ASA 8. 2: Настройте Системный журнал с помощью ASDM

Содержание

Введение

Этот документ предоставляет сведения о том, как настроить системный журнал на устройстве адаптивной защиты Cisco (ASA) 8.x при помощи GUI Менеджера устройств адаптивной безопасности (ASDM) (ASDM). Сообщения журнала системы являются сообщениями, генерируемыми Cisco ASA для уведомления администратора относительно любого изменения в конфигурации, изменений в сетевой установке или изменений в производительности устройства. Путем анализа сообщений журнала системы администратор может легко устранить неполадки ошибки путем выполнения анализа основных причин.

Сообщения системного журнала в основном дифференцируются на основе их уровня

важности.

1. Степени серьезности ошибки 0 - Сообщения об аварии - Ресурс неприменимы
2. Степени серьезности ошибки 1 - Сигнальные сообщения - Срочные меры необходимы
3. Степени серьезности ошибки 2 - Критические сообщения - Критические условия
4. Степени серьезности ошибки 3 - Сообщения об ошибках - Состояния ошибки
5. Степени серьезности ошибки 4 - Предупреждающие сообщения - Состояния предупреждения
6. Степени серьезности ошибки 5 - Сообщения с уведомлением - Обычный, но значащие условия
7. Степени серьезности ошибки 6 - Информационные сообщения - Информационные сообщения только
8. Степени серьезности ошибки 7 - Сообщения отладки - Сообщения отладки только**Примечание:** Самый высокий уровень важности является аварийной ситуацией, и самый низкий уровень важности отлаживает.

Типовые сообщения системного журнала, генерируемые Cisco ASA, показывают здесь:

- %ASA-6-106012: Запретите IP от IP_address до IP_address, hex IP - режимов.
- %ASA-3-211001: Ошибка выделения памяти
- %ASA-5-335003: Список доступа по умолчанию NAC применился, ACL:ACL-название - host-address

Целочисленное значение X заданный в "%ASA-X-YYYYYY": обозначает степени серьезности ошибки сообщения. Например, "%ASA-6-106012" является Информационное сообщение, и "%ASA-5-335003" является Сообщение об ошибках.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия 8.2 Cisco ASA
- Версия Cisco ASDM 6.2

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

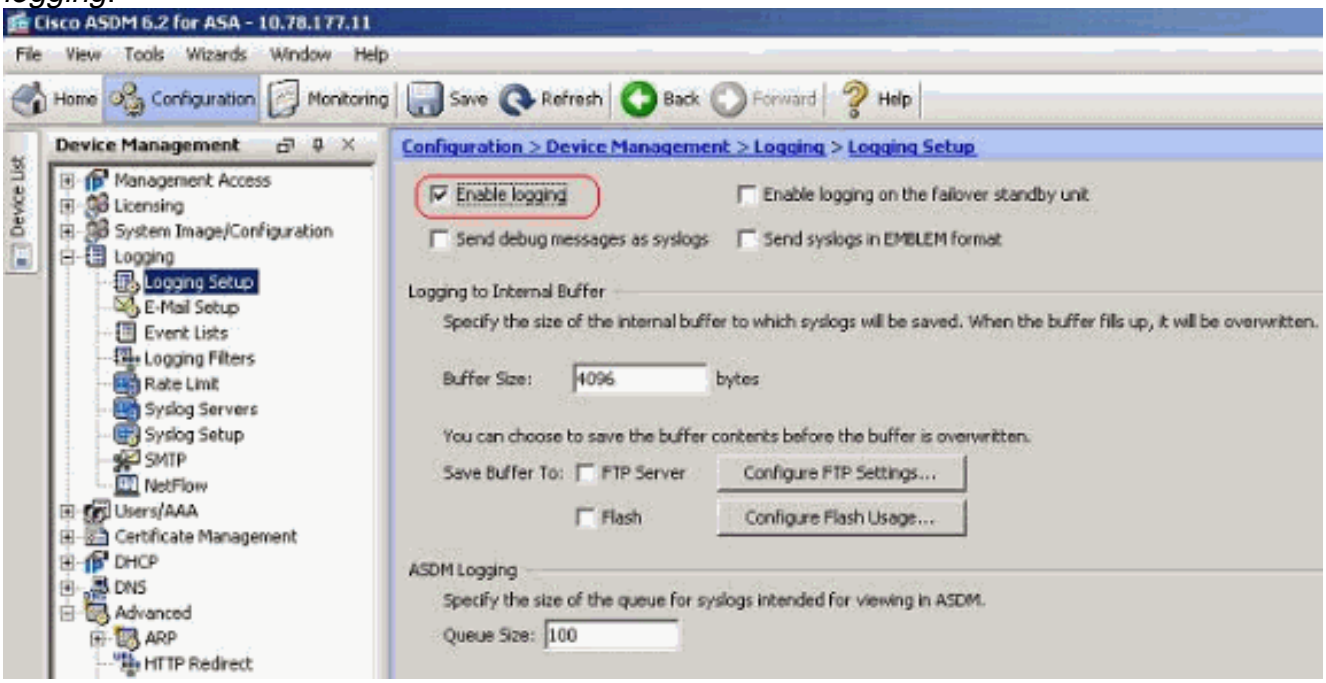
Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Основная Конфигурация системного журнала при помощи ASDM

Enable Logging

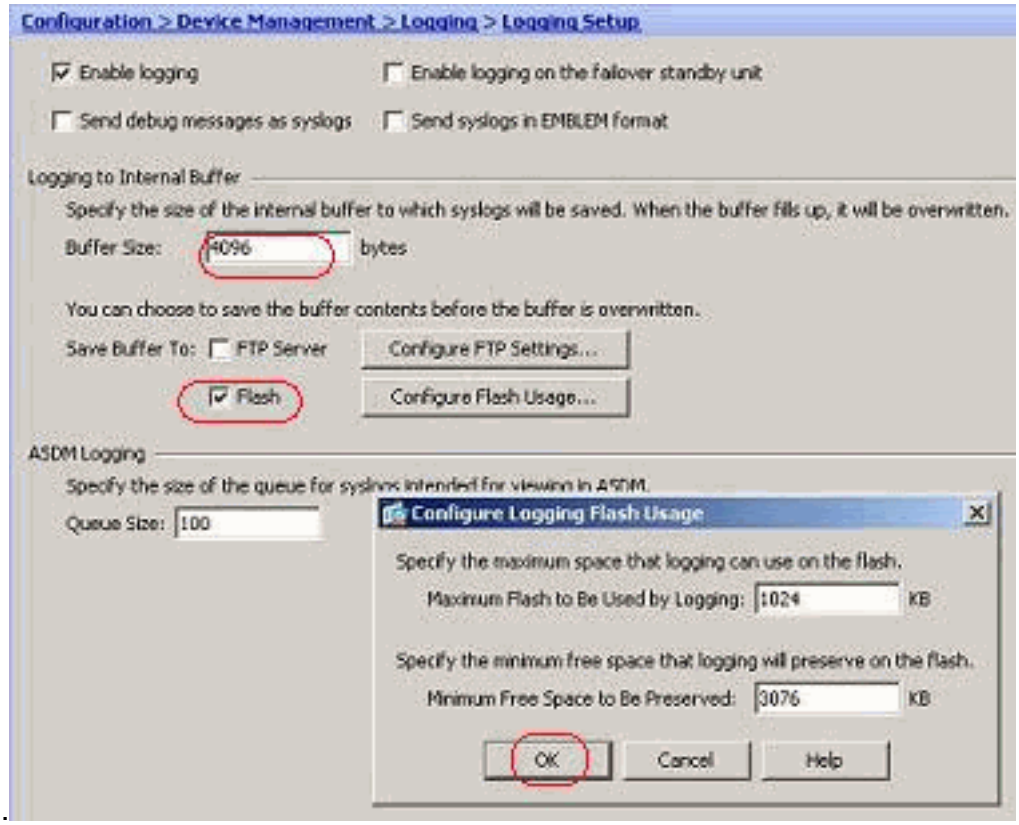
Выполните следующие действия:

1. Выберите *Configuration> Device Management> Logging> Logging Setup* и метка выбора опция *Enable logging*.

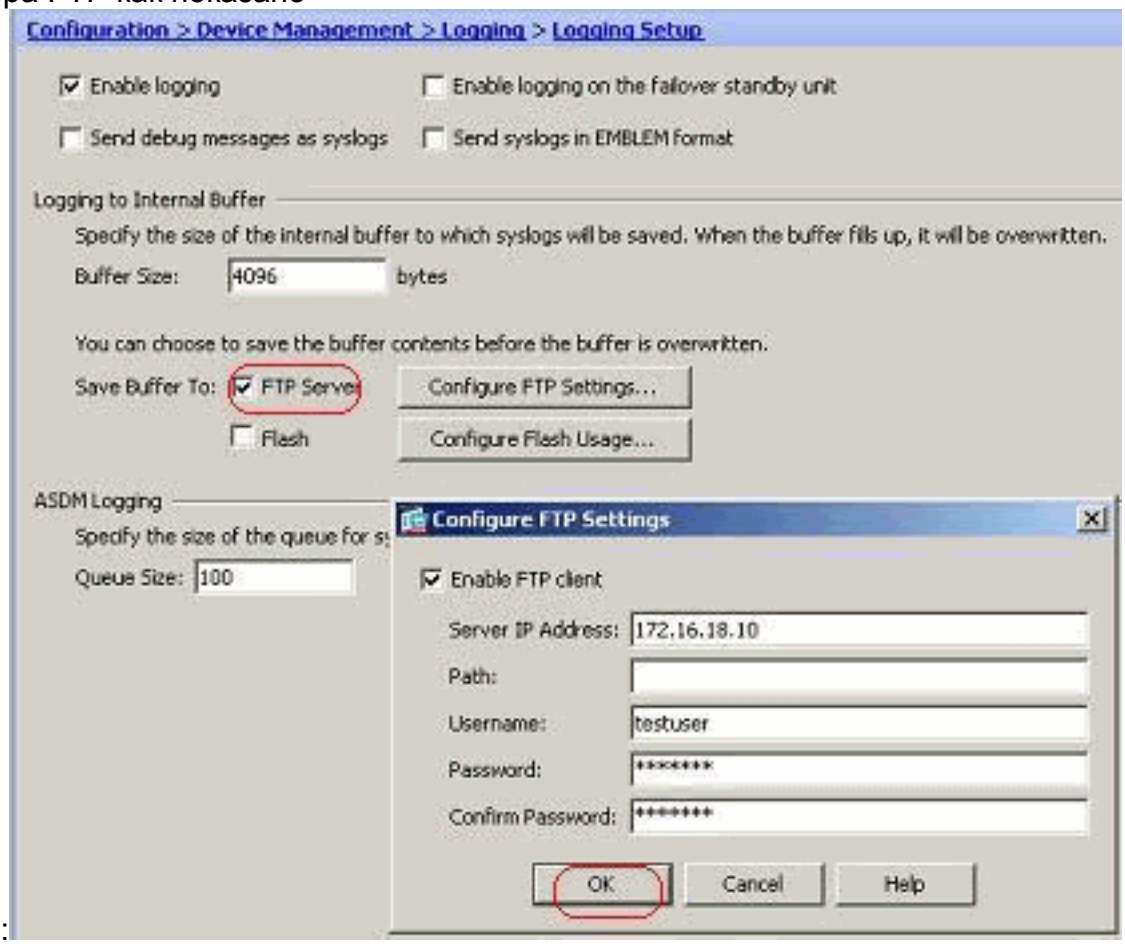


2. Можно регистрировать сообщения системного журнала к внутреннему буферу путем определения размера буфера. Можно также принять решение сохранить содержимое буфера к флэш-памяти путем нажатия *Configure Flash Usage* и определения параметров настройки

Флэша.



