PIX/ASA: Проверка подлинности Kerberos и Группы серверов авторизации LDAP для Пользователей VPN-клиента через Пример ASDM/КОНФИГУРАЦИИ ИНТЕРФЕЙСА КОМАНДОЙ СТРОКИ

Содержание

Введение

В данном документе описано, как использовать диспетчер адаптивного устройства обеспечения безопасности (ASDM) для конфигурации аутентификации Kerberos и групп серверов авторизации LDAP на устройстве безопасности Cisco PIX серии 500. В данном примере группы серверов используются политикой группы VPN-туннеля, чтобы аутентифицировать и авторизовать входящих пользователей.

Предварительные условия

Требования

Этот документ предполагает, что PIX полностью в рабочем состоянии и настроен, чтобы позволить ASDM изменять конфигурацию.

Примечание: Дополнительные сведения о том, как разрешить конфигурацию PIX с помощью

ASDM, см. в разделе Разрешение HTTPS-доступа для ASDM.

Используемые компоненты

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

- ПО Cisco PIX Security Appliance версии 7.x и более поздних версий
- Cisco ASDM версии 5.x и более поздних версий

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.

Родственные продукты

Данную конфигурацию также можно использовать с адаптивным устройством обеспечения безопасности Cisco ASA версии 7.x.

Условные обозначения

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

Общие сведения

Не все возможные способы аутентификации и авторизации доступные в ПО PIX/ASA 7.x поддерживаются при взаимодействии с пользователями VPN. В следующей таблице отображены доступные способы для пользователей VPN:

	ЛОКАЛЬНЫЙ	RADIUS	TACACS +	SDI	NT	Kerberos	LDAP
Authentication	Да	Да	Да	Да	Да	Да	Нет
Authorization	Да	Да	Нет	Нет	Нет	Нет	Да

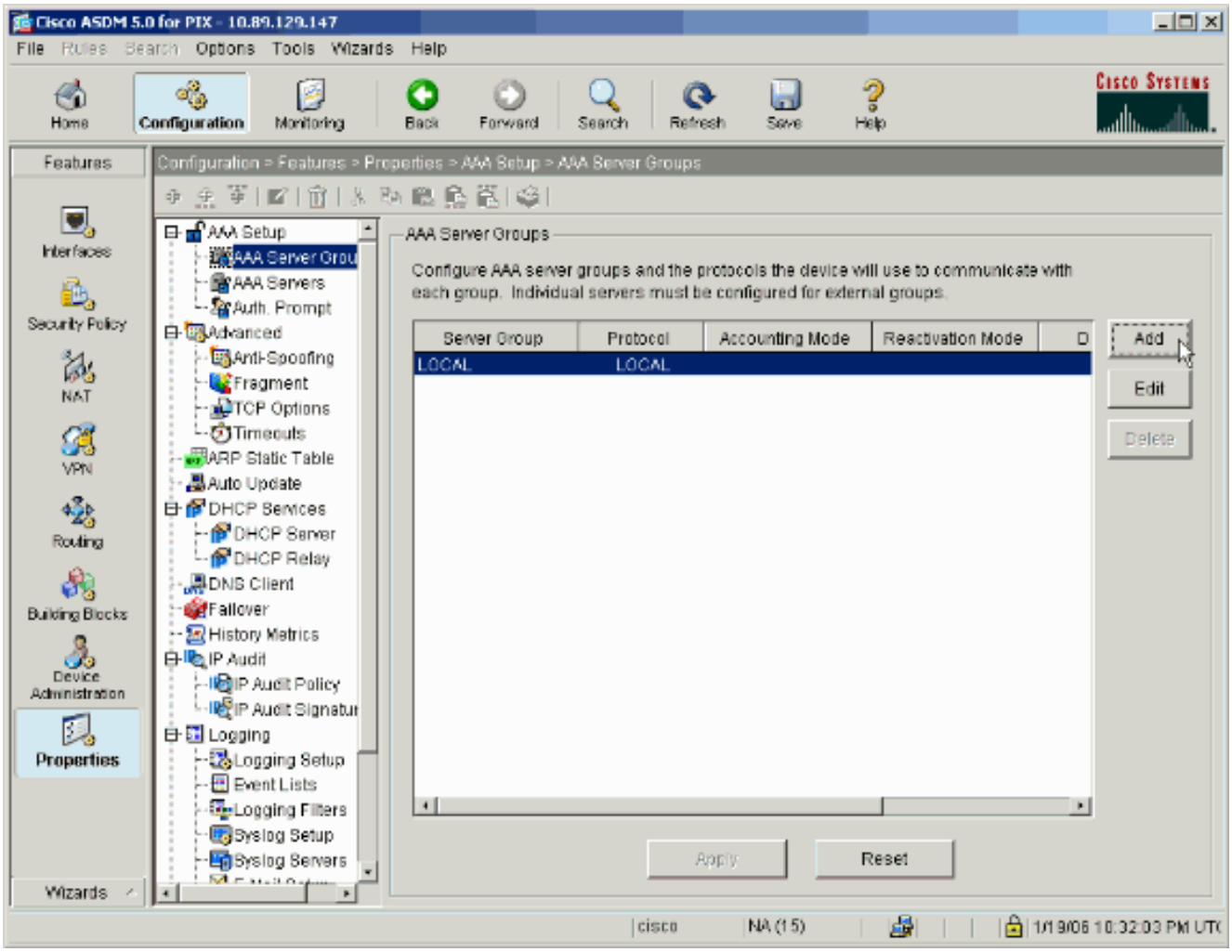
Примечание: В данном примере Kerberos используется для аутентификации, а LDAP – для авторизации пользователей VPN.

