



Cisco Expo
2007

Обнаружение и предотвращение угроз безопасности



Михаил Кадер
Инженер-консультант
security-request@cisco.com

Enable Your Network
Empower Your Business

Обзор

- Структура атаки
- Контроль и обнаружение
- Отражение в проактивном режиме
- Отражение в реактивном режиме

Структура атаки



Знать своего врага: структура атаки



Контроль и обнаружение



Обнаружение

- Работу с макроаналитическими данными можно сравнить с ситуацией с несколькими стогами сена и попыткой определить, в каком из них может находиться иголка
 - NetFlow
 - Статистические данные интерфейса устройства
 - MRTG на основе SNMP
- Работа с микроаналитическими данными сходна с попыткой точного нахождения иголки и всей связанной с ней информации
 - Сигнатуры IPS
 - События CSA
 - Системные журналы
 - PIX/ASA

Макроаналитическая идентификация: NetFlow

```
router#show ip cache flow
IP packet size distribution (126502449 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .009 .622 .036 .007 .008 .008 .004 .012 .000 .000 .004 .001 .002 .002 .007

  512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .001 .190 .012 .065 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  42 active, 65494 inactive, 64005154 added
  187735066 aged polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 402056 bytes
  42 active, 16342 inactive, 3532666 added, 3532666 added to flow
  0 alloc failures, 0 force free
  1 chunk, 10 chunks added
  last clearing of statistics never
```

Protocol	Total	Flows	Packets	Bytes	Packets	Active(Sec)	Idle(Sec)
-----	Flows	/Sec	/Flow	/Pkt	/Sec	/Flow	/Flow
TCP-Telnet	11403610	2.6	1	49	3.0	0.0	1.5
TCP-FTP	6769	0.0	8	53	0.0	6.0	7.7
TCP-FTPD	665	0.0	3334	889	0.5	54.0	0.4
TCP-WWW	163728	0.0	13	750	0.5	4.2	9.2

Макроаналитическая идентификация: статистические данные устройства

```
router#show ip traffic
```

```
IP statistics:
```

```
Rcvd: 89038506 total, 4288288 local destination  
      43999 format errors, 0 checksum errors, 553 bad hop count  
      2 unknown protocol, 929 not a gateway  
      21 security failures, 190123 bad options, 542769 with options  
Opts: 352227 end, 453 nop, 36 basic security, 2 loose source route  
      45 timestamp, 59 extended security, 41 record route  
      53 stream ID, 3 strict source route, 40 alert, 45 cipso, 0 ump  
      361634 other  
Frag: 0 reassembled, 10008 timeouts, 56866 couldn't reassemble  
      0 fragmented, 0 fragments, 0 couldn't fragment  
Bcast: 126217 received, 0 sent  
Mcast: 3110810 received, 4700653 sent  
Sent: 5594057 generated, 84410137 forwarded  
Drop: 4262 encapsulation failed, 0 unresolved, 0 no adjacency  
      352 no route, 43502 unicast RPF, 509 forced drop  
      0 options denied  
Drop: 0 packets with source IP address zero  
Drop: 0 packets with internal loop back IP address
```

```
ICMP statistics:
```

```
Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 9048 unreachable  
      12471 echo, 10 echo reply, 0 mask requests, 0 mask replies, 0 quench  
      0 parameter, 0 timestamp, 0 timestamp replies, 0 info request, 0 other  
      0 irdp solicitations, 0 irdp advertisements  
Sent: 19 redirects, 1023 unreachable, 15 echo, 12471 echo reply  
      0 mask requests, 0 mask replies, 0 quench, 0 timestamp, 0 timestamp replies  
      0 info reply, 562 time exceeded, 115439 parameter problem
```

Микроаналитическая идентификация: IPS

```
evIdsAlert: eventId=1170153876969433741 vendor=Cisco severity=high
originator:
  hostId: ips6x
  appName: sensorApp
  appInstanceId: 22954
time: March 30, 2007 1:53:19 AM UTC offset=-300 timeZone=CDT
signature: description=Cursor/Icon File Format Buffer Overflow id=5442
version=S137
  subsigId: 0
  sigDetails: Malicious ANI File
  marsCategory: Penetrate/BufferOverflow/Misc
interfaceGroup: vs0
vlan: 200
participants:
  attacker:
    addr: 192.168.150.1 locality=OUT
    port: 80
  target:
    addr: 192.168.208.63 locality=OUT
    port: 32951
    os: idSource=unknown type=unknown relevance=unknown
context:
  fromAttacker:
triggerPacket:
  riskRatingValue: 60 targetValueRating=medium
  threatRatingValue: 60
interface: ge0_7
protocol: tcp
```

Системный журнал: атака на интерфейс RPC службы DNS в ОС Microsoft

```
May 16 2007 15:08:47: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35565 to 192.168.2.1/1025 Flags SYN on interface outside
May 16 2007 15:08:47: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35566 to 192.168.2.1/1026 Flags SYN on interface outside
May 16 2007 15:08:47: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35567 to 192.168.2.1/1027 Flags SYN on interface outside
May 16 2007 15:08:47: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35568 to 192.168.2.1/1028 Flags SYN on interface outside
May 16 2007 15:08:47: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35569 to 192.168.2.1/1029 Flags SYN on interface outside
May 16 2007 15:08:47: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35570 to 192.168.2.1/1030 Flags SYN on interface outside
May 16 2007 15:08:47: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35571 to 192.168.2.1/1031 Flags SYN on interface outside
May 16 2007 15:08:47: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35572 to 192.168.2.1/1032 flags SYN on interface outside
May 16 2007 15:08:47: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35573 to 192.168.2.1/1033 flags SYN on interface outside
May 16 2007 15:08:49: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35574 to 192.168.2.1/1033 flags SYN on interface outside
May 16 2007 15:08:49: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35575 to 192.168.2.1/1032 flags SYN on interface outside
May 16 2007 15:08:49: %ASA-2-106001: Inbound TCP connection denied
192.168.208.63/35576 to 192.168.2.1/1031 flags SYN on interface outsided
```

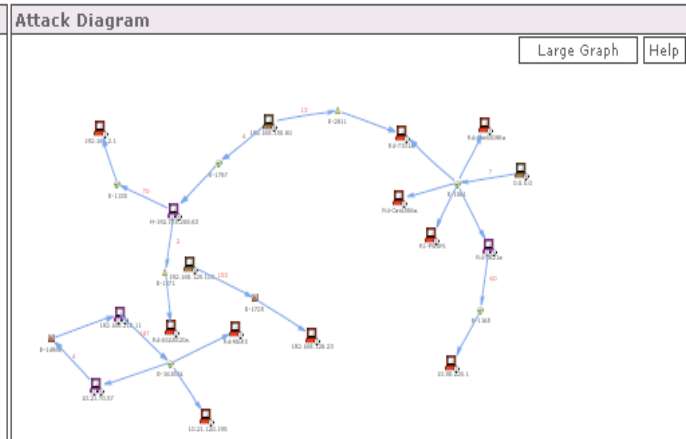
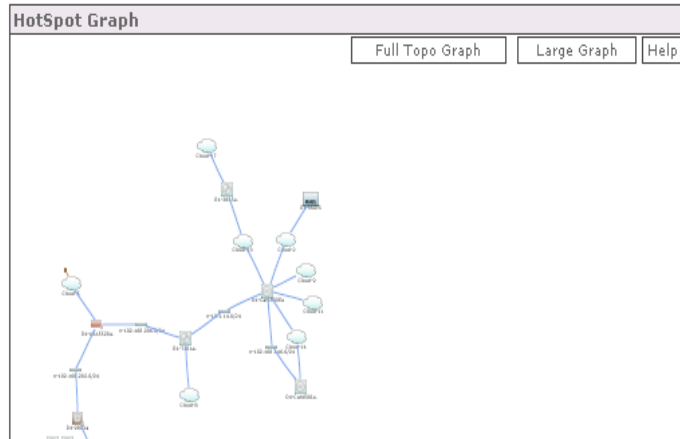
CS-MARS: атака на интерфейс RPC службы DNS в ОС Microsoft

View Cases New Case

Recent Incidents (Last Hour)

All Severities ▼ All Rules ▼ All Case Statuses ▼

Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
I:21075157	TCP High Port Sweep	System Rule: Scans: Stealth, Copied: 07.03.12/23:31:59		May 16, 2007 5:01:28 PM CDT		
I:21075159	TCP High Port Sweep	System Rule: Scans: Stealth, Copied: 07.03.12/23:32:21		May 16, 2007 5:01:28 PM CDT		
I:21075158	TCP High Port Sweep	System Rule: Scans: Stealth		May 16, 2007 5:01:28 PM CDT		
I:21075156	Deny packet due to security policy	System Rule: Network Errors - Likely Routing Related		May 16, 2007 5:01:25 PM CDT		
I:21075155	Inactive CS-MARS reporting device	System Rule: Inactive CS-MARS Reporting Device		May 16, 2007 5:00:04 PM CDT		



Уведомления и предупреждения

- Могут быть предвестниками более серьезных событий. Идентификация этих событий может иметь большое значение для более поздних событий. Уведомления и предупреждения могут присутствовать как в микро-, так и в макроаналитических данных
- В отдельных случаях ранее обнаружение может привести к устранению и сдерживанию будущих атак
- Существует множество форм уведомлений и предупреждений, однако опытный атакующий может изменить способы и временные соотношения, чтобы остаться необнаруженным
- Благодаря знанию собственной сети, использование уведомлений и предупреждений становится более эффективным.

Уведомления и предупреждения: сеть

- Направленное сканирование и зондирование. За счет изменения методик сканирования опытные хакеры могут избежать обнаружения.
- Мониторинг пространства IP-адресов злоумышленников (темного пространства) позволяет не только легко определять попытки проникновения, но и помогает обнаруживать попытки зондирования в результате обычного сетевого сканирования
- Службы, скрывающие адреса источников, такие как web-прокси
- IP-адреса, содержащиеся в черных списках
- Аномалии протоколов

Уведомления и предупреждения: приложения

- Использование протокола, отличного от стандартного протокола HTTP для обычного просмотра сайта.
- Странные схемы web-ссылок, автоматические программы поиска с заданными временными промежутками, необычные значения поля «user agent» в заголовке HTTP, большое количество сообщений HTTP 404, отправка sql команд — все это указывает на сканирование приложения
- Слишком большое количество ошибок при аутентификации, например при подборе пароля SSH
- Спам и фишинг
- В качестве источника подобных сведений можно использовать системные журналы.
Некоторые возможности проведения идентификации предоставляются IPS.