3. Буферизованные сообщения журнала могут быть переданы серверу FTP, прежде чем они будут перезаписаны. Нажмите *Configure FTP Settings* и задайте подробные данные сервера FTP как показано здесь:

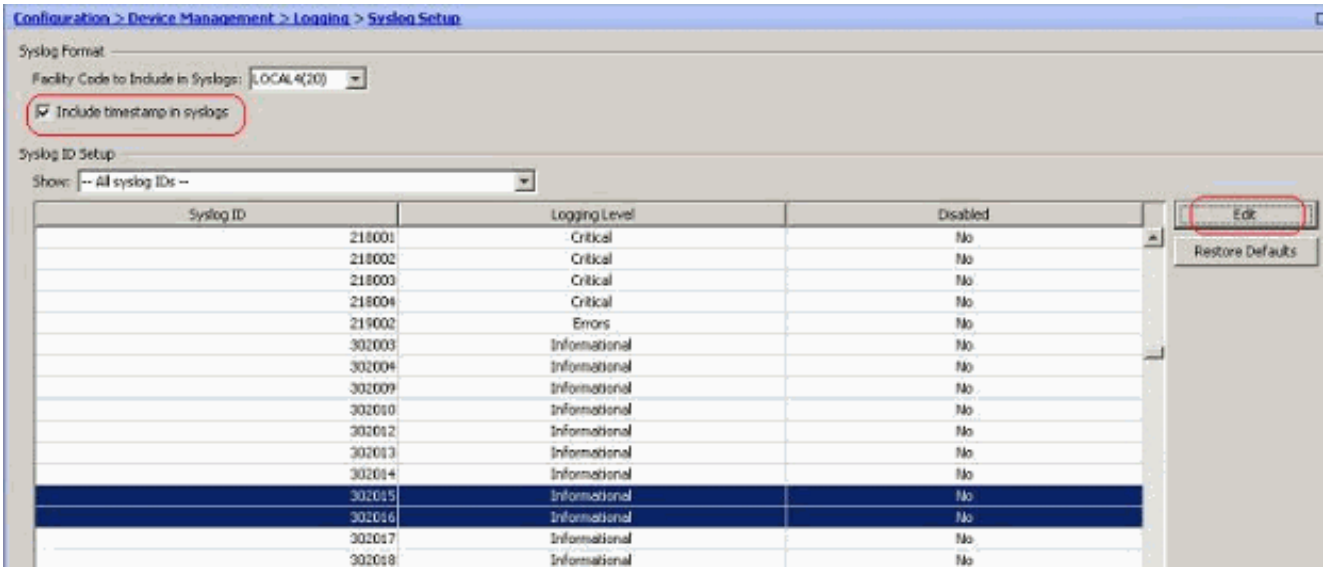


Отключите Регистрацию

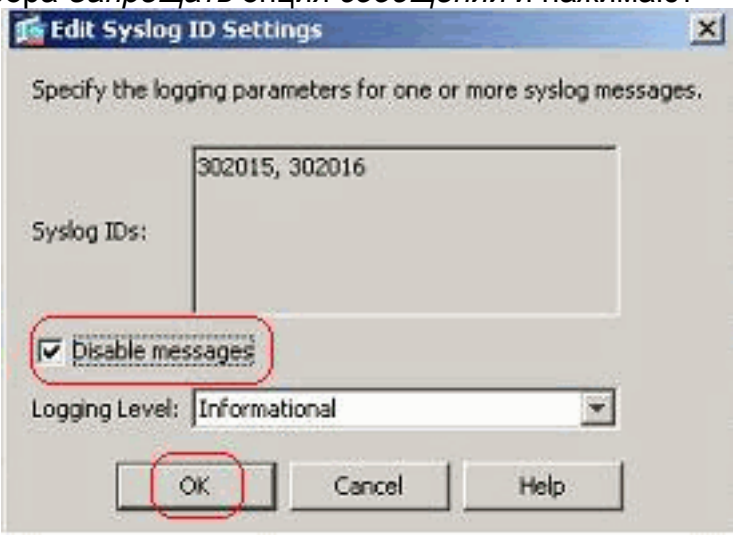
Можно отключить определенные идентификаторы системного журнала на основе требования.

Примечание: Путем выбора метки выбора для *Включать метки времени в* опции *системных журналов* можно добавить дату и времю, что они генерировались как поле к системным журналам.

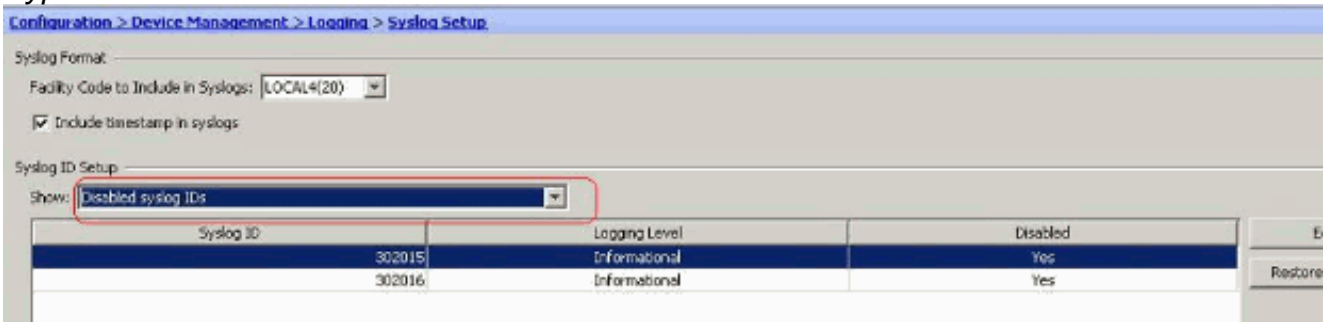
1. Выберите системные журналы, чтобы отключить и нажать *Edit*.



2. От *Окна настроек Идентификатора системного журнала Редактирования*, метка выбора *Запрещать* опция *сообщений* и нажимают *OK*.



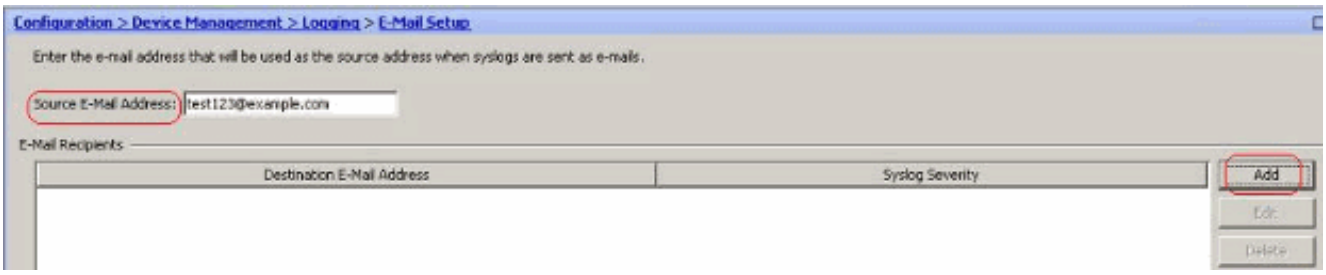
3. Отключенные системные журналы могут быть просмотрены в отдельной вкладке путем выбора *идентификаторов системного журнала Disabled* от раскрывающегося меню *Настройки Идентификатора системного журнала*.



Регистрация к электронной почте

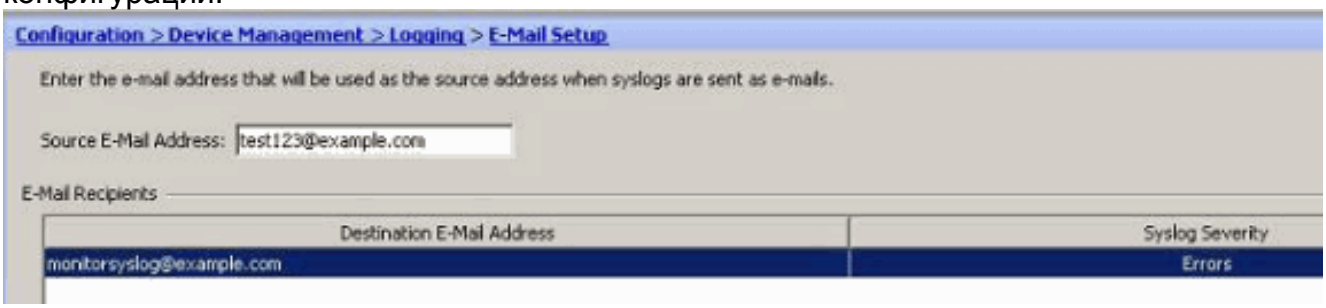
Выполните эти шаги с помощью ASDM для передачи системных журналов к электронной почте:

1. Выберите *Configuration> Device Management> Logging> E-Mail Setup*. Поле *Source E-Mail Address* полезно в присвоении почтового ID как источник для системных журналов. Задайте исходный адрес электронной почты. Теперь, *нажмите Add* для добавления получателей e-mail.

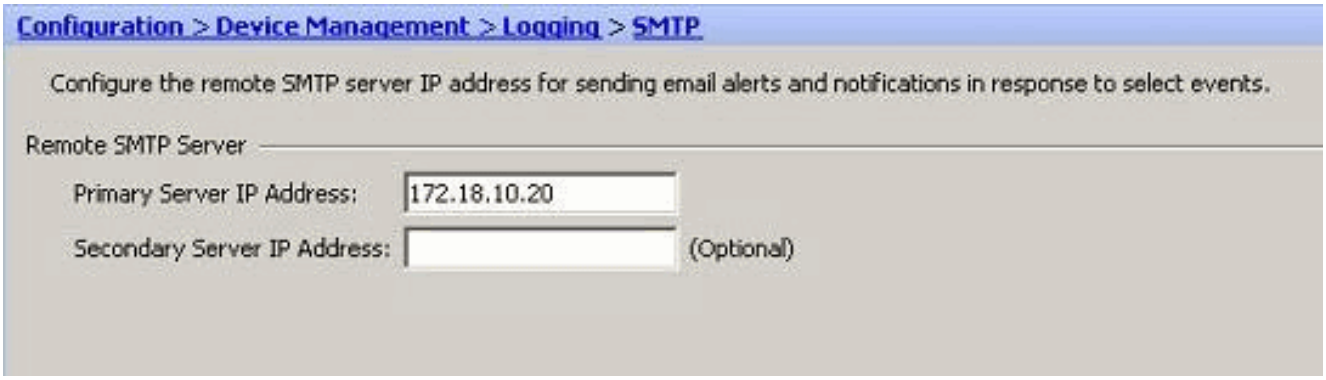


2. Задайте *Целевой Адрес электронной почты* и выберите *Уровень важности*. На основе уровней важности можно определить других получателей e-mail. Нажмите *OK* для возврата назад к области *E-Mail Setup*.

Это приводит к этой конфигурации:

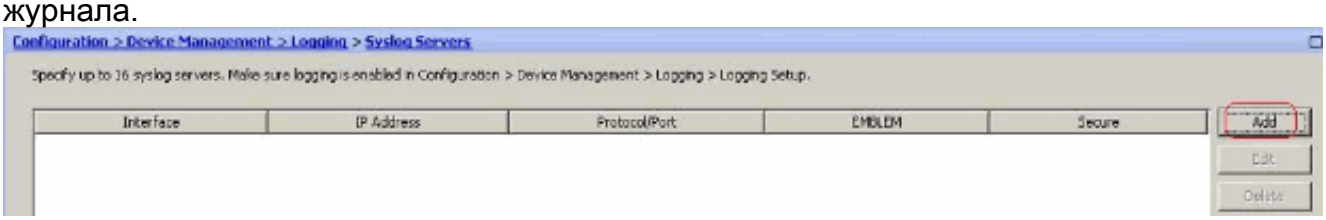


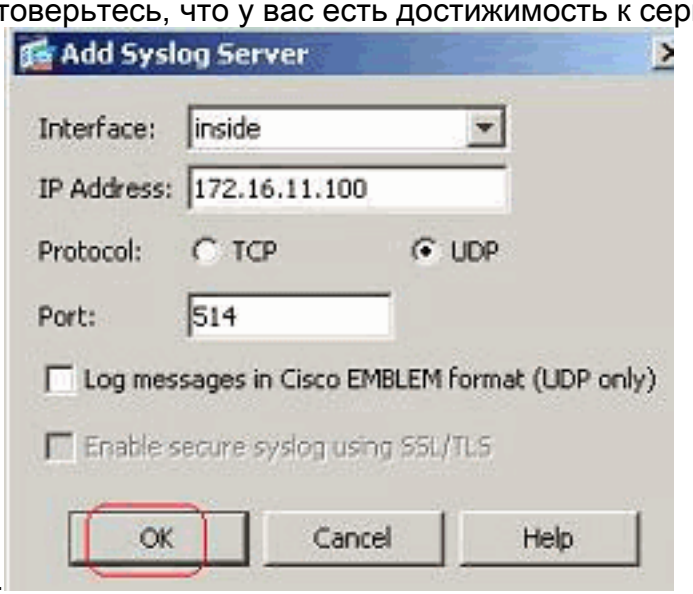
3. Выберите *Configuration> Device Setup> Logging> SMTP* и задайте сервер SMTP.