Настройка аутентификации и авторизации для пользователей VPN с помощью ASDM

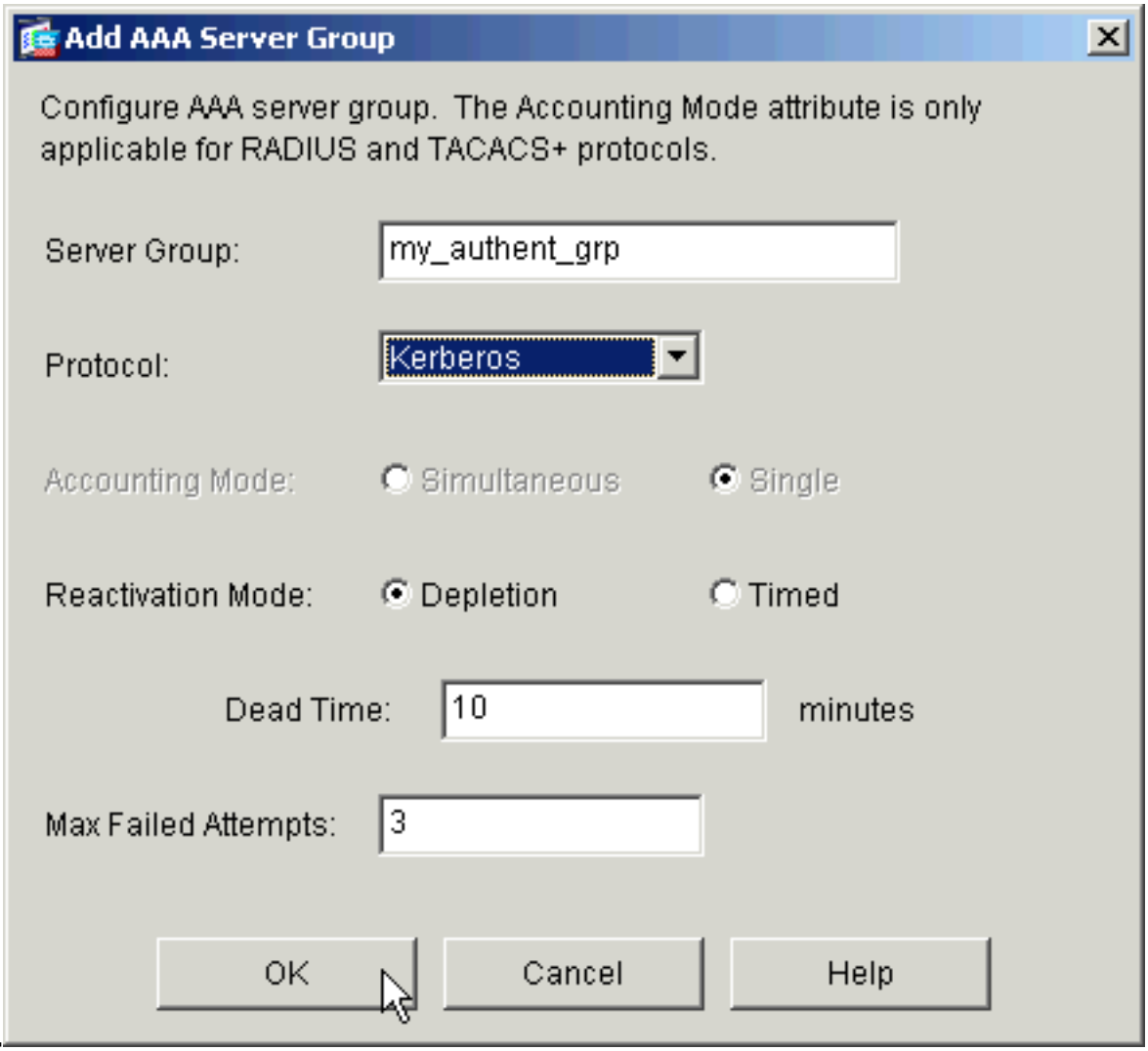
Настройка серверов аутентификации и авторизации