Уведомления и предупреждения: IPS

```
evIdsAlert: eventId=1170160696969433672 severity=informational vendor=Cisco
  originator:
    hostId: ips6x
    appName: sensorApp
    appInstanceId: 587
  time: 2007/05/16 23:56:16 2007/05/16 18:56:16 CDT
  signature: description=Illegal IP Space Monitoring id=60000 version=custom
  subsigId: 0
  sigDetails: Checks for Illegal IP Destination
  marsCategory: info/misc
  interfaceGroup: vs0
  vlan: 144
  participants:
    attacker:
      addr: locality=OUT 192.168.208.63
    target:
      addr: locality=OUT 192.168.249.5
      os: idSource=unknown relevance=relevant type=unknown
  triggerPacket:
<truncated>
  riskRatingValue: attackRelevanceRating=relevant targetValueRating=medium 32
  threatRatingValue: 32
  interface: ge0_7
  protocol: icmp
```

Уведомления и предупреждения: системный журнал

- С помощью таких средств, как `syslog-ng`, можно проводить автоматический анализ данных системных журналов для создания уведомлений и предупреждений
- Для автоматического анализа или разбора данных системных журналов существует несколько средств на основе открытого кода
- Данные системного журнала можно импортировать в систему CS-MARS, после чего из нее могут быть выполнены запросы или правила и соотнесены с другими событиями
- Системный журнал промежуточных устройств (например, устройств маршрутизации, коммутации и контроля доступа) содержит сведения о событиях, происходящих в сети
- Системный журнал конечных устройств содержит реальную информацию о событиях на хосте

Уведомления и предупреждения: системные журналы

```
root@ubuntu:/var/log/apache# more access.log
10.10.2.3 - - [17/May/2007:06:19:46 -0400] "GET / HTTP/1.1" 200 5300 "-"
"Mozilla/4.75 (Nikto/1.36 )" "-"
10.10.2.3 - - [17/May/2007:06:19:46 -0400] "GET /cgi.cgi/ HTTP/1.1" 404 277 "-"
"Mozilla/4.75 (Nikto/1.36 )" "-"
10.10.2.3 - - [17/May/2007:06:19:46 -0400] "HEAD / HTTP/1.1" 200 0 "-"
"Mozilla/4.75 (Nikto/1.36 )" "-"
10.10.2.3 - - [17/May/2007:06:19:46 -0400] "OPTIONS / HTTP/1.0" 200 - "-"
"Mozilla/4.75 (Nikto/1.36 )" "-"
10.10.2.3 - - [17/May/2007:06:19:50 -0400] "TRACE / HTTP/1.0" 200 117 "-"
"Mozilla/4.75 (Nikto/1.36 )" "-"
10.10.2.3 - - [17/May/2007:06:19:50 -0400] "TRACK / HTTP/1.0" 501 315 "-"
"Mozilla/4.75 (Nikto/1.36 )" "-"
```

```
root@ubuntu:/var/log/apache# more error.log
[Wed May 16 02:04:30 2007] [error] [client 10.10.2.3] File does not exist:
/var/www/Nikto-1.36-6iGnKngtBo8ZYOFE0kp.htm
[Wed May 16 02:04:30 2007] [error] [client 10.10.2.3] File does not exist:
/var/www/cgi.cgi/
[Wed May 16 02:04:30 2007] [error] [client 10.10.2.3] File does not exist:
/var/www/webcgi/
[Wed May 16 02:04:30 2007] [error] [client 10.10.2.3] File does not exist:
/var/www/cgi-914/
[Wed May 16 02:04:30 2007] [error] [client 10.10.2.3] File does not exist:
/var/www/cgi-915/
```

Уведомления и предупреждения: CSA

- Правило на основе CS-MARS для доступа к пространству IP-адресов злоумышленников
- Оно может быть распространено на IP-адреса, содержащиеся в черном списке, прокси-серверы, серверы для кэширования web-страниц. Правила CS-MARS не обязательно должны учитывать особенности определенного устройства обнаружения.

The screenshot shows the Cisco MARS web interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. Below the tabs, the current page is 'Inspection Rules' with a sub-tab 'Drop Rules'. The page title is 'CS-MARS Standalone: R4-MARS v4.2'. The user is logged in as 'Administrator (padmin)'. The rule configuration is as follows:

Rule Name:	User Created: Dark Space Scanning	Status:	Active
Action:	None	Time Range:	0h:10m
Description:	This rule detects access to illegal IP address space within the network.		

Offset	Open	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation
1		ANY	192.168.249.0-192.168.252.255	ANY	ANY	ANY	None	ANY	GREEN	1		

The screenshot shows the rule configuration form. The 'Rule Name' field contains 'User Created: Dark Space Scanning'. The 'Rule Description' field contains 'This rule detects access to illegal IP address space within the network.' Below the form are 'Apply' and 'Next' buttons.

Анализ

- Проверка
- Определение степени достоверности обнаружения атаки
- Контекст (среда выполнения)
- Влияние
- Системы IPS и CS-MARS до известной степени определяют уровень достоверности обнаружения атаки, ее контекст и оказываемое ею влияние

Контекст и определение степени достоверности обнаружения атаки

- CS-MARS определяет контекст путем анализа события в контексте политики и других связанных сетевых и системных событий
- В этом случае имеется преимущество в определении конкретного уровня достоверности обнаружения и проверки атаки
- IPS версии 6 определяет контекст атаки с помощью рейтинга релевантности атаки и реакции сети IPS
- IPS определяет степень достоверности обнаружения атаки за счет использования атрибута рейтинга точности сигнатура, назначенного сигнатуре

Рейтинг рисков IPS

$$RR = (ASR * TVR * SFR) / 10000 + ARR - PD + WLR$$

- ASR = Рейтинг серьезности (25,50,75,100)
- SFR = Рейтинг точности (степень точности сигнатуры 55–100)
- TVR = Рейтинг значимости цели (определяется пользователем)
- ARR = Рейтинг релевантности атаки (изучается или определяется пользователем)
- WLR = Рейтинг в списке контроля (при использовании с CSA)
- PD = Разность в режиме promiscuous (при развертывании в режиме promiscuous)

Рейтинг угрозы IPS

- Рейтинг угрозы представляет собой рейтинг риска, который снижен на основании действий при событии, выполненных устройством IPS

- **TR = RR – действие**

Блокирование передачи от атакующего на промежуточном узле – 45,
Блокирование передачи от атакующего к цели на промежуточном узле – 40

Блокирование передачи от атакующего к службе на промежуточном узле – 40

Блокирование соединения на промежуточном узле – 35,
Блокирование передачи пакетов на промежуточном узле – 35

Изменение передачи пакетов – 35

Блокирование запросов от хоста – 20,
Блокирование запросов на соединение – 20

Сброс TCP-соединения – 20, Запрос на ограничение скорости – 20

Рейтинг угрозы IPS: неизвестная цель

```
evIdsAlert: eventId=1170153876969433741 vendor=Cisco severity=high
  originator:
    hostId: ips6x
    appName: sensorApp
    appInstanceId: 22954
    time: March 30, 2007 1:53:19 AM UTC offset=-300 timeZone=CDT
    signature: description=Cursor/Icon File Format Buffer Overflow id=5442
version=S137
  subsigId: 0
  sigDetails: Malicious ANI File
  marsCategory: Penetrate/BufferOverflow/Misc
interfaceGroup: vs0
vlan: 200
participants:
  attacker:
    addr: 192.168.150.1 locality=OUT
    port: 80
  target:
    addr: 192.168.208.63 locality=OUT
    port: 32951
    os: idSource=unknown type=unknown relevance=unknown
context:
  fromAttacker:
  triggerPacket: <truncated>
  riskRatingValue: 60 targetValueRating=medium
  threatRatingValue: 60
interface: ge0_7
protocol: tcp
```

Рейтинг угрозы IPS: цель — Windows

```
evIdsAlert: eventId=1170153876969433784 vendor=Cisco severity=high
  originator:
    hostId: ips6x
    appName: sensorApp
    appInstanceId: 22954
    time: March 30, 2007 04:01:46 AM UTC offset=-300 timeZone=CDT
    signature: description=Cursor/Icon File Format Buffer Overflow id=5442
version=S137
  subsigId: 0
  sigDetails: Malicious ANI File
  marsCategory: Penetrate/BufferOverflow/Misc
interfaceGroup: vs0
vlan: 144
participants:
  attacker:
    addr: 192.168.150.1 locality=OUT
    port: 80
  target:
    addr: 192.168.130.68 locality=OUT
    port: 1117
  os: idSource=learned type=windows-nt-2k-xp relevance=relevant
context:
  fromAttacker:
  triggerPacket: <truncated>
  riskRatingValue: 70 targetValueRating=medium attackRelevanceRating=relevant
  threatRatingValue: 70
interface: ge0_7
protocol: tcp
```

Обзор контекстного анализа CS-MARS

- События — необработанные сообщения, отправленные устройствами формирования отчетов в систему CS-MARS. Примеры: данные системных журналов, SNMP-сообщения, статистика NetFlow и сигнатуры IPS.
- Сеансы — коррелированные события
- Инциденты — сеансы, соответствующие правилам, которые свидетельствуют о неправомерном поведении
- Правила используются для выполнения логического анализа событий, формирующих сеансы и, возможно, инциденты

Правила CS-MARS

- Корреляция событий, происшедших в течение определенного времени, позволит считать их инцидентами

Rule Name: System Rule: Server Attack: Database - Attempt											Status: Active	
Action: None											Time Range: 0h:30m	
Description: This correlation rule detects attacks on a database server, preceded by reconnaissance attempts targeted to that host, if any. The attacks include buffer overflows, denial of service attempts, SQL Injection and other remote command execution attempts using database server privileges.												
Offset	Open (Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count) Close	Operation
1	(ANY	SAME, \$TARGET01, ANY	ANY	Probe/HostInfo/All, Probe/ServerInfo/DB, Penetrate/ViewFiles/HTTPSource, Penetrate/ViewFiles/DB, Penetrate/GuessPassword/DB, Penetrate/ViewFiles/Sensitive, Penetrate/SpoofIdentity/TCP/IP	ANY	None	ANY	ANY	1)	FOLLOWED-BY
2		ANY	SAME, \$TARGET01, ANY	ANY	Penetrate/BufferOverflow/DB, Penetrate/RemoteCmdExec/DB, Penetrate/SQLInjection, DoS/DBServer	ANY	None	ANY	ANY	1)	OR
3		ANY	SAME, \$TARGET01, ANY	ANY	Penetrate/BufferOverflow/DB, Penetrate/RemoteCmdExec/DB, Penetrate/SQLInjection, DoS/DBServer	ANY	None	ANY	ANY	1)	


































































Правила CS-MARS в действии

- Корреляция событий для одних и тех же IP-адресов отправителей и получателей в течение определенного времени позволит считать их инцидентом

Incident ID: 21074995  

Expand All

Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	False Positive
1		WWW dumpenv.pl recon 	92.168.208.63  33152 	192.168.150.1  80 	TCP 	May 16, 2007 12:08:32 PM CDT	R4-IPS4240a		 Total: 2	
1	S:23419542, I:21074995  , I:21074989  , I:21074991  , I:21074994  , I:21074993 	WWW dumpenv.pl recon  	92.168.208.63  33152 	192.168.150.1  80 	TCP 	May 16, 2007 12:08:32 PM CDT	R4-IPS4240a 		 	False Positive
1	S:23419544, I:21074995  , I:21074989  , I:21074991  , I:21074994  , I:21074993 	WWW dumpenv.pl recon  	92.168.208.63  33152 	192.168.150.1  80 	TCP 	May 16, 2007 12:08:32 PM CDT	R4-IPS4240a 		 	False Positive
2		phpBB highlight parameter SQL Injection 	92.168.208.63  33473 	192.168.150.1  80 	TCP 	May 16, 2007 12:08:33 PM CDT	R4-IPS4240a		 Total: 2	
2		Generic SQL Injection in HTTP Request Attempt 	92.168.208.63  34574 	192.168.150.1  80 	TCP 	May 16, 2007 12:08:44 PM CDT	R4-IPS4240a		 Total: 2	
3		phpBB highlight parameter SQL Injection 	92.168.208.63  33473 	192.168.150.1  80 	TCP 	May 16, 2007 12:08:33 PM CDT	R4-IPS4240a		 Total: 2	
3		Generic SQL Injection in HTTP Request Attempt 	92.168.208.63  34574 	192.168.150.1  80 	TCP 	May 16, 2007 12:08:44 PM CDT	R4-IPS4240a		 Total: 2	

Автоматизация

- До устранения угрозы необходимо провести надлежащий анализ идентифицированных данных, чтобы как следует понять события и выполнить автоматическое отражение
- Существует несколько способов, с помощью которых можно получить некоторую степень автоматизации. К ним относятся корреляция на устройстве, корреляция между устройствами, целевой мониторинг известной неправомерной сетевой деятельности, например пространства IP-адресов злоумышленников или honeypot.