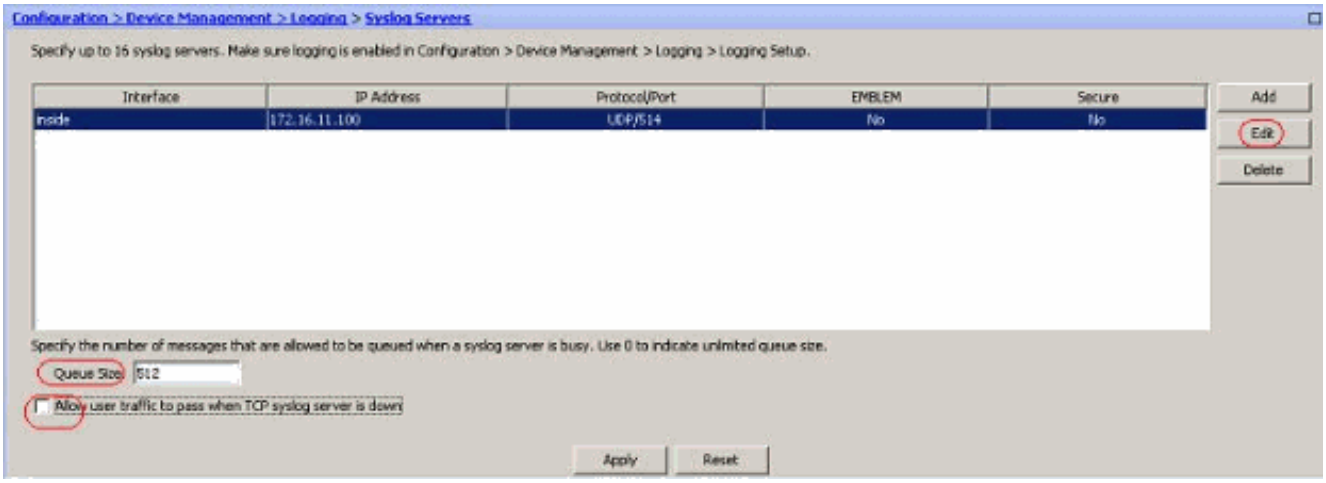
Регистрация к серверу системного журнала

Можно передать все сообщения системного журнала к специализированному серверу системного журнала. Выполните эти шаги при помощи ASDM:

1. Выберите *Configuration> Device Management> Logging> Syslog Servers* и *нажмите Add* для добавления сервера системного журнала.


Окно *Add Syslog Server* появляется.
2. Задайте интерфейс, что сервер привязан к наряду с IP-адресом. Задайте *Протокол* и *Port detail* в зависимости от вашей сетевой установки. *Затем нажмите кнопку OK.***Примечание:** Удостоверьтесь, что у вас есть достижимость к серверу системного журнала от Cisco ASA.


3. Настроенный сервер системного журнала замечен как показано здесь. Модификации могут быть сделаны при выборе этого сервера затем нажмите *Edit*.



Примечание: Метка выбора *Позволять трафик пользователя для передачи, когда сервер системного журнала TCP не работает* на опцию. В противном случае сеансы нового пользователя запрещены через ASA. Это применимо только, когда транспортный протокол между ASA и сервером системного журнала является TCP. По умолчанию, когда сервер системного журнала не работает по любой причине, новые сеансы доступа к сети запрещены Cisco ASA.Для определения типа сообщений системного журнала, которые должны быть переданы серверу системного журнала, видеть раздел Logging Filter.

Усовершенствованная Конфигурация системного журнала при помощи ASDM

Работа со Списками событий

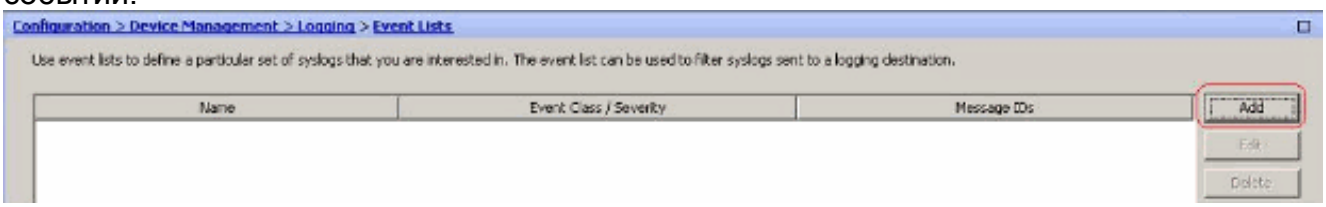
Списки событий позволяют нам создать настроенные списки, которые содержат группу сообщений системного журнала, которые должны быть переданы назначению. Списки событий могут быть созданы тремя другими способами:

- Идентификатор сообщения или Диапазон идентификаторов сообщения
- Важность сообщения
- Класс сообщения

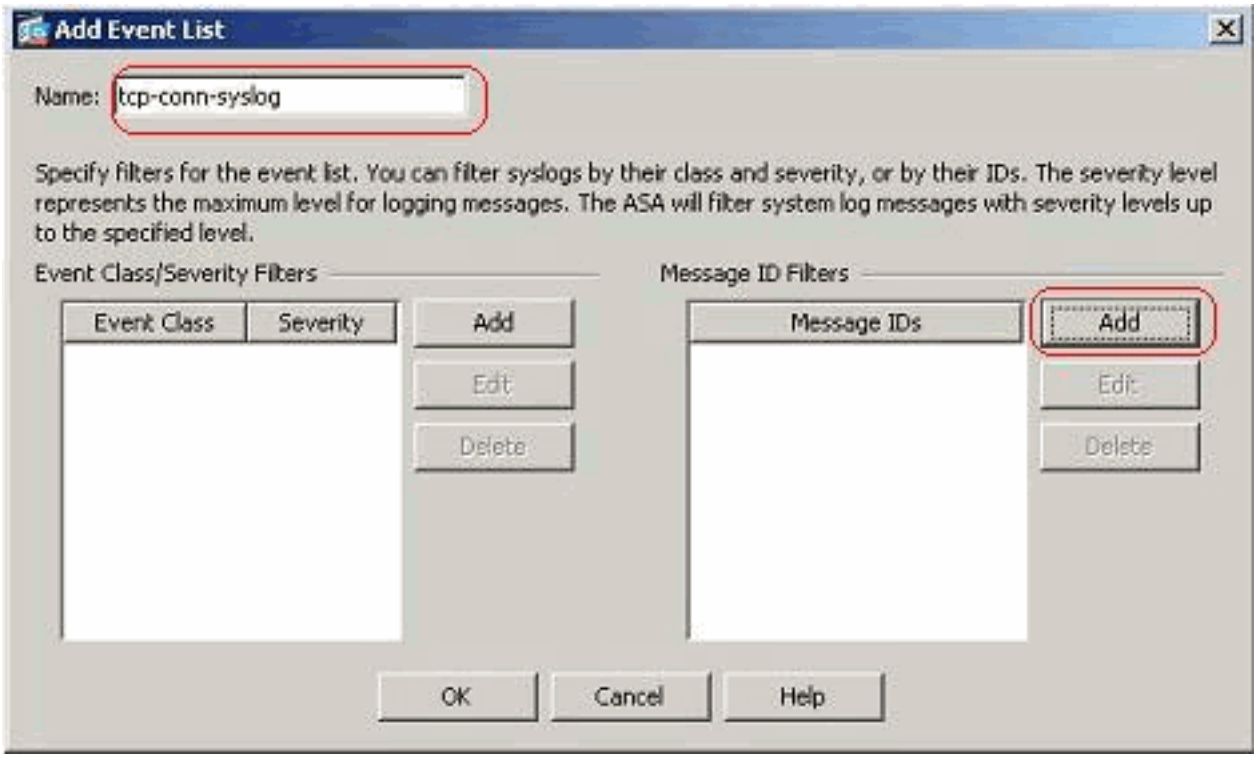
Идентификатор сообщения или Диапазон идентификаторов сообщения

Выполните данные действия:

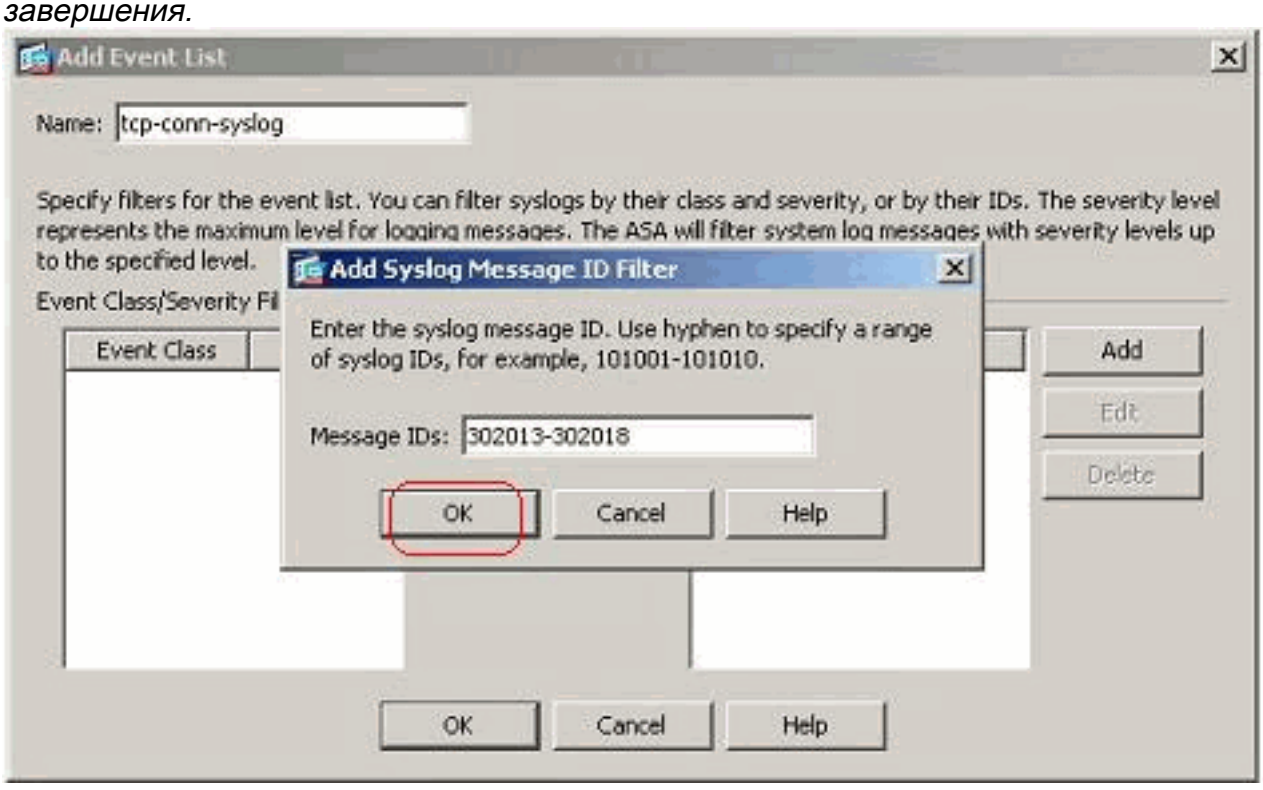
1. Выберите *Configuration> Device Management> Logging> Event Lists* и *нажмите Add* для создания нового Списка событий.