Выполните эти шаги для настройки групп серверов проверки подлинности и авторизация для пользователей VPN через ASDM.

1. **Выберите Configuration > Properties > AAA Setup > AAA Server Groups и нажмите Add.**

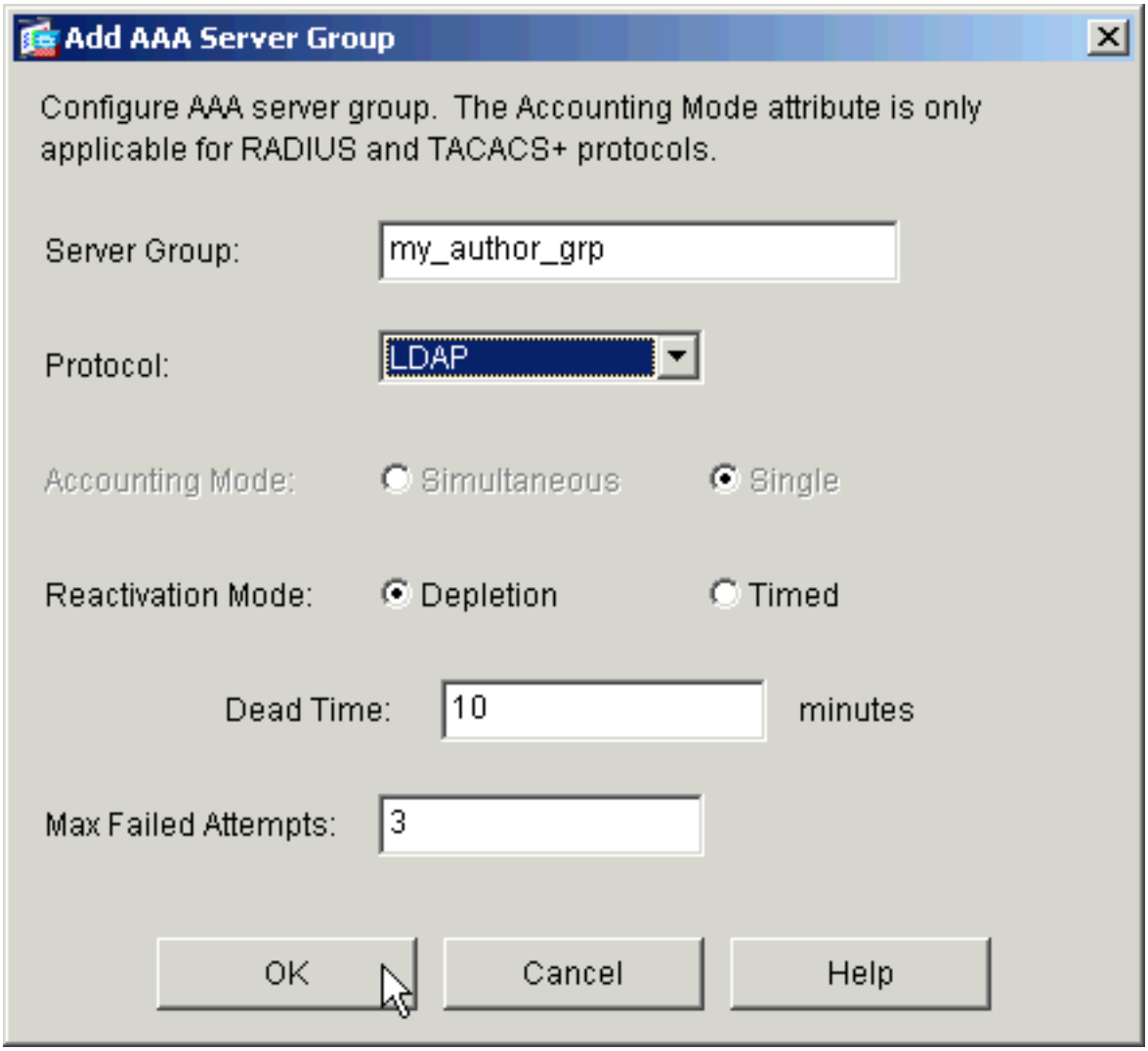


2. Определите имя для новой группы серверов аутентификации и выберите протокол.Параметр Accounting Mode используется только для RADIUS и TACACS+. **Закончив все действия, нажмите кнопку**