Автоматизация

- Взаимодействие IPS / CSA имеет несколько существенных преимуществ.
IPS может автоматически получать информацию о состоянии оконечного устройства, которая используется для вычисления рейтинга угрозы, что обеспечивает более точное ее обнаружение. Неизвестные или зашифрованные эксплойты, которые не удалось определить с помощью IPS, возможно будут обнаружены CSA. CSA-MS может выполнять корреляцию данных и создавать автоматические списки контроля, которые могут быть направлены в IPS, а также автоматически настраивать рейтинг угрозы для событий, определяемых по адресам, которые входят в список контроля.
- CS-MARS может сократить количество событий за счет корреляции и применения известных методов снижения ложных тревог. Передача данных по существу сходна с использованием источника данных и, к сожалению, направленные атаки могут быть не зарегистрированы источником данных, уходя, таким образом от CS-MARS.
- Механизм метасобытий IPS может использоваться на некоторых устройствах для корреляции событий, каждое из которых не является достаточно значимым

Автоматизация взаимодействия CSA/IPS

The screenshot displays two windows from the Cisco Security Agents Management Center. The left window shows a table of events, and the right window shows the configuration for an external product interface.

Events Table:

<input type="checkbox"/> IP Address	Quarantine Time	Source	Events
<input type="checkbox"/> 192.168.124.5	2007-03-29 20:10:55	entered by administrator	
<input type="checkbox"/> 192.168.208.63	2007-05-17 11:42:37	entered by administrator	

Edit External Product Interface Configuration:

- External Product's IP Address: 192.168.130.68
- Enable receipt of information
- Communication Settings:**
 - SDEE URL: /csamc/sdee-server
 - Port: 443
 - Use TLS: Yes
- Login Settings:**
 - Username: secintel
 - Change the password
 - Password: *****
 - Confirm Password: *****
- Watch List Settings:**
 - Enable receipt of watch list
 - Manual Watch List RR increase: 25
 - Session-based Watch List RR Increase: 25
 - Packet-based Watch List RR Increase: 10
- Host Posture Settings:**
 - Enable receipt of host postures
 - Allow unreachable hosts' postures
- Permitted and Denied Host Posture Addresses:**

Name	Active	IP Address	Network Mask	Action
------	--------	------------	--------------	--------

 - Select All
 - Add
 - Edit
 - Move Up
 - Move Down
 - Delete

Buttons: OK, Cancel, Help

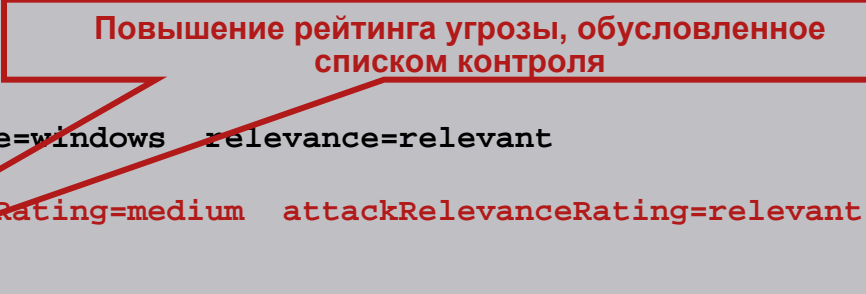
Footer: IDM is initialized successfully.

Автоматизация взаимодействия CSA/IPS

```
evIdsAlert: eventId=1166774738236274233 vendor=Cisco severity=low
originator:
  hostId: ips6x
  appName: sensorApp
  appInstanceId: 388
time: May 17, 2007 5:58:18 PM UTC offset=-300 timeZone=CDT
signature: description=TCP SYN Port Sweep id=3002 version=S2
  subsigId: 0
  marsCategory: Probe/PortSweep/Non-stealth
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: 192.168.208.63 locality=OUT
    port: 57696
  target:
    addr: 192.168.150.60 locality=OUT
    port: 53
    port: 23
    port: 389
    port: 554
    port: 21
    port: 113
  os: idSource=learned type=linux relevance=relevant
triggerPacket: <truncated>
  riskRatingValue: 52 targetValueRating=medium attackRelevanceRating=relevant
  threatRatingValue: 52
interface: ge0_0
protocol: tcp
```

Автоматизация взаимодействия CSA/IPS

```
evIdsAlert: eventId=1166774738236276775 vendor=Cisco severity=low
originator:
  hostId: ips6x
  appName: sensorApp
  appInstanceId: 388
time: May 17, 2007 8:33:28 PM UTC offset=-300 timeZone=CDT
signature: description=TCP SYN Port Sweep id=3002 version=S2
  subsigId: 0
  marsCategory: Probe/PortSweep/Non-stealth
interfaceGroup: vs0
vlan: 0
participants:
  attacker:
    addr: 192.168.208.63 locality=OUT
    port: 55852
  target:
    addr: 192.168.130.68 locality=OUT
    port: 663
    port: 33
    port: 231
    port: 564
    port: 838
    os: idSource=imported type=windows relevance=relevant
triggerPacket: <truncated>
riskRatingValue: 77 targetValueRating=medium attackRelevanceRating=relevant
watchlist=25
threatRatingValue: 77
interface: ge0_0
protocol: tcp
```



Повышение рейтинга угрозы, обусловленное списком контроля

Автоматизация: метасобытия IPS

The image shows two overlapping windows from the Cisco IPS configuration interface. The 'Edit Signature' window (left) displays configuration for signature 62001, 'Targeted HTTP Probing'. The 'Component List' window (right) shows a list of active entries for this signature.

Edit Signature Configuration:

Name	Value
Signature ID	62001
SubSignature ID	0
Alert Severity	Medium
Sig Fidelity Rating	75
Promiscuous Delta	0
Signature Name	Targeted HTTP Probing
Alert Notes	Indicative of targeted HTTP probing
User Comments	None
Alert Traits	0
Release	custom
Engine	Meta
Event Action	Produce Alert
Swap Attacker Victim	No
Meta Reset Interval	3600
Component List	4 (Click to view or edit the details)
Meta Key	Attacker address
Unique Victims	1
Component List in Order	No
Event Counter	
Event Count	1
Event Count Key	Attacker address
Specify Alert Interval	Nn

Component List Configuration:

EntryKey
12682
5474

Legend:

- Parameter uses the Default Value. Click the value field to edit the value.
- Parameter uses a User-Defined Value. Click the icon to restore the default value.

Ограничения метасигнатур

- Метасигнатуры оказывают некоторое влияние на обработку данных сенсором
- Временное ограничение метасигнатур составляет 3600 секунд. Чем больше временной период, тем сильнее влияние.
- В настоящее время метасигнатуры располагают только возможностями логического правила «и», поэтому нельзя создавать правила, на основании которых будет выполняться поиск «всех сигнатур сканирования, за которыми следуют ошибки при аутентификации». Необходимо создавать правила, в которых будут учтены все события.

Расширенная автоматизация

- CS-MARS располагает возможностями логических правил «и», «или» и «за которым следует», а также функцией поиска в строке, поэтому можно создавать более расширенные правила
- Например, с помощью комбинации для поиска HTTP, за которым следует попытка атаки SQL Injection, можно более точно обнаружить попытки зондирования HTTP и атаки SQL Injection независимо от оконечного устройства
- Кроме того, можно создать правило, которое выводило бы оповещение при каждом зондировании, выполняемом с IP-адреса, занесенного в черный список, или если IP-адрес, отсутствующий в черном списке, получает доступ к пространству IP-адресов злоумышленников и также выполняет зондирование

Расширенная автоматизация



SUMMARY INCIDENTS QUERY / REPORTS **RULES** MANAGEMENT ADMIN HELP

Inspection Rules Drop Rules May 17, 2007 11:04:08 PM CDT

RULES | CS-MARS Standalone: R4-MARS v4.2 Login: Administrator (pnadmin) :: [Logout](#) :: [Activate](#)

[View Cases](#) [New Case](#)

Rule Name: **Targeted Web attack** Status: Inactive
Action: None Time Range:
Description: Attack for non standard HTTP methods followed by SQL injection

Offset	Open (Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count) Close	Operation
1		ANY	\$TARGET01	ANY	ApplPolicyViolation/Web	ANY	ANY	ANY	ANY	1		FOLLOWED BY
2		ANY	\$TARGET01	ANY	Penetrate/SQLInjection	ANY	ANY	ANY	ANY	1		

Time Range:

Range: Hrs Mins Secs

Start: 2007 May 17 22 Hrs 54 Mins 8 Secs

End: 2007 May 17 23 Hrs 4 Mins 8 Secs

[Previous](#) [Next](#)

Отражение в проактивном режиме



Предотвращение атак на оконечные устройства с помощью CSA

- Для достижения успеха все атаки следуют определенным поведением, CSA позволяет остановить эти действия с помощью модулей перехвата
- **Неизвестные и целевые атаки**
 - Могут обойти или ликвидировать другие развернутые механизмы защиты
- **Защита от неизвестных атак = возможность остановки распространения вредоносного кода без реконфигурации или обновления**
 - Защита оконечных устройств от риска угрозы, поскольку другие средства защиты могут не работать
- **Ограниченное количество «направлений» атак в системе; все атаки должны использовать одно или несколько поведений**
 - Остановив атаку на одном из этих направлений, вы предотвратите развитие всей атаки (существует не одна, а несколько возможностей)
- **Мониторинг и контроль подобных поведений предотвращают выполнение злонамеренных действий**

Предотвращение выполнения

- Cisco Security Agent (CSA) предоставляет несколько модулей перехвата для обнаружения и предотвращения угроз

Сеть

Файловая система

Конфигурация

Область выполнения

- CSA действует наиболее эффективно для предотвращения атак, направленных на конечные устройства
- Не забывайте о методах защиты, **работающих в сети**



Правила политики определяют модули перехвата

Приложение безопасности	Сеть	Файловая система	Конфигурация	Область выполнения
Распределенный межсетевой экран	✓			
Обнаружение вторжения в хост-машину	✓	✓	✓	
Защита от шпионских и вредоносных программ	✓	✓	✓	
Предотвращение вторжения сетевых червей	✓			✓
Гарантия целостности файла		✓	✓	
Управление политикой безопасности беспроводных сетей	✓		✓	
Маркирование трафика	✓			
Интеграция IPS и NAC	✓			

Атака на интерфейс RPC службы DNS в ОС Microsoft — CSA в действии



Средства обеспечения безопасности приложений предоставляют несколько уровней защиты с использованием политик по умолчанию