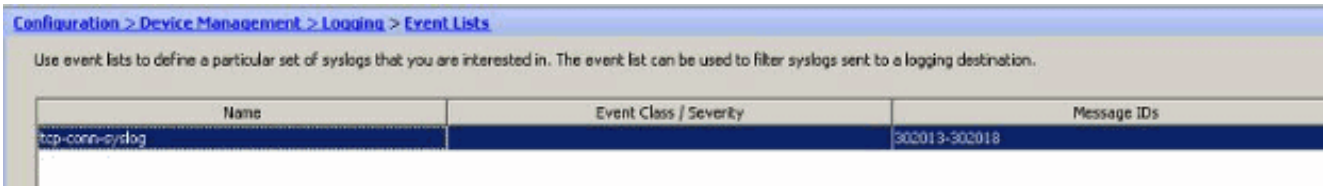
2. Задайте название в *Поле имени*. *Нажмите Add* в области *Message ID Filters* для создания нового Списка событий.



3. Задайте диапазон ID сообщения системного журнала. Здесь сообщения системного журнала TCP взяли, например. *Нажмите OK для завершения.*



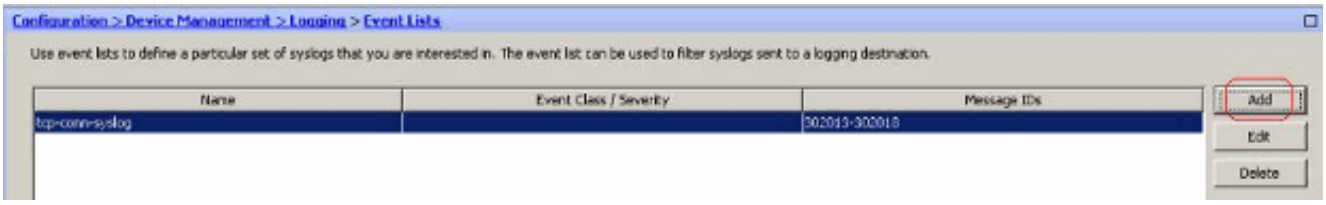
4. Нажмите *OK* снова для возвращения назад к окну *Event Lists*.



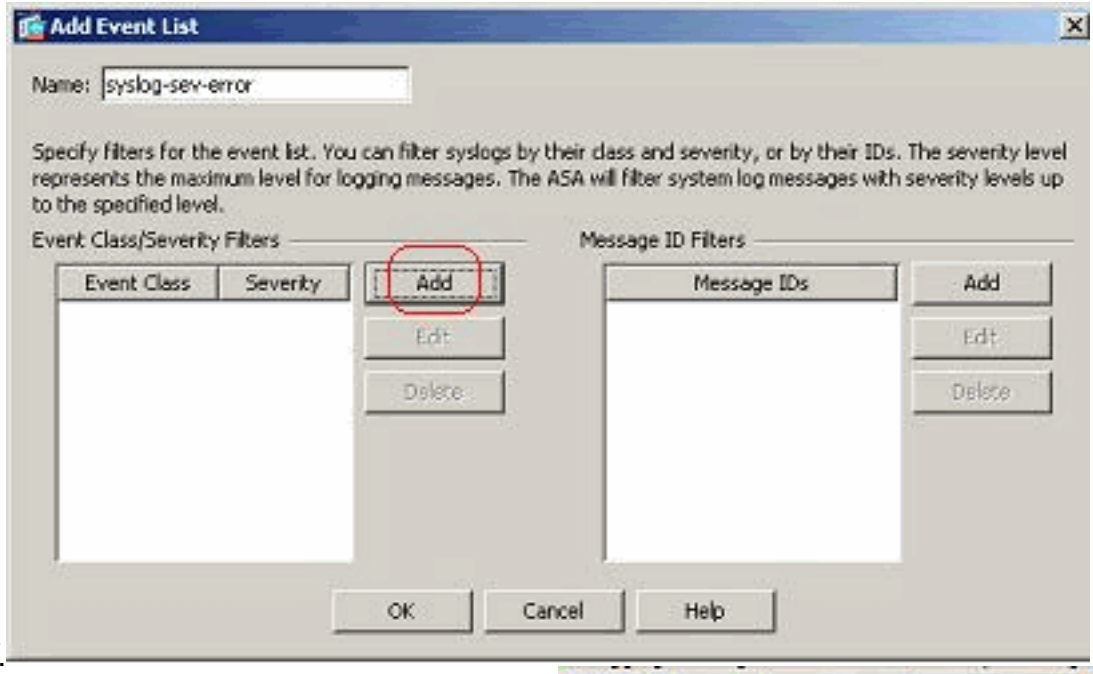
Важность сообщения

1. Списки событий могут также быть определены на основе важности сообщения.

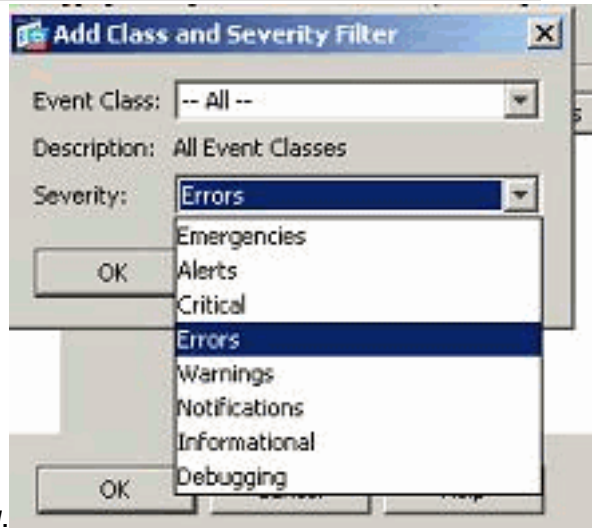
Нажмите Add для создания отдельного Списка событий.



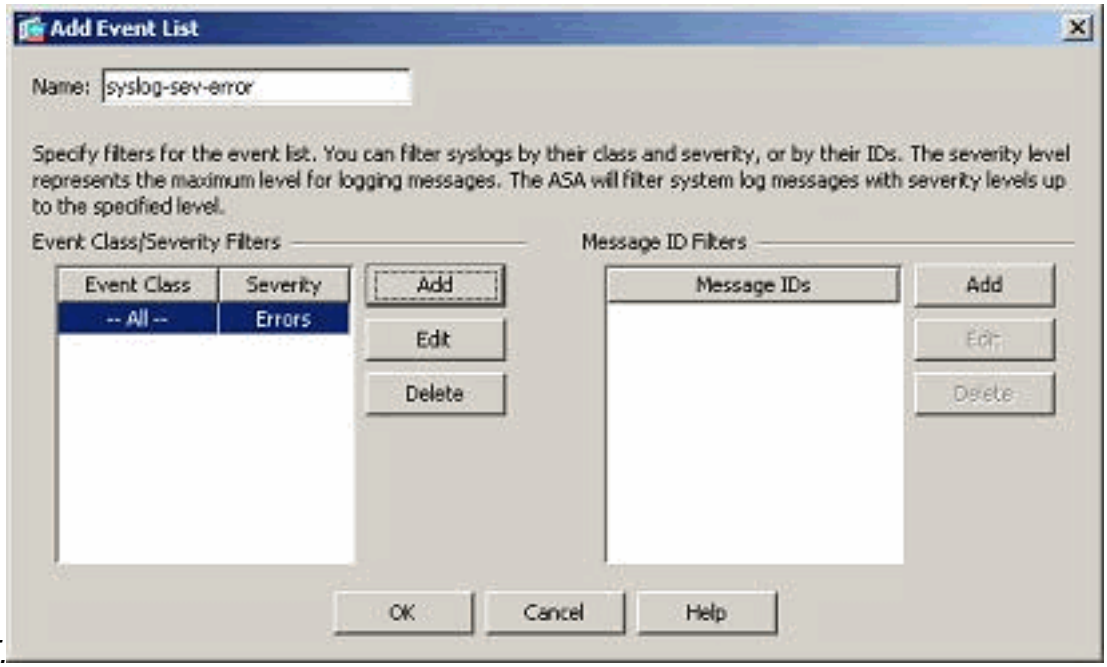
2. Задайте название и *нажмите*



Add.



3. Выберите уровень важности как *Ошибки*.
4. *Нажмите кнопку*



OK.

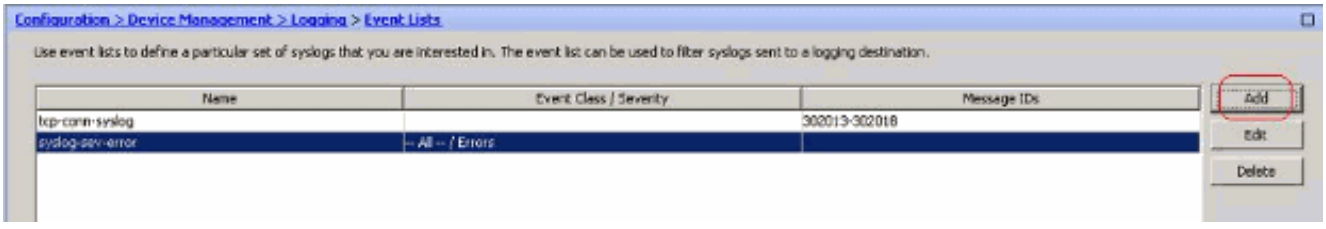
Класс сообщения

Списки событий также настроены на основе Класса сообщения. Класс сообщения является группой сообщений системного журнала, отнесенных к функции устройства безопасности, которая позволяет вам задать весь класс сообщений вместо того, чтобы задать класс для каждого сообщения индивидуально. Например, используйте подлинный класс для выбора всех сообщений системного журнала, которые отнесены к проверке подлинности пользователя. Некоторые доступные классы сообщений показывают здесь:

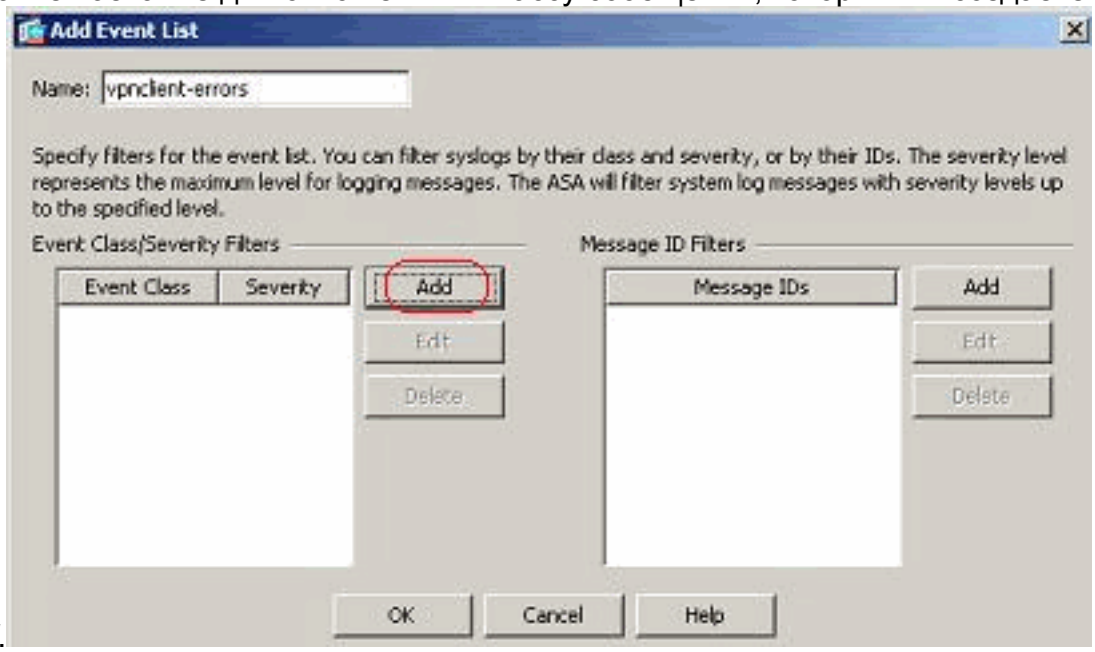
- Все — Все классы события
- auth — Проверка подлинности пользователя
- мост — Прозрачный межсетевой экран
- приблизительно — Центр сертификации PKI
- config — Интерфейс Команды
- ха — Аварийное переключение
- ips — Сервис Защиты от проникновения
- ip — Стек IP
- np — Сетевой процессор
- ospf — Маршрутизатор OSPF
- rip — Маршрутизация RIP
- сеанс — Пользовательский сеанс

Выполните эти шаги для создания класса события на основе *vpnclient-ошибочного* класса сообщения. Класс сообщения, *vpnc*, доступен для категоризации всех сообщений системного журнала, отнесенных к vpnclient. Уровень важности для этого класса сообщения выбран в качестве "ошибок".