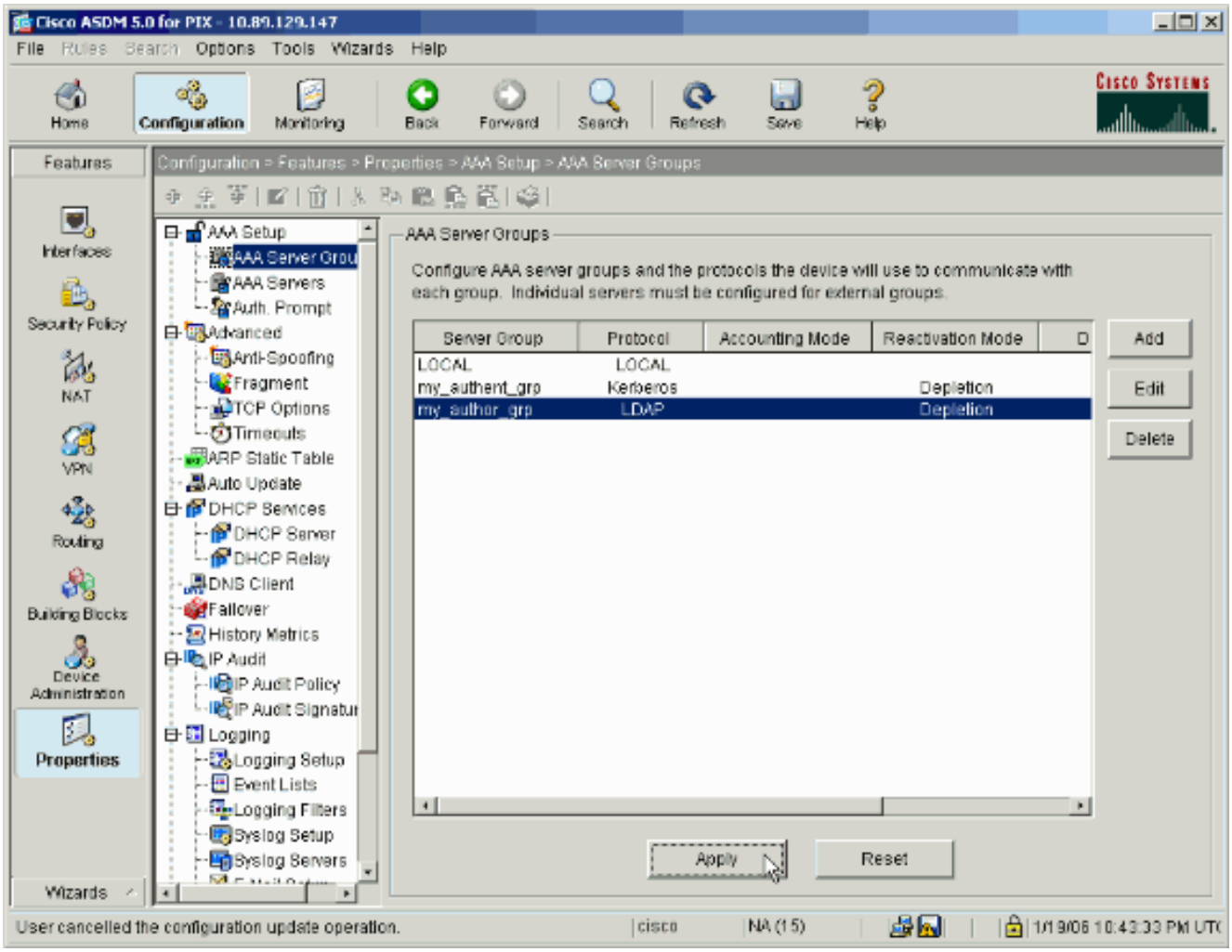


OK.

3. Повторите шаги 1 и 2 для создания новой группы серверов авторизации.