#	Date	Host	Severity	Event
3	4/17/2007 10:43:49 PM	w2ksrvsp4	Alert	TESTMODE: The current application 'C:\WINNT\System32\dns.exe' (as user NT AUTHORITY\SYSTEM) attempted to execute the new application 'C:\WINNT\System32\cmd.exe'. The operation would have been denied. Details Rule 461 Wizard Find Similar
2	4/17/2007 10:43:49 PM	w2ksrvsp4	Notice	TESTMODE: The process 'C:\WINNT\System32\dns.exe' (as user NT AUTHORITY\SYSTEM) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINNT\System32\dns.exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' Details Rule 186 Wizard Find Similar
1	4/17/2007 10:43:46 PM	w2ksrvsp4	Alert	TESTMODE: The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to accept a connection as a server on TCP port 139 from 192.168.58.134 using interface Wired\AMD PCNET Family PCI Ethernet Adapter. The operation would have been denied. Details Rule 59 Wizard Find Similar

Защита от атак с подменой адресов

- RFC3704/BCP84 = пакеты должны отправляться из действительного, назначенного адресного пространства
- Что происходит при **использовании** BCP84
 - Упреждающее предотвращение атак, направленных на подмену адресов
 - Помощь в системной диагностике за счет проверки источника
 - Работа в Интернете за счет средств защиты от атак с подменой адресов
- Что происходит, если BCP84 **не используется**
 - Устройства могут намеренно или непреднамеренно отправлять трафик с подмененными исходными адресами
 - Сложности в отслеживании источников отправки вредоносного трафика
 - Отправка вредоносного трафика связана с расходом ресурсов
 - Атаки с подменой адресов являются более опасными

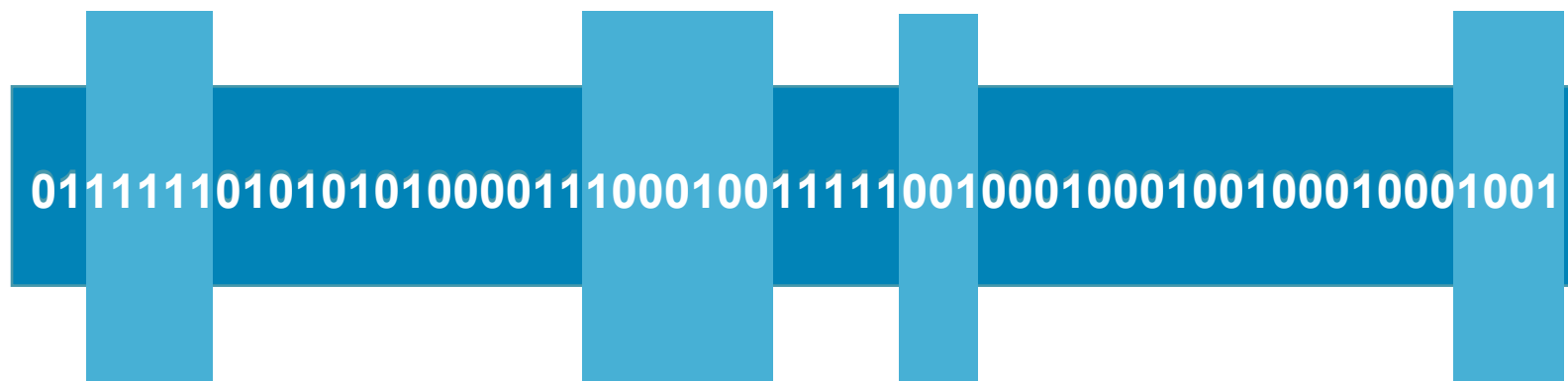
Способы защиты от атак с подменой адресов

- Осуществить защиту как можно ближе к цели, устранить угрозу как можно ближе к атакующему
- Выполнить как можно более точную фильтрацию
 - Источник и получатель (уровень 3 и уровень 4)
- Существует несколько возможностей
 - Списки контроля доступа (ACL)
 - Механизм Unicast RPF
 - IP Source Guard (IPSG)
 - Отслеживание и перехват DHCP Snooping

Отражение в реактивном режиме



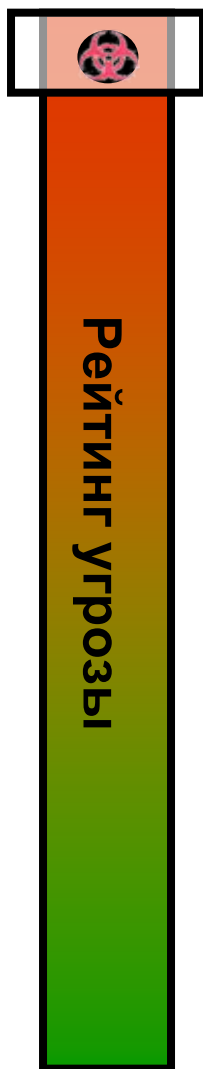
Защита от вторжений в сеть



- Обнаружение вредоносных данных, выполнение анализа на поведенческом уровне, обнаружение аномалий, настройки политик и использование методов быстрого реагирования на угрозы
- Режим работы «в линии передачи данных» или режим promiscuous
- Система автоматического предотвращения угроз в IPS 6.x блокирует пакеты с диапазоном **номинального значения** 90 – 100
- Мультивекторная защита во всех точках сети, настольных систем и серверных оконечных устройств

Интеграция с Cisco CSA и контроллером беспроводных сетей Cisco

IPS: Пороговые значения рисков управляют отражением атаки



- Серьезность события
- Точность сигнатуры
- Релевантность атаки
- Ценность активов объекта

+
+
+

Насколько актуальна угроза?

Насколько вероятна ошибка?

Релевантна ли атака для атакуемого хоста?

Насколько важен хост назначения?

= рейтинг риска

Управление политикой отражения угрозы

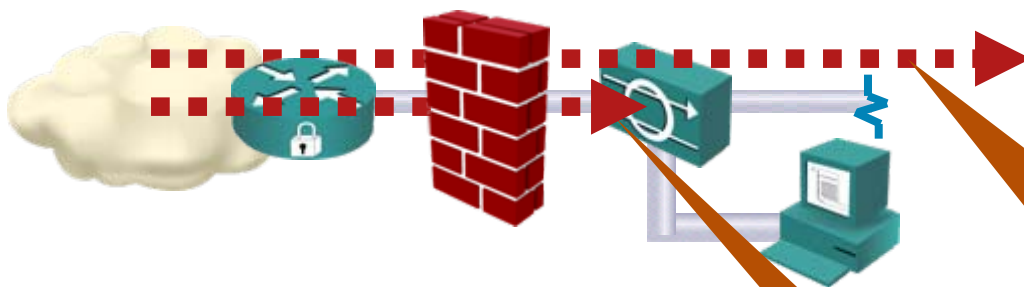


Customizable Risk Rating Thresholds :	
0 < RR < 35	Alarm
35 < RR < 85	Alarm & Log Packets
85 < RR < 100	Drop Packet

Результат: взвешенный рейтинг риска позволяет осуществлять масштабируемое управление эффективными технологиями предотвращения угроз

IPS - Рейтинг угрозы:

оценка серьезности инцидента после применения политики



Рейтинг угрозы

- Динамическая настройка рейтинга риска события на основе успешного выполнения ответного действия
- Если было применено ответное действие, то рейтинг риска уменьшается ($TR < RR$)
- Если ответное действие применено не было, то рейтинг риска не изменяется ($TR = RR$)

Преимущество

- Назначение приоритетов уведомлениям для привлечения внимания оператора
- Оператор может сконцентрировать ответные действия при инциденте на тех угрозах, которые не были отражены

Атака 1:

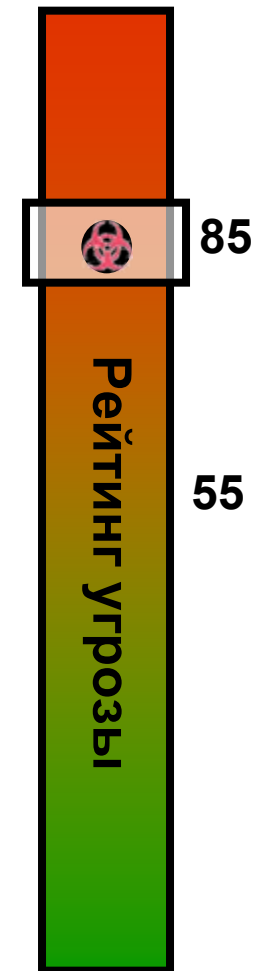
Не настроено никаких действий
Рейтинг риска = 85

Рейтинг угрозы = 85

Атака 2:

Настроенные действия
Отраженные атаки
Рейтинг риска = 85

Рейтинг угрозы = 55



IPS: Что делать — запретить, заблокировать или сбросить?

- Запрет на передачу трафика осуществляется с использованием устройств, инспектирующих потоки
 - Определение вредоносного или несанкционированного трафика и его отклонение
 - Знание состояния трафика для протоколов на основе соединения
- Блокировка трафика осуществляется с помощью вспомогательного устройства
 - Позволяет устранять угрозу ближе к злоумышленнику
 - Возможное возникновение DoS, блокирование разрешенного трафика
- Отправление TCP RST для потоков трафика на основе соединений
 - Ограничение области действия протокола и добавление пакетов RST в сеть
 - В зависимости от структуры IPS существует возможность устранения угрозы ближе к объекту воздействия

IOS: Расширенные списки контроля доступа

Кадр	Заголовок уровня 2	Заголовок уровня 3	Заголовок уровня 4	Первый...Второй...	Область данных...Область данных...Область данных...	Кадр
------	--------------------	--------------------	--------------------	--------------------	-----------------------------------------------------	------

- Flexible Packet Matching (FPM) выполняет глубокую инспекцию пакетов для сдерживания распространения угроз и соблюдения политики
 - Сопоставление полей заголовков протоколов и/или контекста области данных
 - Уровень со 2 по 7 – возможность сопоставления с любым битом/байтом в пакете
- Политики фильтрации, определенные пользователем (классификаторы трафика)
 - Возможность выбора ответных действий
- Адаптация к динамически изменяющимся профилям атак
 - Быстрое распространение политик фильтрации (для ответных действий на угрозы в режиме почти реального времени можно использовать EEM)
- Возможность развертывания механизмов защиты и предотвращения ближе к объекту воздействия и злоумышленнику

IOS: Определение политики FPM

1: Создание стека протоколов

2: Создание фильтра FPM

3: Создание политики FPM

4: Создание вложенной политики FPM

5: Вложение политики FPM

IOS: Политика FPM для червя Slammer

```
load protocol disk0:ip.phdf
load protocol disk0:udp.phdf
!
class-map type stack match-all ip_udp_class
  description "match UDP over IP packets"
  match field ip protocol eq 17 next udp
1
class-map type access-control match-all slammer_class
  description "match on slammer packets"
  match field udp dest-port eq 1434
  match field ip length eq 404
  match start udp payload-start offset 196 size 4 eq 0x4011010
!
policy-map type access-control fpm_udp_policy
  description "policy for UDP based attacks"
  class slammer_class
    drop
    log
!
policy-map type access-control fpm_policy
  description "drop worms and malicious attacks"
  class ip_udp_class
    service-policy fpm_udp_policy
!
interface gigabitEthernet 0/1
  service-policy type access-control input fpm_policy
```