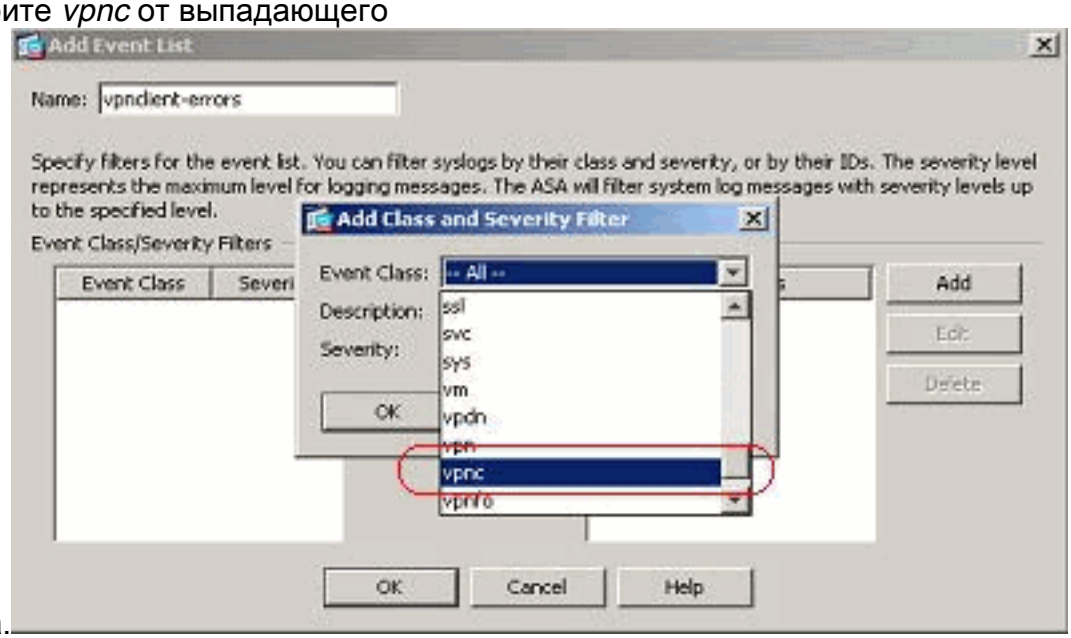
1. Нажмите Add для создания нового Списка событий.



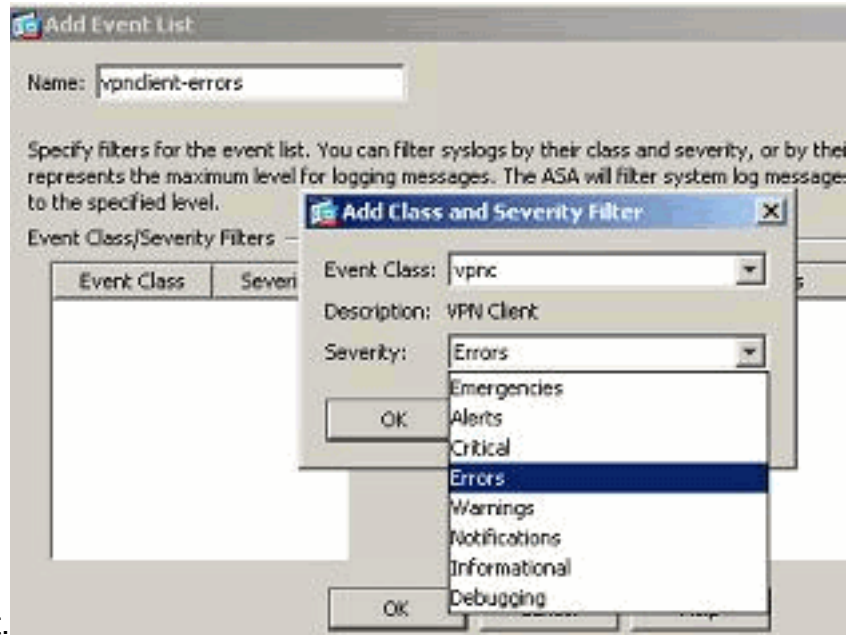
2. Задайте название для отношений к классу сообщения, который вы создаете и *нажмите Add*.



3. Выберите *vpnc* от выпадающего списка.

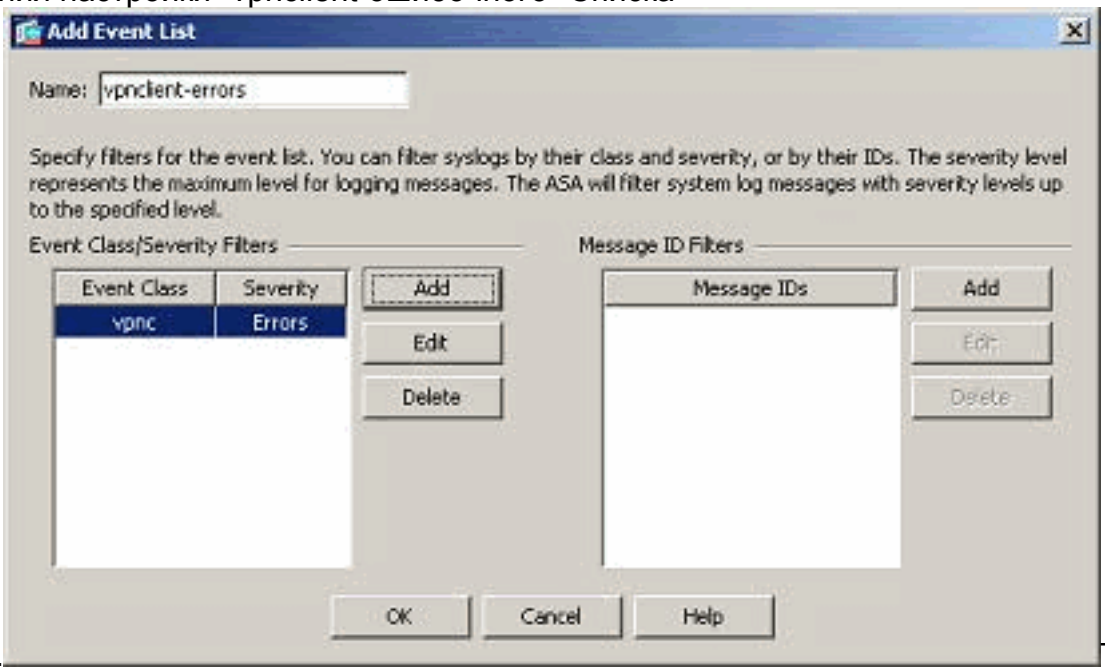


4. Выберите уровень важности как *Ошибки*. Этот уровень важности применим для тех сообщений, которые зарегистрированы для этого класса сообщения только. Нажмите *OK* для возвращения назад к окну Add Event

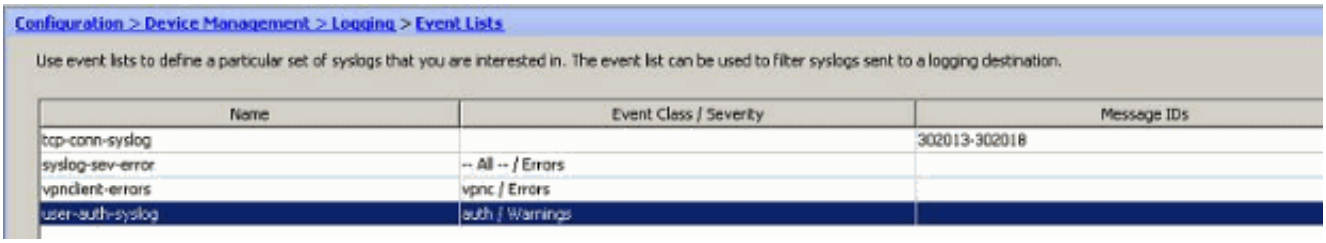


List.

5. Класс события / степени серьезности ошибки показывают здесь. Нажмите *OK* для завершения настройки "vpnclient-ошибочного" Списка



событий.Также показано в следующем снимке экрана, что новый Список событий, "user-auth-syslog", создан с классом сообщения как "аутентификация" и уровень важности для системных журналов этого определенного класса сообщения как "Предупреждения". Путем настройки этого Список событий задает все сообщения системного журнала, которые отнесены к "подлинному" классу сообщения с уровнями важности **до** уровня "Предупреждений".**Примечание:** Здесь, термин "до" имеет значение. При обозначении уровня важности имейте в виду, что все сообщения системного журнала будут зарегистрированы до того уровня.**Примечание:** Список событий может содержать классы несколька событий. "Vpnclient-ошибочный" Список событий модифицируется путем нажатия **Edit** и определения нового класса события "ssl/error".



Работа с logging filter

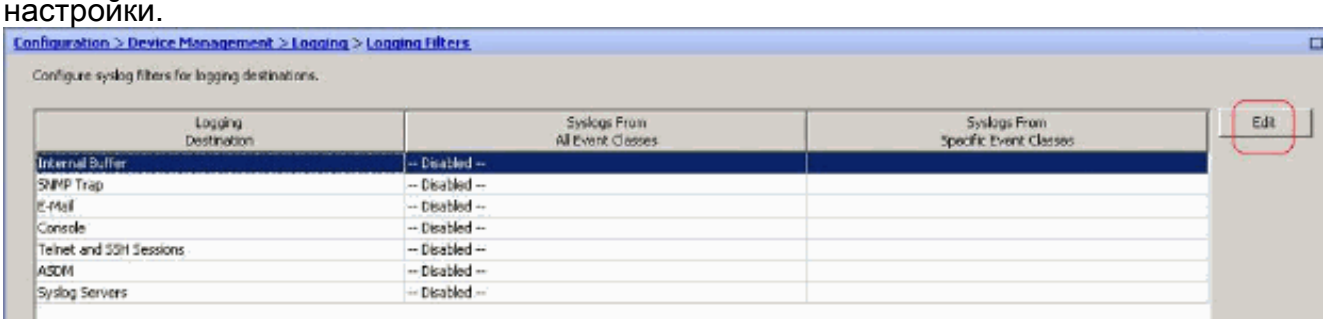
Logging filter используется для передачи сообщений системного журнала к указанному месту назначения. Эти сообщения системного журнала могут основываться на "Степенях серьезности ошибки" или "Даже Списки".