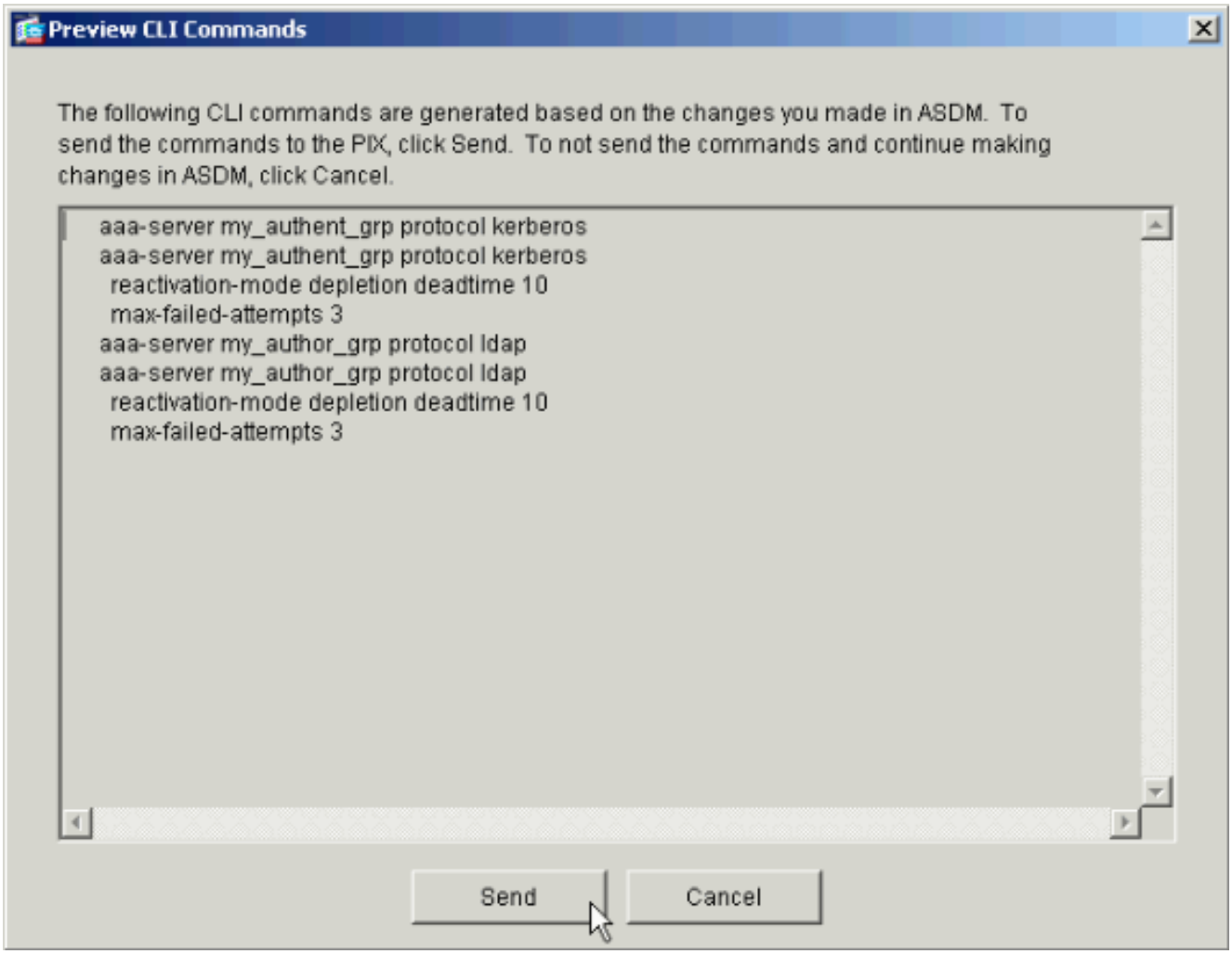


4. Нажмите **Apply** для передачи изменений к устройству.