IOS: PHDF – файл определения заголовка протокола

<http://www.cisco.com/cgi-bin/tablebuild.pl/fpm>

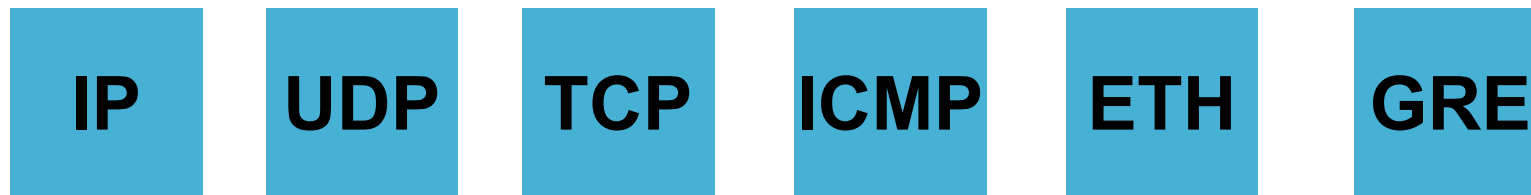
```
<?xml version="1.0" encoding="UTF-8"?>
<phdf>
  <version>1</version>
  <protocol name="ip" description="IP-Protocol">
    <field name="version" description="IP-Version">
      <offset type="fixed-offset" units="bits"> 0 </offset>
      <length type="fixed" units="bits">4</length>
    </field>
    --- TRUNCATED OUTPUT ---
    <field name="dest-addr" description="IP-Destination-Address">
      <offset type="fixed-offset" units="bytes">16</offset>
      <length type="fixed" units="bytes">4</length>
    </field>
    <field name="payload-start" description="IP-Payload-Start">
      <offset type="fixed-offset" units="bytes">20</offset>
      <length type="fixed" units="bytes">0</length>
    </field>
    <headerlength type="fixed" value="20"></headerlength>
    <constraint field="version" value="4" operator="eq"></constraint>
    <constraint field="ihl" value="5" operator="eq"></constraint>
  </protocol>
</phdf>
```

IOS: TCDF – файл определения классификации трафика

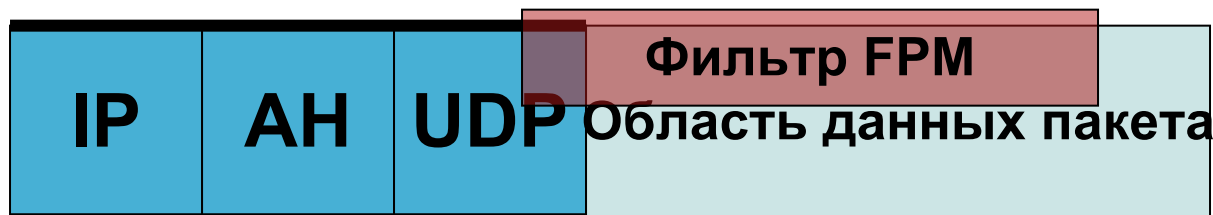
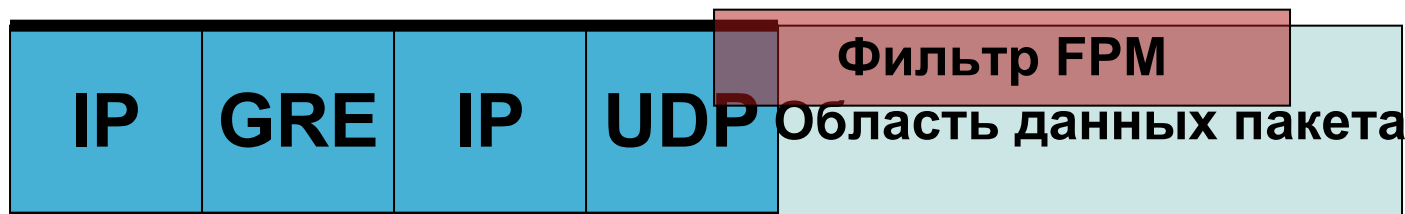
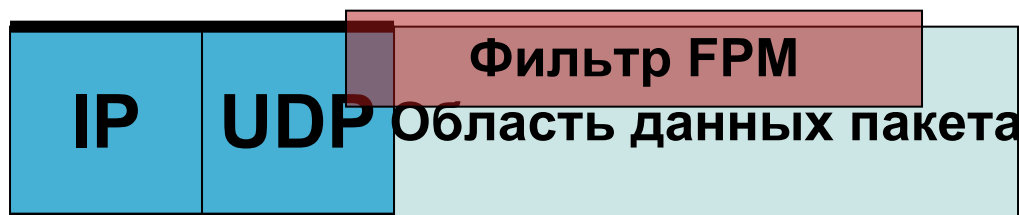
<http://www.cisco.com/cgi-bin/tablebuild.pl/fpm> – 12.4(6)T

```
<?xml version="1.0" encoding="UTF-8"?>
<tcdf>
  <class name="ip_udp_stack" type="stack">
    <match>
      <eq field="ip.protocol" value="0x11" next="udp"></eq>
    </match>
  </class>
  <policy type="access-control" name = "udp_policy" >
  </policy>
  <policy type = "access-control" name = "fpm_policy_template">
    <class name = "ip_udp_stack"></class>
    <action>service-policy udp_policy</action>
  </policy>
</tcdf>
```

IOS: Гибкость стека



Один и тот же фильтр FPM можно применить к нескольким стекам протоколов



IOS: Политика FPM для IP-инкапсулированного червя Slammer

```
load protocol disk0:ip.phdf
load protocol disk0:udp.phdf
!
class-map type stack match-all ip_ip_udp_class
  description "match UDP over IP packets in a IP tunnel"
  match field layer 2 ip protocol eq 4 next ip
  match field [layer 1] ip protocol eq 17 next udp
!
class-map type access-control match-all slammer_class
  description "match on slammer packets"
  match field udp dest-port eq 1434
  match field [layer 1] ip length eq 404
  match start udp payload-start offset 196 size 4 eq 0x4011010
  match start udp payload-start offset 128 size 8 string "X.Y*#1.2"
!
policy-map type access-control fpm_udp_policy
  description "policy for UDP based attacks"
  class slammer_class
    drop
    log
!
policy-map type access-control fpm_policy
  description "drop worms and malicious attacks"
  class ip_udp_class
    service-policy fpm_udp_policy
!
interface GigabitEthernet 0/1
  service-policy type access-control input fpm_policy
```

IOS: FPM – Мониторинг

- Отображение всех или назначенных карт класса FPM

```
router# show class-map type [stack | access-control] [<name>]
```

- Отображение всех или назначенных карт политик FPM

```
router# show policy-map type access-control [<name>]
```

- Отображение карт политик FPM в назначенном интерфейсе. Отображение количества совпавших пакетов

```
router# show policy-map type access-control interface <interface>
```

или

```
router# show policy-map type access-control control-plane <>
```

- Отображение сведений о времени выполнения для загруженных классов и политик FPM

```
router# show protocols phdf <loaded-protocol>
```

- Отображение листинга определенных пользователем файлов PHDF, хранящихся локально на маршрутизаторе

```
router# dir disk0:*.phdf
```

- Отслеживание всех событий FPM на плоскости управления и плоскости данных

```
router# debug fpm event
```

IOS: Производительность FPM и эквивалентные ACL

- Сравнение FPM с ACL (процентное отношение использования)
- Десять классов FPM или эквивалентный ACL
- Совпадение в src/dst ip addr, src/dst tcp port и протоколе tcp
- Десять потоков трафика TCP, совпадение 50% сгенерированного трафика
- 7206VXR NPE-400, 128 Мбайт, 12.4(4)T

Тип фильтра	1 000 пакетов в секунду	2 000 пакетов в секунду	3 000 пакетов в секунду	4 000 пакетов в секунду	5 000 пакетов в секунду
Фильтр отсутствует	13%	14%	15%	16%	17%
Первое сопоставление FPM	38%	42%	43%	43%	43%
Первое сопоставление ACL	30%	36%	37%	37%	37%
Пятое сопоставление FPM	42%	50%	59%	59%	59%
Пятое сопоставление ACL	32%	39%	40%	41%	41%
Десятое сопоставление FPM	42%	50%	50%	50%	50%
Десятое сопоставление ACL	32%	39%	39%	39%	39%

IOS: Этапы и возможности FPM

Функциональность	ACL	FPM Этап 1 12.4(4)T	FPM Этап 1+ 12.4(6)T1	FPM Этап 2	FPM Этап 3
Количество ACE на каждый интерфейс	Неограничено	32 класса	32 класса	Неограничено	Неограничено
Количество критериев сопоставления/ACE	4	8	8	Неограничено	Неограничено
Глубина инспекции	44 байта	256 байт	256 байт	Полный пакет	Поток
Грубое смещение	Нет	Да	Да	Да	Да
Относительное смещение (Поддержка фиксированной длины заголовка)	Нет	Да	Да	Да	Да
Динамическое смещение (Поддержка переменной длины заголовка)	Нет	Нет	Нет	Да	Да
Совпадение в данных TLV полей	Нет	Нет	Нет	Нет	Да
Вложенные политики	Нет	Да	Да	Да	Да
Вложенные карты классов	Нет	Нет	Нет	Да	Да
Поиск с использованием регулярного выражения	Нет	Да	Да	Да	Да
Поиск по строке	Нет	Нет	Да	Да	Да
Окно шаблона строки для поиска	Нет	32 байта	32 байта	Полный пакет	Полный пакет
Поддерживаемые протоколы	IPv4, TCP, UDP, ICMP	IPv4, TCP, UDP, ICMP, Ethernet	Этап 1	Этап 1+ + GRE, IPSec	Этап 2 + DNS, SNMP, HTTP, IPv6

IOS: Этапы и возможности FPM (продолжение)

Функциональность	ACL	FPM Этап 1 12.4(T)T	FPM Этап 1+ 12.4(6)T1	FPM Этап 2	FPM Этап 3
Поддерживаемые действия	Разрешение, Запрет, Регистрация в журнале	Разрешение, подсчет, удаление, регистрация в журнале, отправка-ответ, вложенная политика	Этап 1	Этап 1+ + переадресация, ограничение скорости	Этап 2
Поддерживаемые операции	eq, neq	eq, neq, gt, lt, range, regex, логика И ИЛИ	Этап 1 + строка	Этап 1+	Этап 2
Поиск во фрагментах	Нет	Нет	Нет	Да	Да
Поиск в пакетах потока	Нет	Нет	Нет	Нет	Да

PIX/ASA:

Среда модульных политик (MPF)

- MPF предоставляет возможность определения конкретной политики или набора политик для классификации трафика для расширенной проверки
- MPF построен на основе трех связанных команд CLI:

Карта класса (Class-map) - идентификация трафика, для которого требуется определенный тип контроля; карты классов имеют определенные имена, связывающие их в карту политики

Карта политики (Policy-map) - описание действий, применяемых к трафику, описанному в карте класса; карты политик также имеют определенные имена, связывающие их в политику услуг

Политика услуг (Service-policy) - описание места контроля трафика; для каждого интерфейса может существовать только одна политика услуг; для трафика и приложения глобальной политики определена дополнительная политика услуг, называемая «глобальной политикой услуг», она применяется к трафику на всех интерфейсах

ASA: Точный контроль действий приложений

- В данном примере политика разрешает только команды FTP «**GET**» и отправляет TCP RST для команд, указанных в списке «**match request-command**»

```
class-map type inspect ftp match-all ftp-class-inspect
  match request-command appe cdup dele help mkd put rmd rnfr rnto site stou
!
policy-map type inspect ftp ftp-app-inspect
  class ftp-class-inspect
    reset
!
policy-map global_policy
  class inspection_default
    inspect ftp strict ftp-app-inspect
!
service-policy global_policy global
!
```