Это типы назначений, к которым эти фильтры применимы:

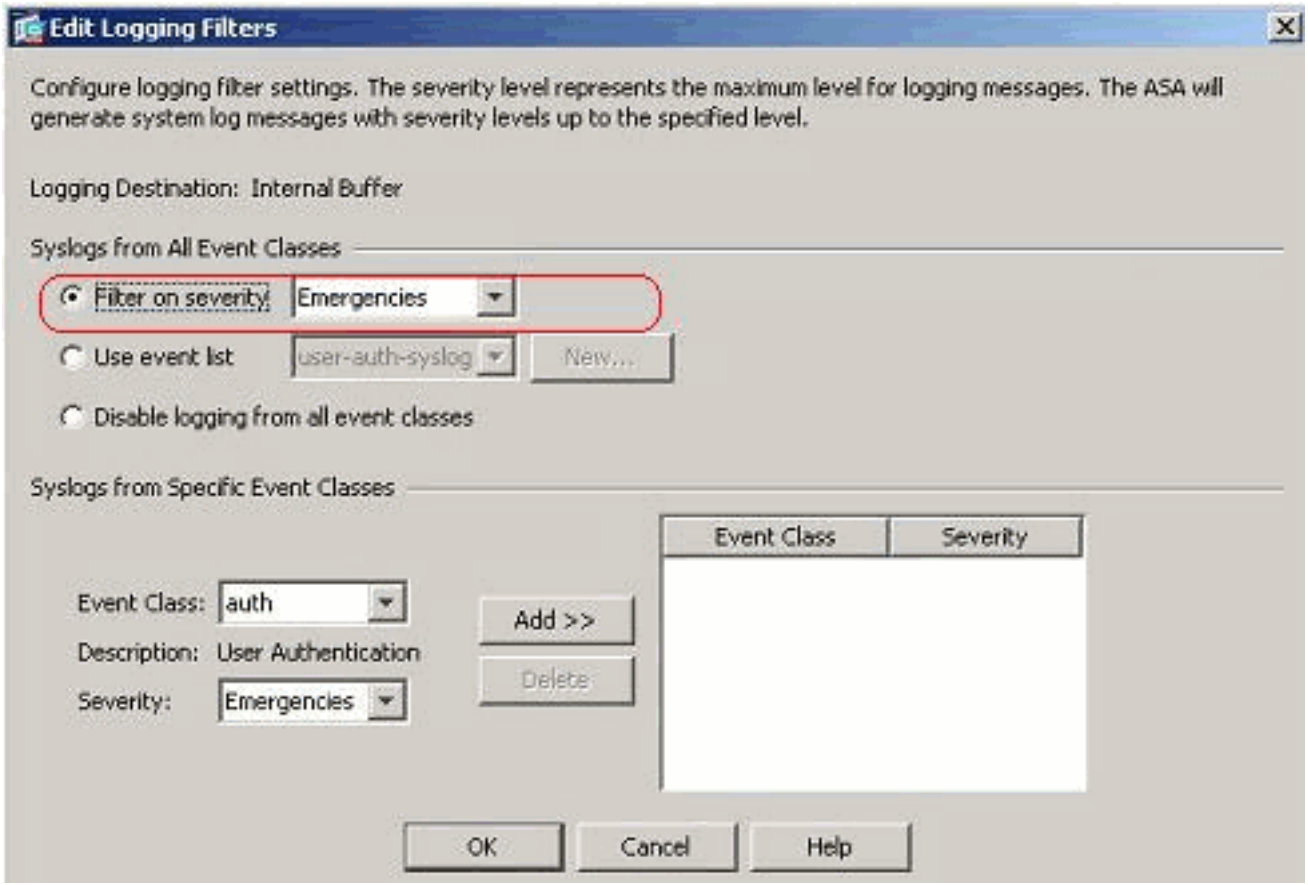
- Внутренний буфер
- Сообщение SNMP
- Электронная почта
- Консоль
- Сеансы Telnet
- ASDM
- Серверы системного журнала

Выполните данные действия:

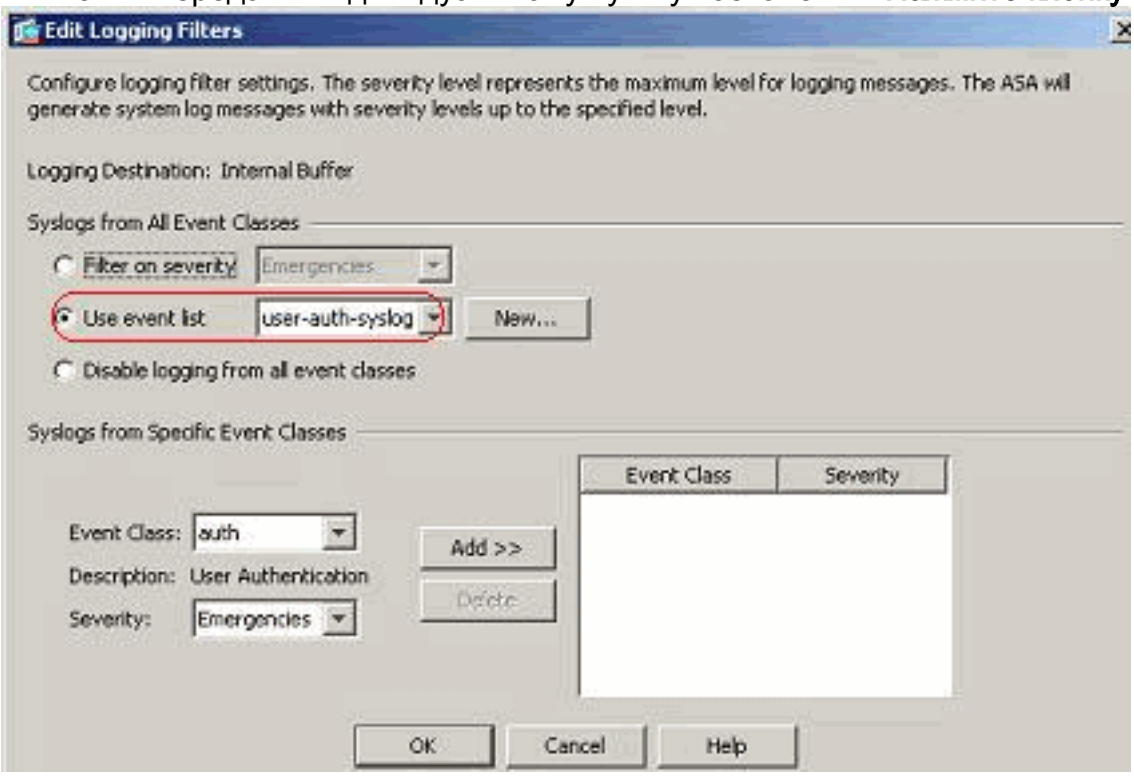
1. Выберите **Configuration> Device Management> Logging> Logging Filters** и выберите конечное место регистрации. Затем нажмите **Edit** для изменения параметров настройки.



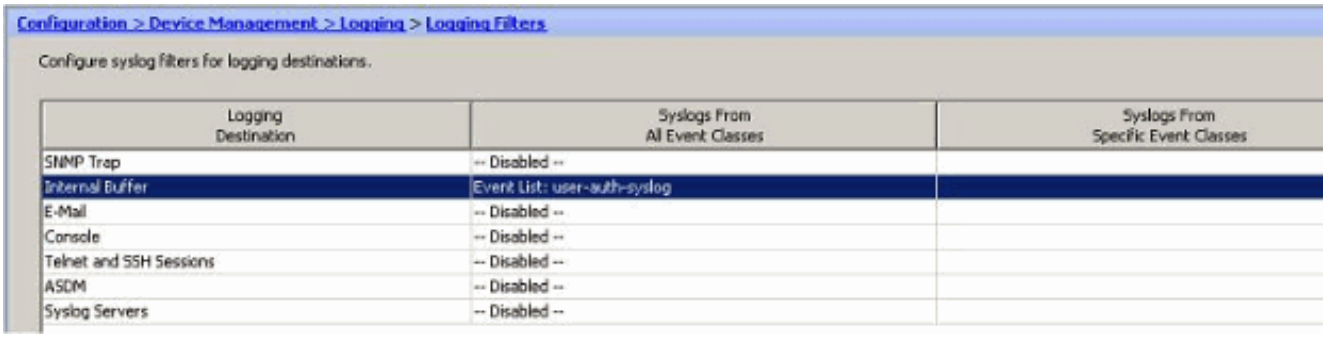
2. Можно передать сообщения системного журнала на основе степеней серьезности ошибки. Здесь, **Аварийные ситуации** были выбраны для показа как пример.



3. Список событий может также быть выбран для определения, какой тип сообщений должны быть переданы индивидуальному пункту назначения. **Нажмите кнопку ОК.**

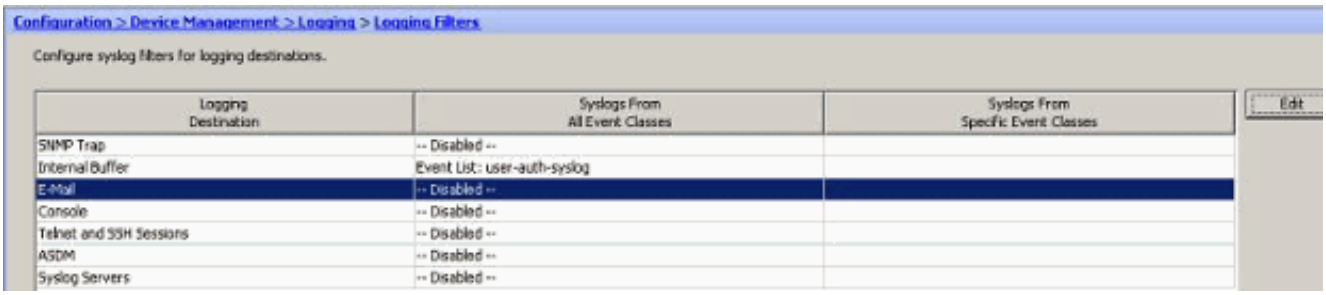


4. Проверьте модификацию.

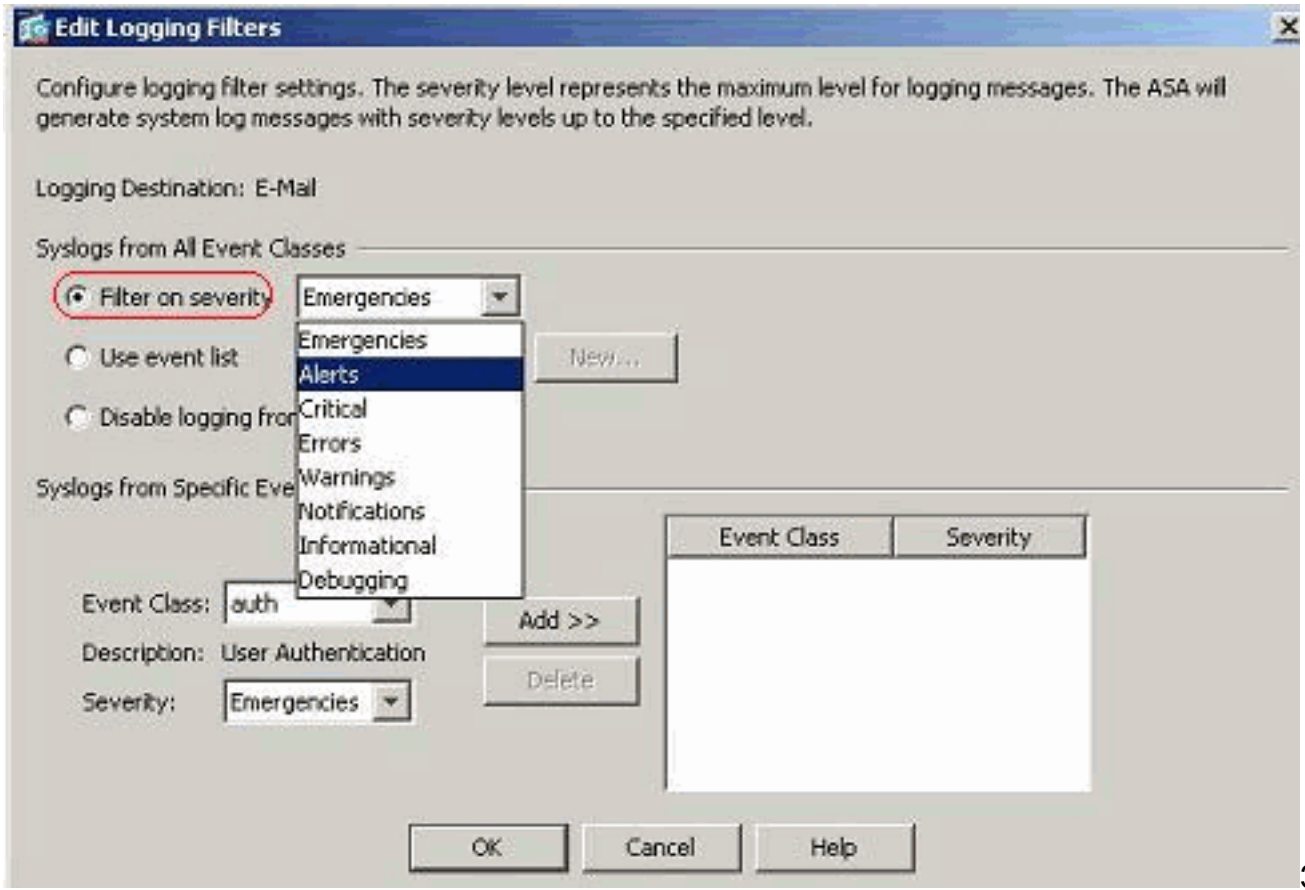


Это шаги в то, как передать группу сообщений (на основе их уровня важности) к E-mail сервер.