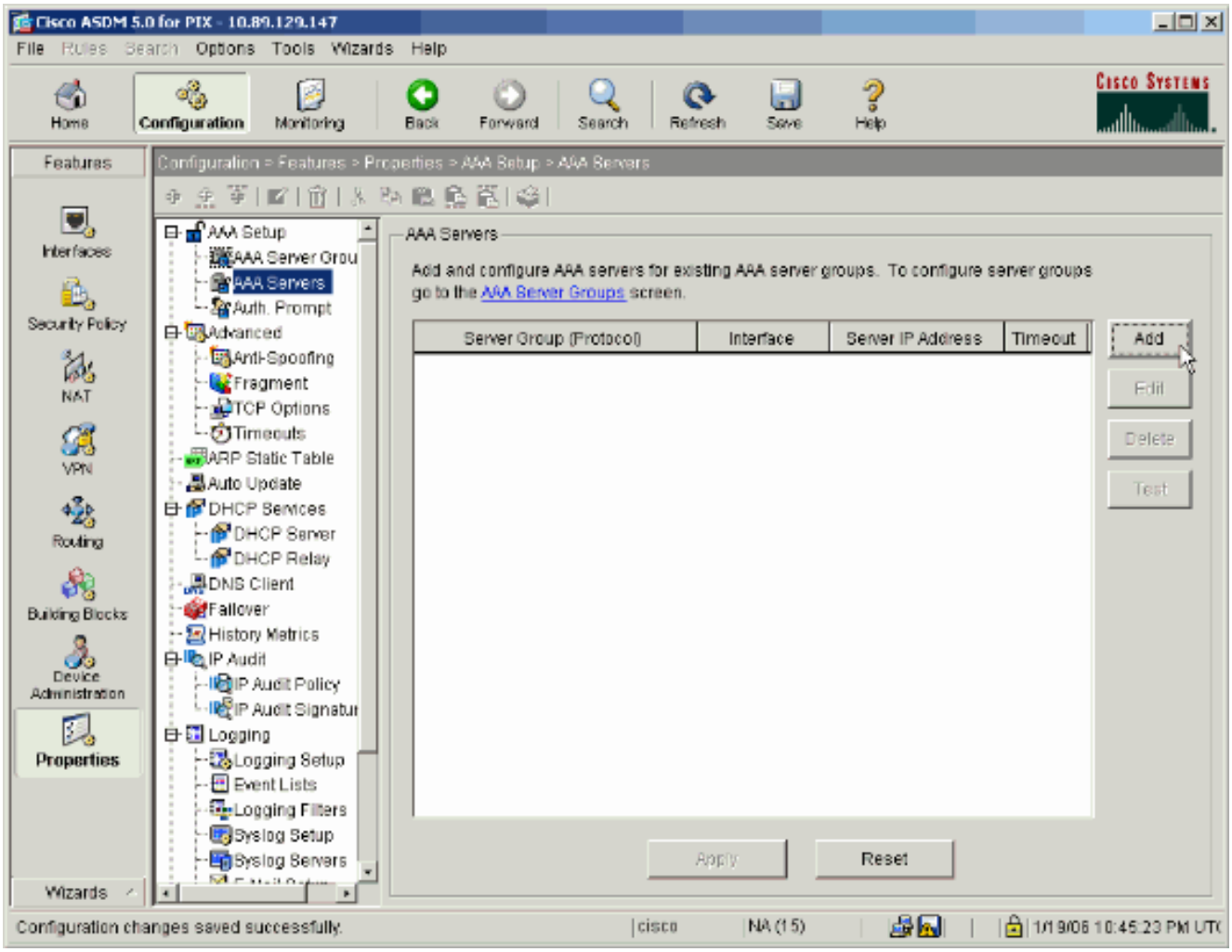
Если устройство уже настроено, в нем предварительно можно просмотреть команды, которые добавляются к текущей конфигурации.