ASA: В версию 7.2 включен механизм поиска с использованием регулярных выражений

- Поиск с использованием регулярных выражений обеспечивает значительную гибкость при контроле работы приложений
- Регулярное выражение представляет собой строку символов, описывающую искомый текст, и имеет определенный синтаксис
- Можно выполнять поиск совпадений по имени файла, его содержимому, строке или любой их комбинаций
- В средствах межсетевой защиты PIX/ASA включен мастер регулярных выражений, содержащий полезное средство тестирования
- Дополнительные сведения о регулярных выражениях см. по адресу <http://en.wikipedia.org/wiki/Regex>

ASA:

Сокращения регулярных выражений

Для удобства используется ряд общих сокращений. Типичные примеры:

<u>Сокращение</u>	<u>Значение</u>	<u>Примечания</u>
r+	(rr*)	1 или более вхождений
r?	(r ε)	0 или 1 вхождение
[a-z]	(a b ... z)	1 символ в заданном диапазоне
[^a-z]	^(a b ... z)	1 символ, НЕ содержащийся в заданном диапазоне
[abxyz]	(a b x y z)	1 из заданных символов
^	Точка привязки	Привязывает соответствие к началу строки

ASA:

Пример регулярного выражения

Требование: Совпадение в любых сообщениях HTTP GET или POST:

```
asa(config)# regex test_get "get"
```

```
asa(config)# regex test_post "post"
```

- Совпадение только с GET и POST, которые были введены в нижнем регистре
- Оптимальное регулярное выражение для поиска совпадений при комбинации регистров:

```
asa(config)# regex test_get "[Gg][Ee][Tt]"
```

```
asa(config)# regex test_post "[Pp][Oo][Ss][Tt]"
```

- Для проверки синтаксиса строки регулярного выражения следует использовать либо команду CLI **test regex <reg exp>**, либо мастер ASDM Regex Wizard

ASA:

Развитие процессов контроля HTTP

- До выхода версии 7.0 контроль HTTP ограничивался простой регистрацией запросов GET URL-адресов при условии надлежащего определения уровней регистрации.
- В версии 7.0 представлено несколько новых возможностей контроля HTTP:

команда `http-map` для улучшенного контроля

разрешение/запрет определенных методов HTTP и
разрешение/запрет определенных расширений HTTP

настройка максимального размера заголовка HTTP и URI

разрешение/запрет подмножества
определенных типов MIME

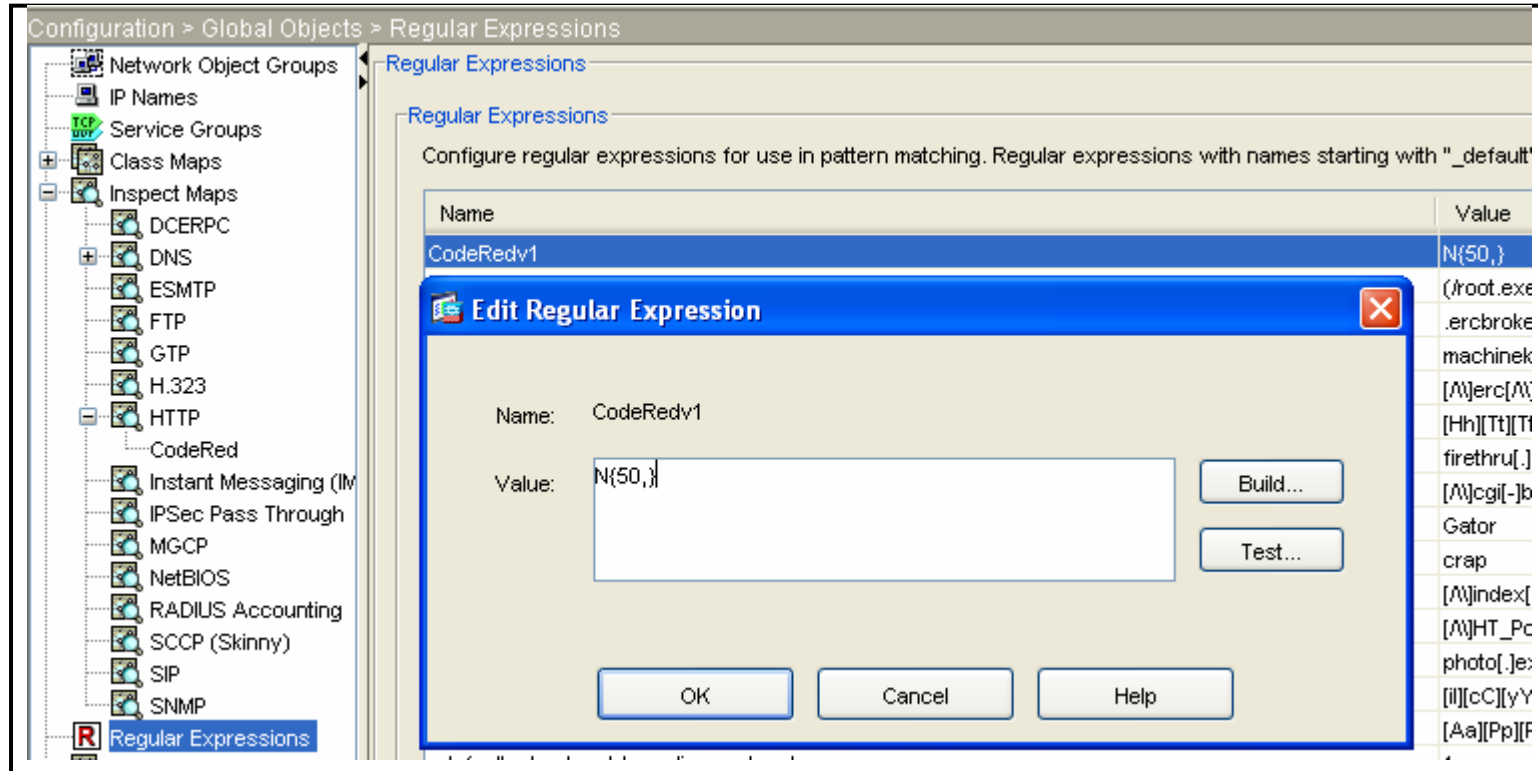
настройка максимального и минимального
размера тела HTTP

ASA:

Развитие процессов контроля HTTP

- Политики контроля по умолчанию для протоколов IM, P2P и протоколов туннелирования (использование **show run all** для отображения в конфигурации)
- В версии 7.2 добавлены дополнительные возможности контроля (неполный список):
 - разрешение/запрет передачи пакетов с заголовками, содержащими несколько типов содержимого
 - выборочный контроль протоколов внутри HTTP
 - разрешение/запрет нулевого кодирования HTTP
 - разрешение/запрет заголовков запросов, параметров форм, заголовков ответов, не соответствующих ASCII
 - Маскирование баннера сервера HTTP
 - Java, ActiveX и другие возможности фильтрации апплетов/скриптов для улучшения действия существующих команд фильтра

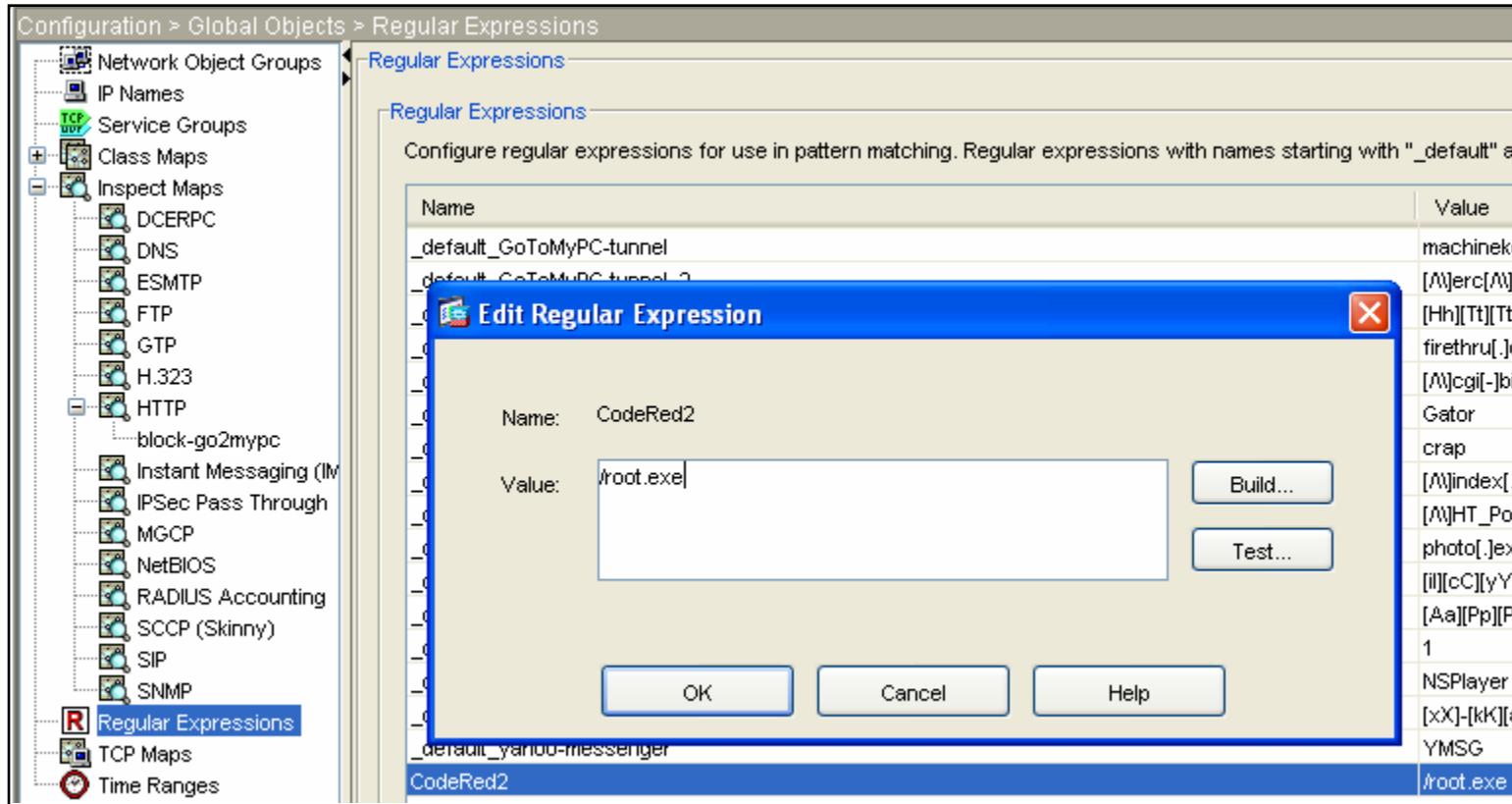
ASA: Регулярное выражение для поиска Code Red v1



```
asa(config)# regex CodeRed1 "N{50,}"
```

По этой строке выполняется поиск минимум 50 вхождений буквы «N», являющейся показателем деятельности хоста, зараженного червем CodeRed

ASA: Регулярное выражение для поиска Code Red II



asa(config)# regex CodeRed2 "/root.exe"

ASA: Фильтрация URI Code Red I и II

CodeRed

Edit the basic settings for the HTTP map in the Basic View. Make advanced changes for the HTTP map in the Advanced View.