1. Выберите **E-mail** в поле Logging Destination. Затем нажмите **Edit**.

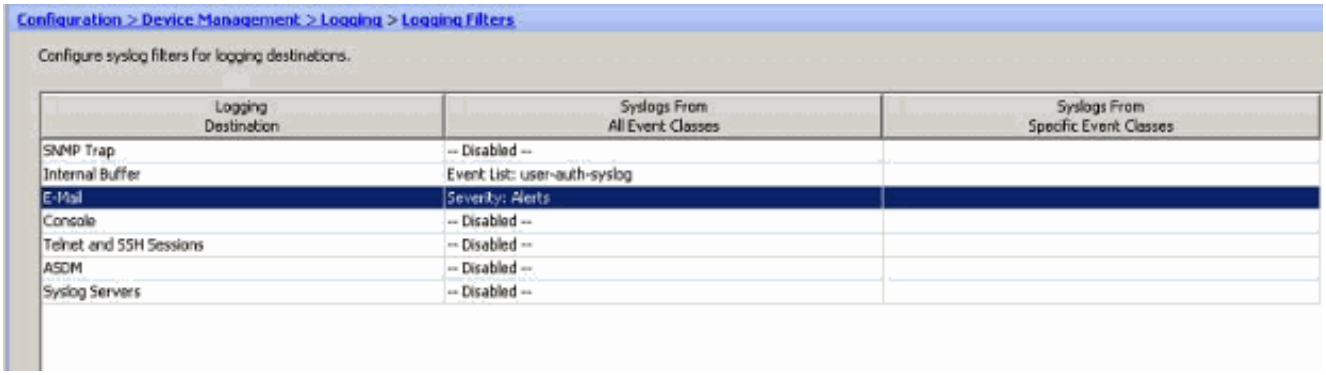


2. Выберите **Filter на опции severity** и выберите требуемый уровень важности.

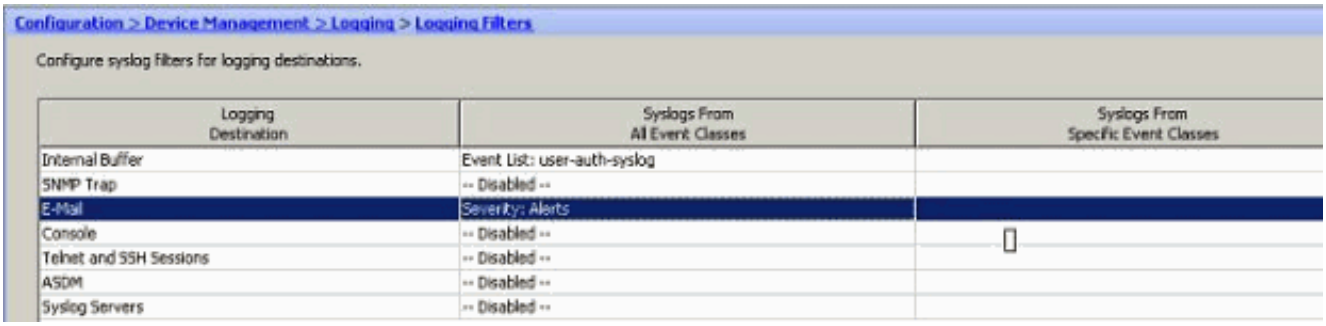


3

десь, **Предупреждения** были выбраны как уровень важности.



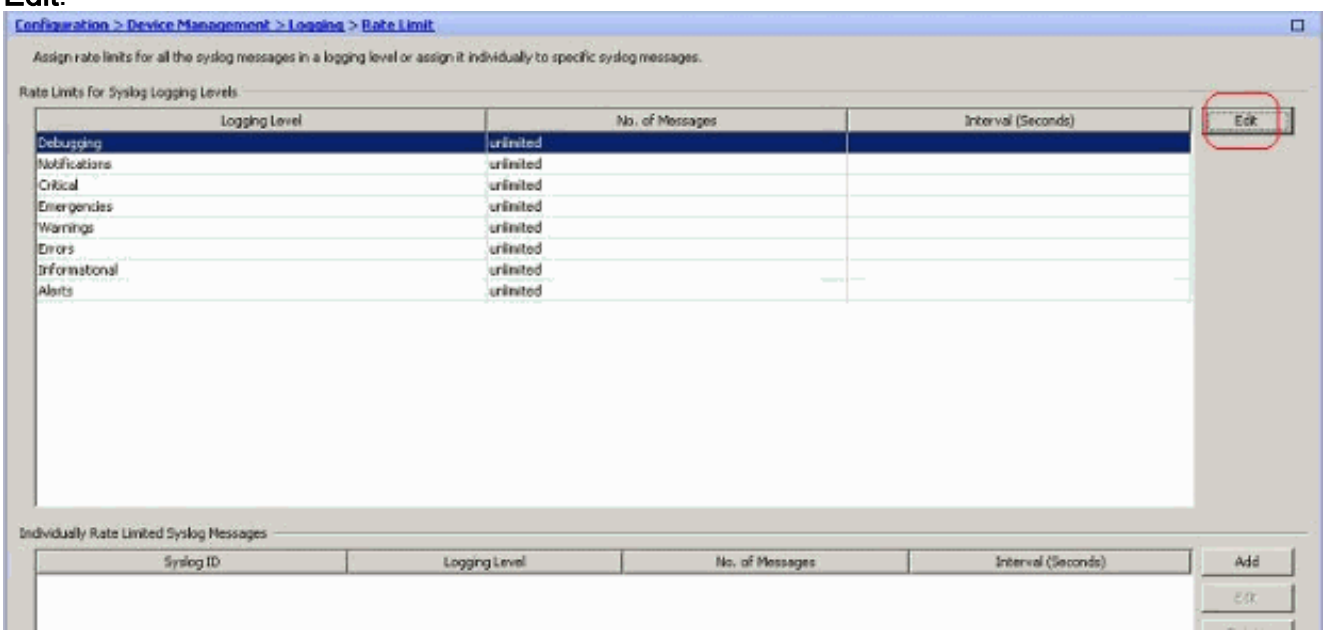
Вы видите, что все Аварийные сообщения системного журнала должны быть переданы настроенной Электронной
почте.



Rate limit

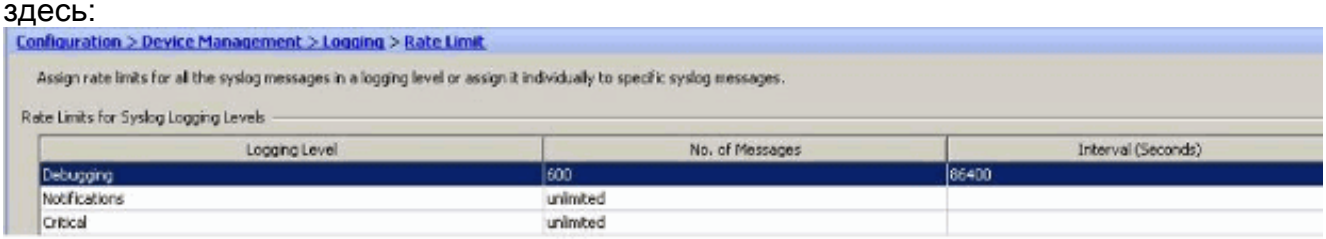
Это задает количество сообщений системного журнала, которые Cisco ASA передает назначению в указанном периоде времени. Это обычно определяется для уровня важности.

1. Выберите **Configuration> Device Management> Logging> Rate Limit** и выберите требуемый уровень важности. Затем нажмите
Edit.



2. Задайте Количество сообщений, которые будут передаваться наряду с Временным интервалом. **Нажмите кнопку**

OK. **Примечание:** Эти номера даны как пример. Они отличаются в зависимости от среды типа сети.Модифицированные значения замечены
здесь:

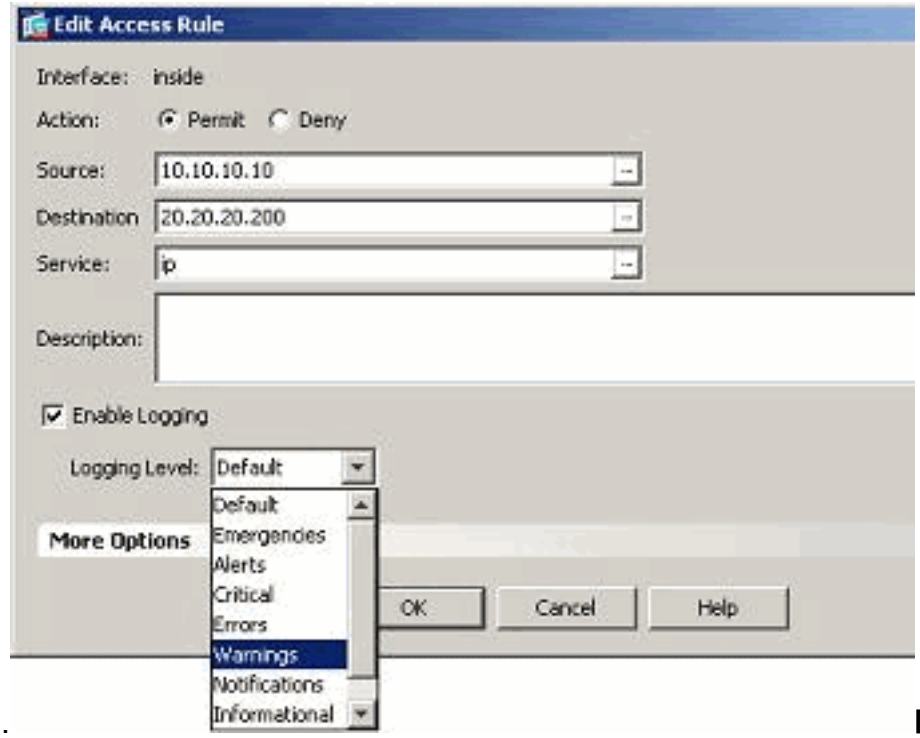


Регистрация соответствия правила доступа

Можно регистрировать соответствия правила доступа с помощью ASDM. Поведение регистрации по умолчанию состоит в том, чтобы передать сообщение системного журнала за всеми отклоненными пакетами. Не будет никакого сообщения системного журнала для разрешенных пакетов, и они не будут зарегистрированы. Однако можно определить пользовательский уровень важности регистрации к правилу доступа отследить количество пакетов, которое поражает это правило доступа.

