j ACCEPT
-dpi-protocol-accept HTTP –j ACCEPT
Default rule –j DROP
```

Пример работы разрешающих правил



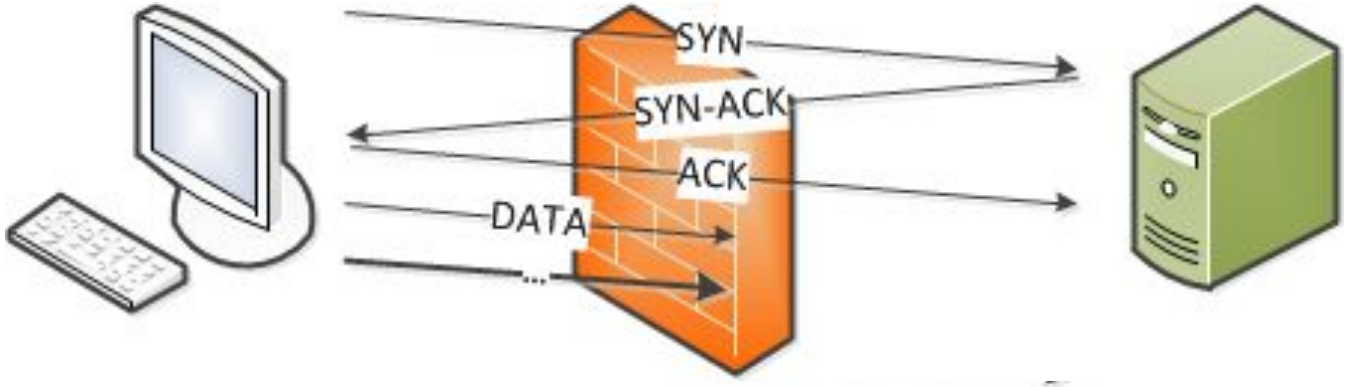

```
-dpi-drop-mark DROP
! -dpi-result-change -m conntrack --ctstate ESTABLISHED -j ACCEPT
-dpi-protocol-accept HTTP –j ACCEPT
Default rule –j DROP
```

Пример работы запрещающих правил




```
-dpi-drop-mark DROP
! -dpi-result-change -m conntrack --ctstate ESTABLISHED -j ACCEPT
-dpi-protocol-accept HTTP –j ACCEPT
Default rule –j DROP
```

Пример работы запрещающих правил




```
-dpi-drop-mark DROP
! -dpi-result-change -m conntrack --ctstate ESTABLISHED -j ACCEPT
-dpi-protocol-accept HTTP –j ACCEPT
Default rule –j DROP
```

Правила по классифицированным приложениям

Для работы правил по классифицированным приложениям необходима следующая информация:

1. Текущее классифицированное движком приложение.
2. Флаг окончательной классификации приложения.

Так как приложение может работать через несколько разных протоколов, то при задании правил по классифицированным приложениям определяется множество родительских протоколов для данного приложения A:[X1, X2, …] и создается несколько правил:

```
-dpi-protocol X1 –dpi-application A  DROP/ACCEPT
-dpi-protocol X2 –dpi-application A  DROP/ACCEPT
```

Правила по классифицированным приложениям

Пошаговая логика работы разрешающих определенное приложение правил:

1. Если классифицированное движком DPI приложение для текущего пакета совпадает с заданным – применить правило.
2. Если флаг окончательной классификации приложения не установлен – применить правило.
3. Не применять правило.

Пошаговая логика работы запрещающих определенное приложение правил:

1. Если классифицированное движком DPI приложение для текущего пакета совпадает с заданным – применить правило.
2. Не применять правило.

Таблица истинности для правил

Результат классификации		Цель правила	
Классифицированное приложение совпадает с заданным	Флаг окончательной классификации приложения установлен	ACCEPT	DROP
-	-	+	-
-	+	-	-
+	-	+	+
+	+	+	+


infotecs
Спасибо