Name: CodeRed

Description:

URI Filtering

Match Type	Criterion	Value	Action	Log
	Request URI	CodeRedClass	Drop Connection	Yes

Edit HTTP Inspect

Match Criteria

Match Type: Match No Match

Criterion: Request URI

Value

Regular Expression: CodeRedv1

Regular Expression Class: CodeRedClass

Actions

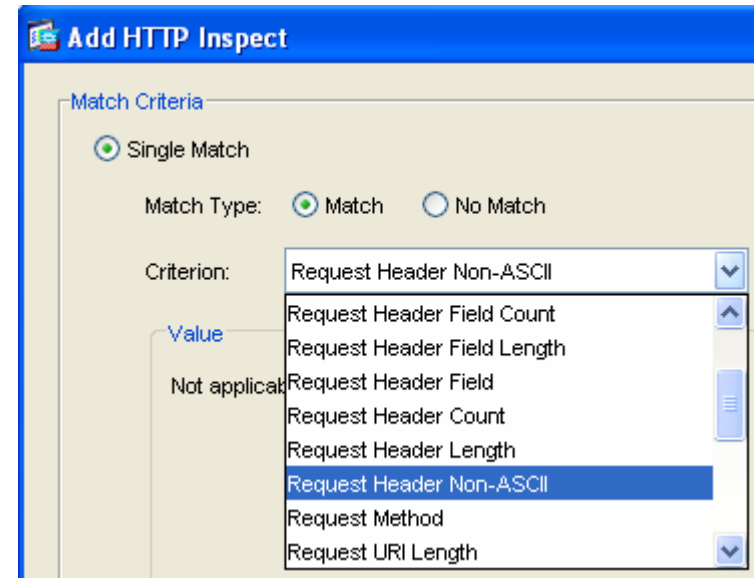
Action: Drop Connection Reset Log

Log: Enable Disable

Match Type:

ASA: Вредоносные программы продолжают распространяться: Nimda

- 18 сентября 2001 года: за 24 часа заражено более 1 миллиона хостов
- Мультивекторный червь ищет любые уязвимости MSFT (MIME, HTTP и т. д.)



Обход каталогов IIS с использованием Unicode:

```
GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
```

```
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
```

- Отражение на межсетевом экране за счет блокирования любого запроса HTTP, содержащего заголовки, не соответствующие ASCII

```
asa(config)# match request header non-ascii  
drop-connection log
```

ASA: Дамп трафика на межсетевом экране для профилирования приложения

```
access-list HOSTCHECK extended permit ip host 192.168.1.201 any
access-list HOSTCHECK extended permit ip any host 192.168.1.201

asa>#capture CAP-HOST access-list HOSTCHECK interface inside

asa>#sh capture CAP-HOST
26 packets captured
...
11: 192.168.1.201.1935 > 66.151.158.177.80: S
    4141954911:4141954911(0) win 64240 <mss 1460,nop,nop,sackOK>
12: 192.168.1.201.1936 > 66.151.158.177.8200: S
    999298953:999298953(0) win 64240 <mss 1460,nop,nop,sackOK>
13: 192.168.1.201.1937 > 66.151.158.177.443: S
    2462372042:2462372042(0) win 64240 <mss 1460,nop,nop,sackOK>
14: 66.151.158.177.80 > 192.168.1.201.1935: S
    2862815220:2862815220(0) ack 4141954912 win 8190 <mss 1380>
15: 192.168.1.201.1935 > 66.151.158.177.80: . ack 2862815221 win
    64860
16: 192.168.1.201.1935 > 66.151.158.177.80: P
    4141954912:4141954975(63) ack 2862815221 win 64860
...
HTTP GET с web-узла
```

SYN - на порт 80

SYN - на порт 8200

SYN - на порт 443

SYN-ACK от порта 80

(подтверждение установления трехстороннего соединения)

ASA: Использование дампа трафика для профилирования приложения

- Альтернативным вариантом является сохранение дампа в формате .pcap и просмотр в анализаторе протоколов
- Использование обозревателя:
https://<fw_ipaddr>/захват/<имя_захвата>/pcap/<имя_файла>.pcap
и сохранение файла для анализа
- Функция Wireshark «Follow the TCP stream» позволяет просмотреть запуск приложения Go2myPC (приложение для организации удаленного доступа):

```
GET /servlet/com.ec.ercbroker.servlets.PingServlet
HTTP/1.0

HTTP/1.0 200 OK

Pragma: no-cache

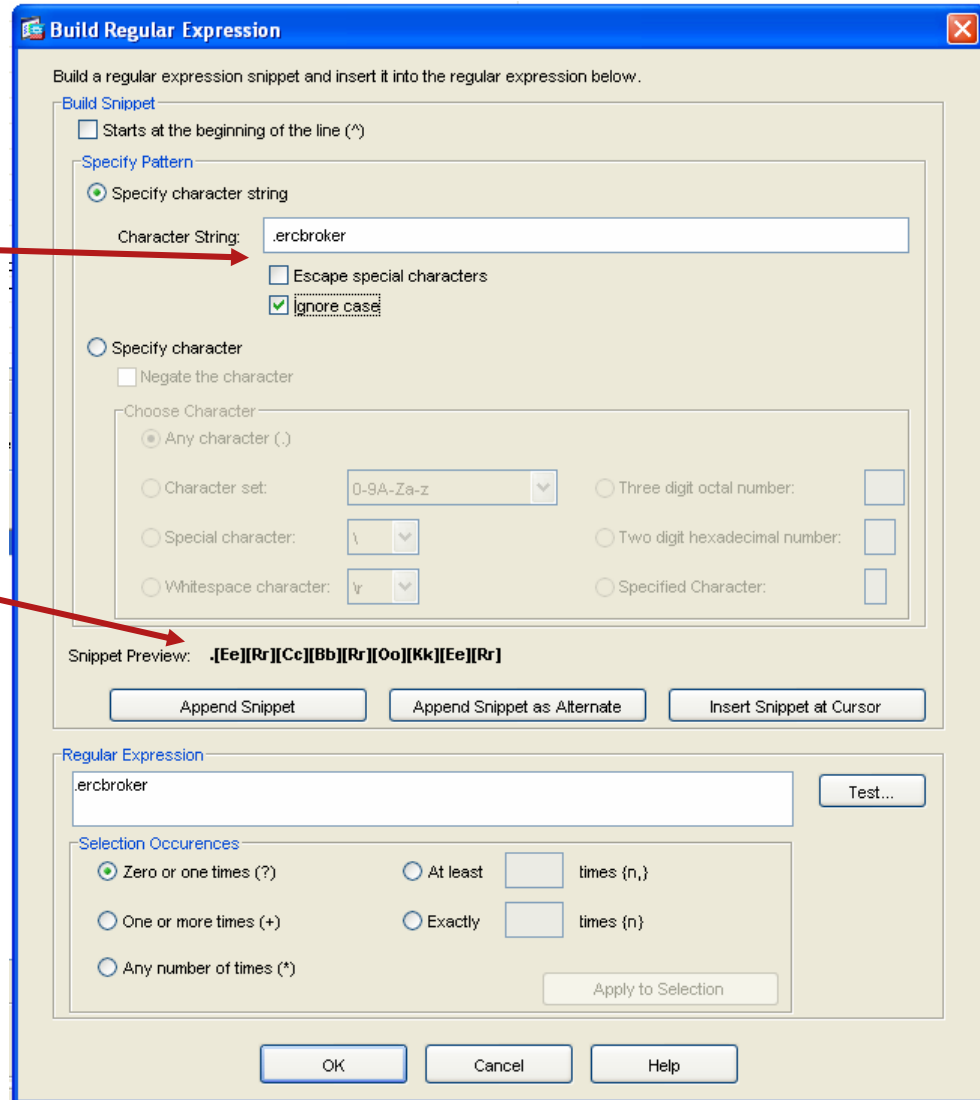
Content-Type: text/plain

Content-Length: 41

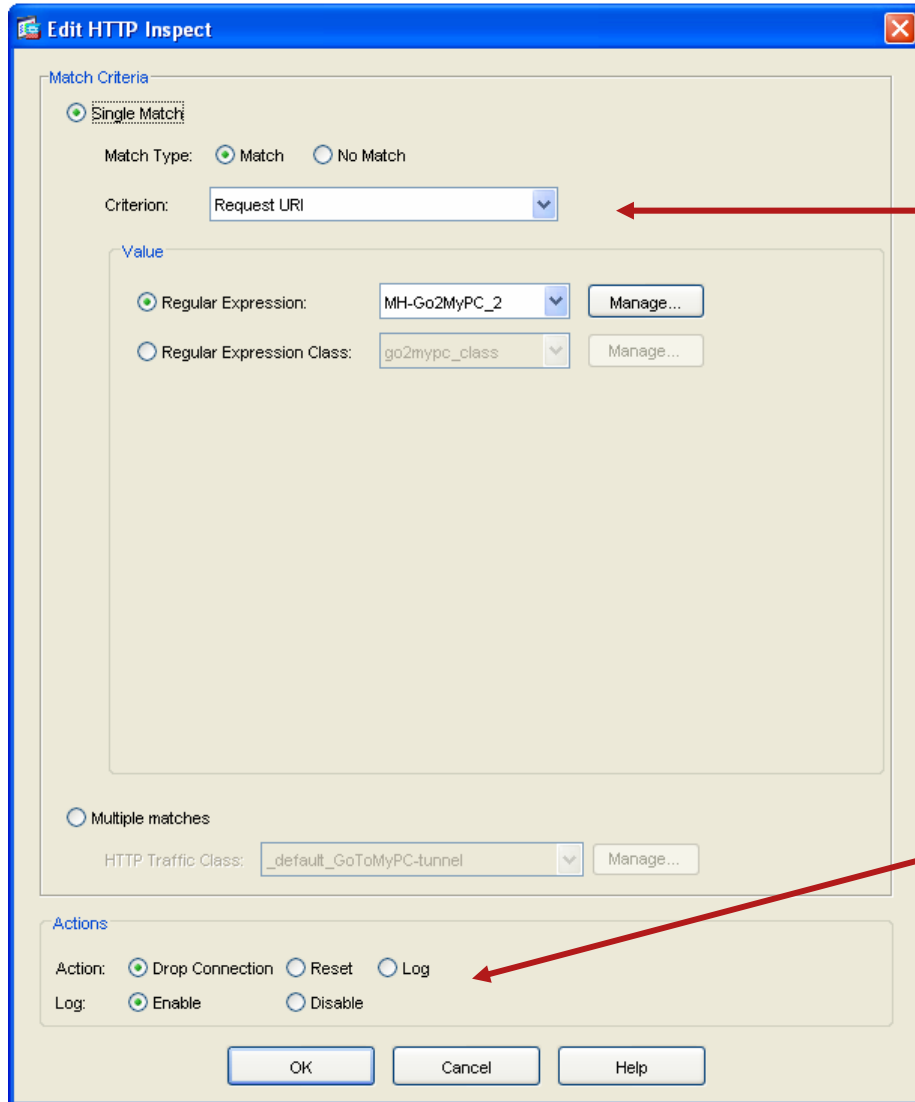
ERCBroker broker http://www.gotomypc.com
```

ASA: Мастер создания регулярных выражений ASDM

- Это строка, по которой выполняется поиск
- Установлен параметр игнорирования регистра при поиске