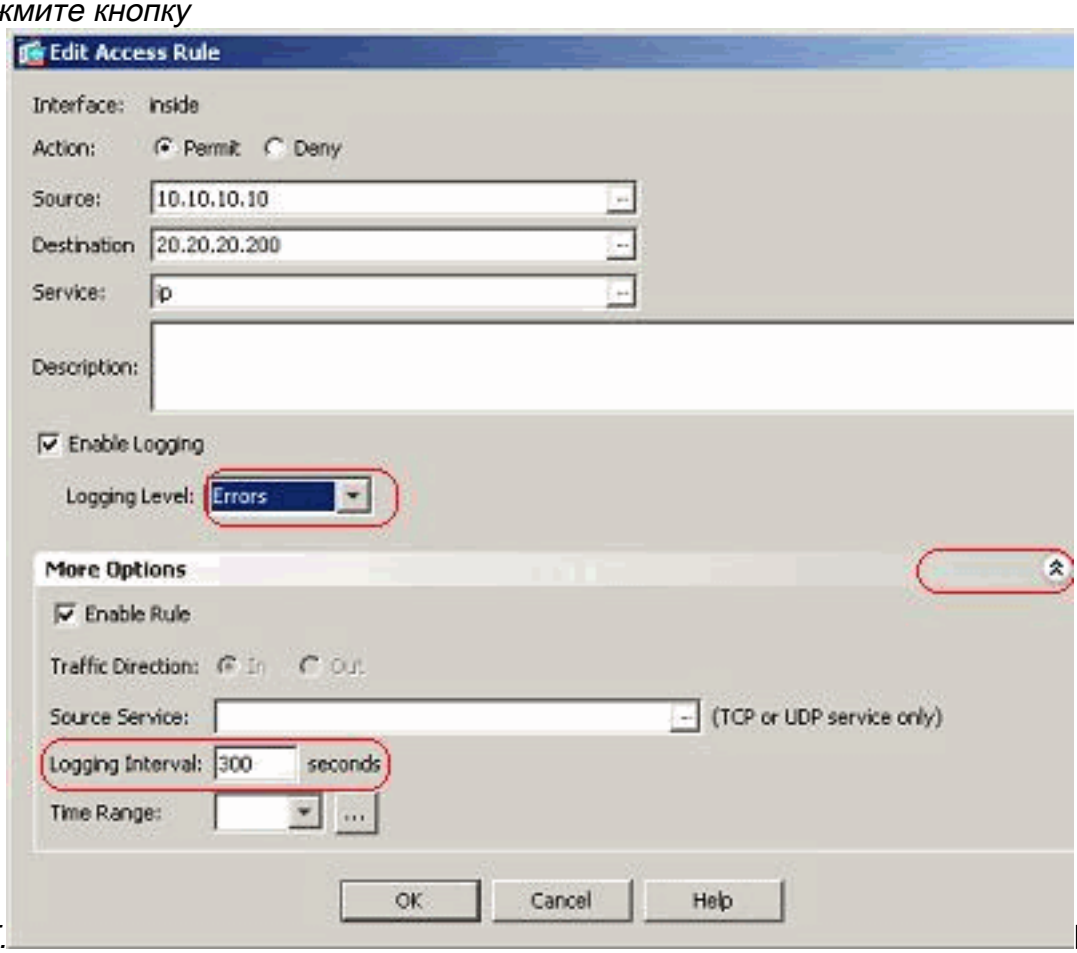
Выполните данные действия:

1. Выберите требуемое правило доступа и нажмите *Edit*.Окно *Edit the Access Rule*



появляется. **Примечание:** В этом образе *Параметр по умолчанию* в *поле Logging Level* указывает на поведение регистрации по умолчанию Cisco ASA. Для получения дополнительной информации об этом, обратитесь к разделу Действия Списка доступа Регистрации.

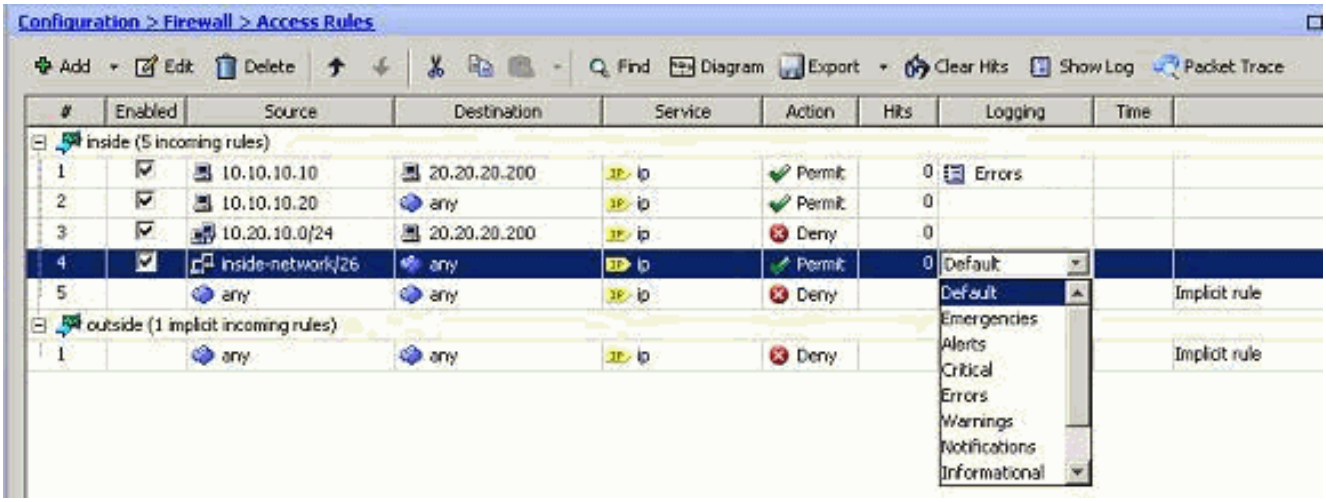
2. Метка выбора опция *Enable logging* и задает требуемый уровень важности. *Затем нажмите кнопку*



OK. **Примечание:** Путем нажатия *опций More* раскрывают вкладку, вы видите *опцию Interval Регистрации*. Эта опция выделена только, когда отмечена вышеупомянутая опция *Enable Logging*. Значение по умолчанию этого таймера составляет 300 секунд. Эта установка полезна в определении значения таймаута для статистики потока, которая

будет удалена, когда там не идет ни в какое сравнение с тем правилом доступа. Если существуют какие-либо соответствия, то ASA ждет до Интервала времени Регистрации и передает это к системному журналу.

3. Модификации показывают здесь. Также можно дважды нажать поле *Logging* определенного правила доступа и установить уровень важности там.



Примечание: Этот другой способ определения *Уровня регистрации* в той же области *Access Rules* двойным нажатием (клавиши) действительно работает для только вручную созданных записей правила доступа, но не к Неявным Правилам.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Конфигурации

Эти конфигурации используются в данном документе:

Cisco ASA

```
: Saved
:
ASA Version 8.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/1
 nameif outside
```

```
 security-level 0
 ip address 209.165.201.2 255.255.255.0
!
interface Ethernet0/2
 nameif inside
 security-level 100
 ip address 10.78.177.11 255.255.255.192
!
!!--- Output Suppressed ! access-list inside_access_in
extended permit ip host 10.10.10.10 host 20.20.20.200
log errors access-list inside_access_in extended permit
ip host 10.10.10.20 any access-list inside_access_in
extended deny ip 10.20.10.0 255.255.255.0 host
20.20.20.200 access-list inside_access_in extended
permit ip 10.78.177.0 255.255.255.192 any log
emergencies pager lines 24 logging enable logging list
user-auth-syslog level warnings class auth logging list
TCP-conn-syslog message 302013-302018 logging list
syslog-sev-error level errors logging list vpnclient-
errors level errors class vpnc logging list vpnclient-
errors level errors class ssl logging buffered user-
auth-syslog logging mail alerts logging from-address
test123@example.com logging recipient-address
monitorsyslog@example.com level errors logging queue
1024 logging host inside 172.16.11.100 logging ftp-
bufferwrap logging ftp-server 172.16.18.10 syslog
testuser **** logging permit-hostdown no logging message
302015 no logging message 302016 logging rate-limit 600
86400 level 7 mtu outside 1500 mtu inside 1500 icmp
unreachable rate-limit 1 burst-size 1 asdm image
disk0:/asdm-623.bin asdm history enable arp timeout
14400 ! !--- Output Suppressed ! timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225
1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout sip-provisional-media 0:02:00
uauth 0:05:00 absolute timeout TCP-proxy-reassembly
0:01:00 dynamic-access-policy-record DfltAccessPolicy !
!--- Output Suppressed ! ! telnet timeout 5 ssh timeout
5 console timeout 0 threat-detection basic-threat
threat-detection statistics access-list no threat-
detection statistics TCP-intercept ! !--- Output
Suppressed ! username test password /FzQ9W6s1KjC0YQ7
encrypted privilege 15 ! ! class-map inspection_default
match default-inspection-traffic ! ! policy-map type
inspect dns preset_dns_map parameters message-length
maximum 512 policy-map global_policy class
inspection_default inspect dns preset_dns_map inspect
ftp inspect h323 h225 inspect h323 ras inspect netbios
inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc inspect tftp inspect sip
inspect xdmcp ! service-policy global_policy global
smtp-server 172.18.10.20 prompt hostname context
Cryptochecksum:ad941fe5a2bbea3d477c03521e931cf4 : end
```

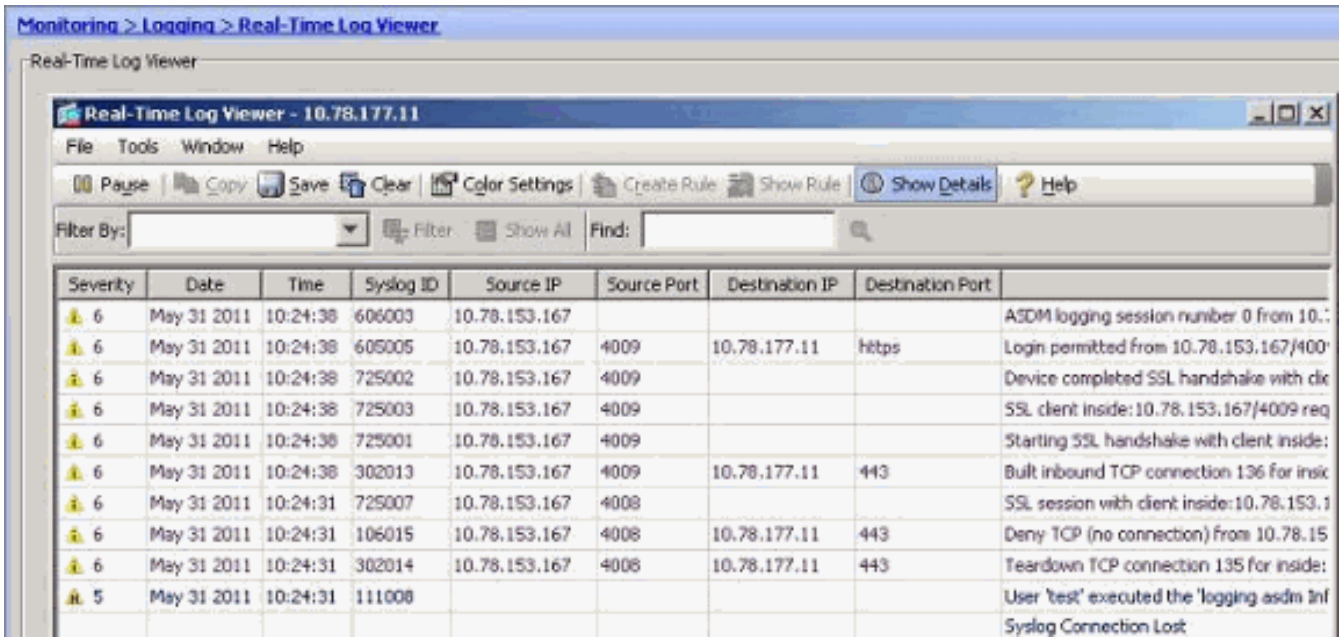
Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает

определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- Можно просмотреть системные журналы от ASDM. Выберите **Monitoring> Logging> Real Time Log Viewer**. Пример вывода приведен ниже:



Устранение неполадок

Проблема: Потерянное соединение - завершенное соединение системного журнала-

Эта ошибка получена при попытке включить регистрацию ASDM в Информационной панели Устройства для любого из контекстов.

```
"Connection Lost -- Syslog Connection Terminated --"
```

Когда ASDM используется для соединения непосредственно с контекстом администратора, и регистрация ADSM отключена там, затем переключитесь к подконтексту и включите регистрацию ASDM. Ошибки получены, но сообщения системного журнала достигают прекрасный к серверу системного журнала.

Решение

Это - известное поведение с Cisco ASDM и задокументированный в идентификатор ошибки Cisco CSCsd10699 (только зарегистрированные клиенты). Как обходной путь, включите регистрацию asdm, когда вошел в контекст администратора.

Не может просмотреть журналы реального времени на Cisco ASDM

Проблема - то, что журналы реального времени не могут быть просмотрены на ASDM. Как это настроено?

Решение

Настройте следование Cisco ASA:

```
ciscoasa(config)#logging monitor 6 ciscoasa(config)#terminal monitor ciscoasa(config)#logging on
ciscoasa(config)#logging trap 6
```

Дополнительные сведения

- Поддержка устройств адаптивной защиты Cisco ASA серии 5500
- Cisco Systems – техническая поддержка и документация