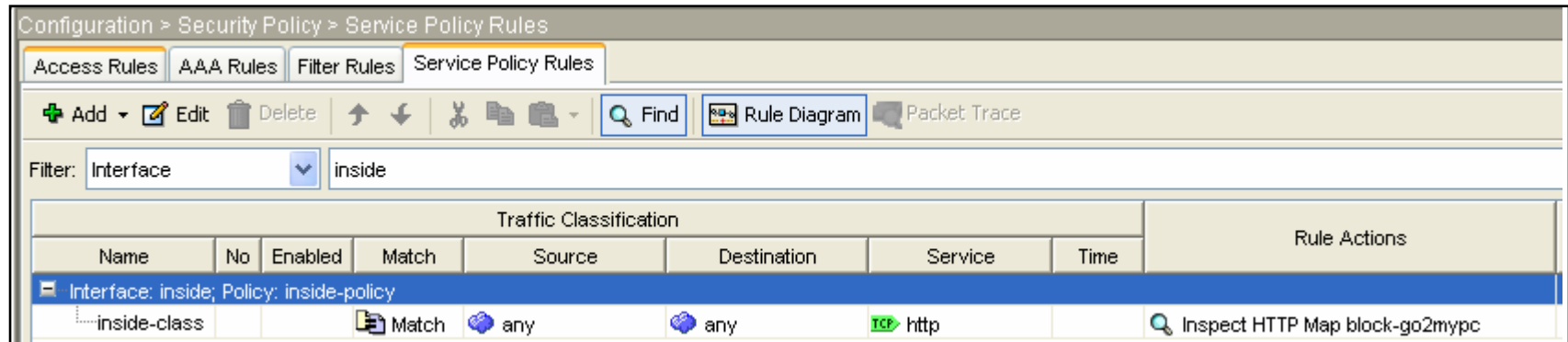


ASA: Пример использования, часть 2 — контроль ASDM HTTP



- Критерий совпадения — проверка URI, отправляемого клиентом
- Следует учесть, что в политике контроля HTTP можно задать условия, предусматривающие прерывание соединения, сброс клиента и сервера (TCP RST) или регистрацию подключения
- Поскольку наша политика безопасности не позволяет выполнять удаленное управление компьютером, соединение будет прервано, соответствующая запись будет занесена в журнал

ASA: Применение политики сервисов к интерфейсу



Traffic Classification								Rule Actions
Name	No	Enabled	Match	Source	Destination	Service	Time	
Interface: inside; Policy: inside-policy								
inside-class			Match	any	any	TCP http		Inspect HTTP Map block-go2mypc

- В этом примере следует учесть, что политика сервисов проверяет только tcp/80. Весь остальной трафик не связан с этой политикой
- При необходимости можно было выбрать более точные адреса отправителей и получателей уровня 3

ASA:

Проверка контроля HTTP

```
%ASA-6-302013: Built outbound TCP connection 5559 for
  outside:66.151.158.177/80 (66.151.158.177/80) to
  inside:192.168.1.201/1369 (xx.77.67.190/3184)

%ASA-6-106100: access-list inside_access_in denied tcp
  inside/192.168.1.201(1370) -> outside/66.151.158.177(8200) hit-
  cnt 1 first hit [0xfe57d861, 0x0]

%ASA-5-304001: 192.168.1.201 Accessed URL
  66.151.158.177:/servlet/com.ec.ercbroker.servlets.PingServlet

%ASA-5-415006: HTTP - matched request uri regex Block-Go2MyPC in
  policy-map block-go2mypc URI matched - Dropping connection from
  inside:192.168.1.201/1369 to outside:66.151.158.177/80

%ASA-6-302014: Teardown TCP connection 5559 for
  outside:66.151.158.177/80 to inside:192.168.1.201/1369 duration
  0:00:00 bytes 0 Flow closed by inspection

%ASA-5-304001: 192.168.1.201 Accessed URL
  66.151.158.177:/servlet/com.ec.ercbroker.servlets.PingServlet

%ASA-5-415006: HTTP - matched request uri regex Block-Go2MyPC in
  policy-map block-go2mypc URI matched - Dropping connection from
  inside:192.168.1.201/1371 to outside:66.151.158.177/80
```

ASA:

Краткий обзор контроля приложений

- В версии PIX/ASA 7.0 проведена модернизация и выполнены усовершенствования средств контроля работы приложений в устройствах защиты межсетевых взаимодействий
- Начиная с версии 7.2, в устройствах PIX и ASA был представлен механизм поиска с использованием регулярных выражений.
- Строки регулярных выражений могут быть очень эффективными и комплексными; используйте средство создания регулярных выражений ASDM и проверьте действительность совпадения по строке
- При использовании комплексного поиска по строке и при работе межсетевого экрана с большой нагрузкой следует принимать во внимание возможные проблемы производительности

Сдерживание распространения угроз с помощью TIDP

Передовые средства быстрого сдерживания распространения угроз и организации ответных действий

- Служба устранения угроз (Threat Mitigation Service, TMS) является системой для быстрой организации и распространения ответных действий на угрозы в масштабах всей сети
(**пока в процессе разработки !**)

Реагирование на угрозы практически в режиме реального времени

- Протокол распространения информации об угрозе (Threat Information Distribution Protocol, TIDP) используется для передачи сообщений, содержащих краткие сведения об угрозах и предлагаемые действия по их устранению

Сообщение с информацией об угрозе (TIM)

- Для устройств определены политики для передачи определенного вида трафика и выполнения ответных действий на угрозу

Список контроля доступа

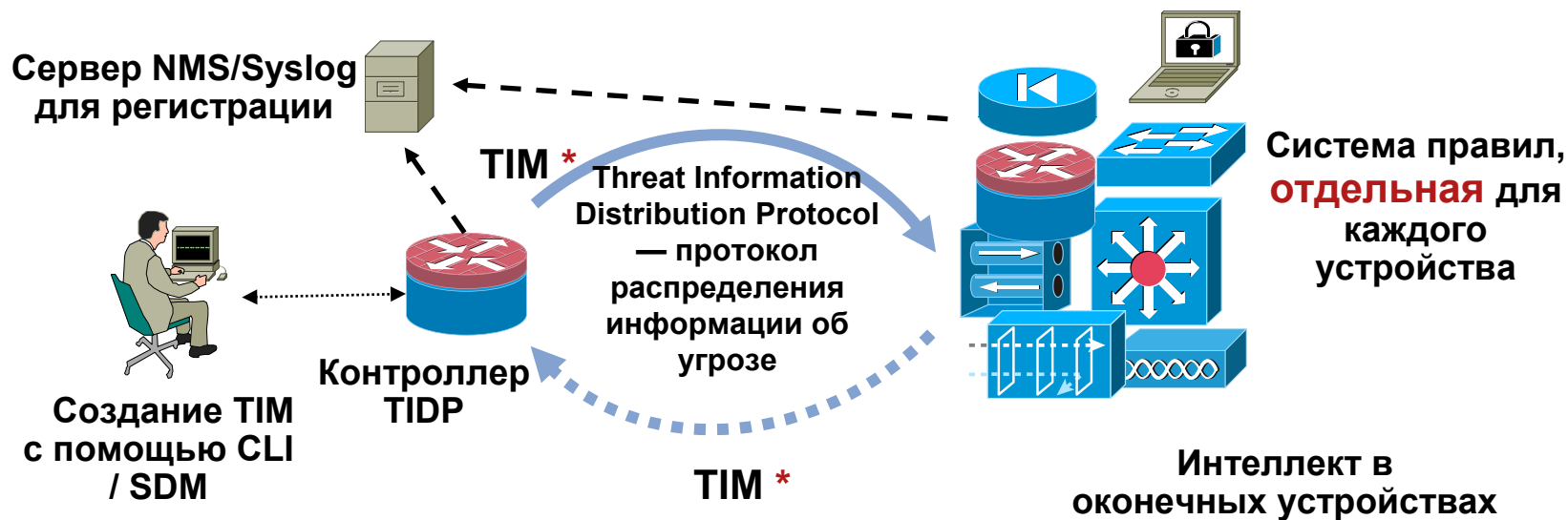
Перенаправление трафика

Протокол распространения информации об угрозе (Threat Information Distribution Protocol, TIDP)

- ТИМ передается потребителям TIDP с контроллера службы TMS
 - Сообщение с информацией об угрозе идентифицирует саму угрозу ТИМ, созданное в файле определения угрозы с использованием XML
- Сообщения аутентифицированы, зашифрованы и имеют защиту от повторной передачи
- Для приемных устройств настроены уникальные политики
 - Устройство использует локальную политику для преобразования ТИМ в средство динамической корректировки политики

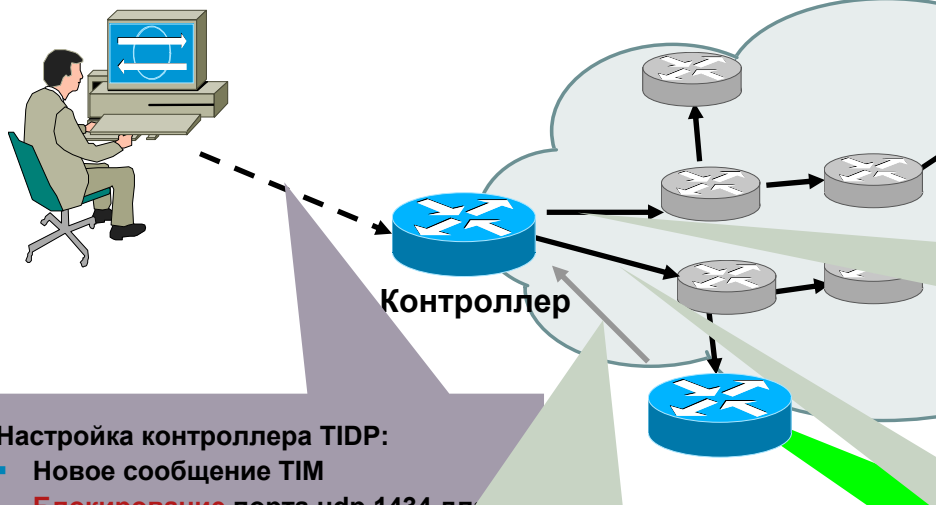
Быстрое устранение угроз

- TIDP — протокол, предназначенный для быстрого распространения информации о сетевых угрозах
- Все узлы, поддерживающие TIDP, используют область данных в соответствии с собственной конфигурацией и преобразовывают ее для выполнения необходимых действий



* TIM – Сообщение с информацией об угрозе

Slammer – TIDP в действии



Настройка контроллера TIDP:

- Новое сообщение TIM
- Блокирование** порта udr 1434 всех адресов отправителя получателя на всех интер маршрутизаторов и комм.
- Отправить новое сообще сеть

```

TIDP Header
-----
Authentication
-----
Response Message Header
TIM ID = 25
Threat ID = 5
ACK
-----
Payload
<XML..... >
  <CLI applied>
    <deny udp any any 1434/>
  </CLI applied>
  <CLI applied to>
    {list of I/Fs}
  </CLI applied to>
  
```

```

TIDP Header
-----
Authentication
-----
TIM Header
TIM ID = 25
Threat ID = 5
-----
Payload
<XML..... >
  <threat description>
    <information attack= "DDoS"/>
    <EventRiskRating Risk= "high"/>
  </threat description>
  <threat classification = "slammer">
    <stack>
      <header protocol="IP"/>
      <header protocol="UDP"/>
    </stack>
    <filter-entry id="sql">
      <match>
        <Eq field="UDP.destPort"
          value="1434"/>
      </match>
      <action type="block"/>
    </filter-entry id="sql"/>
  </threat classification >
  <device class>
    <device type="router"/>
    <device type="swtich"/>
  </device class>
  <device subclass>
    <subclass type="interface"/>
    <direction name="ingress"/>
  </device subclass>
  
```

Вопросы и ответы