5. Нажмите **Send** для передачи команд к устройству.

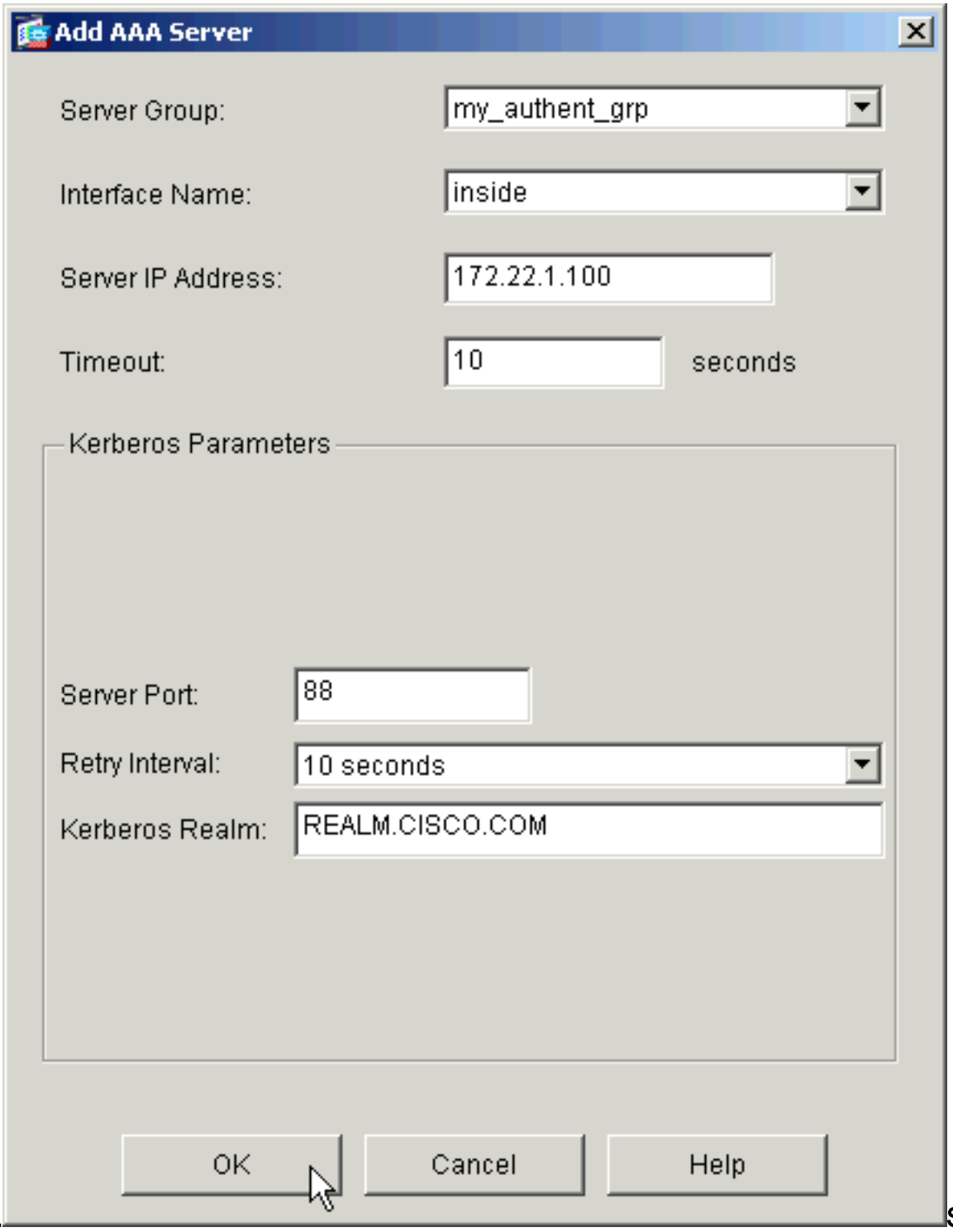


Новые обновленные группы серверов необходимо заполнить серверами аутентификации и авторизации.

6. **Выберите Configuration > Properties > AAA Setup > AAA Server Groups и нажмите Add.**

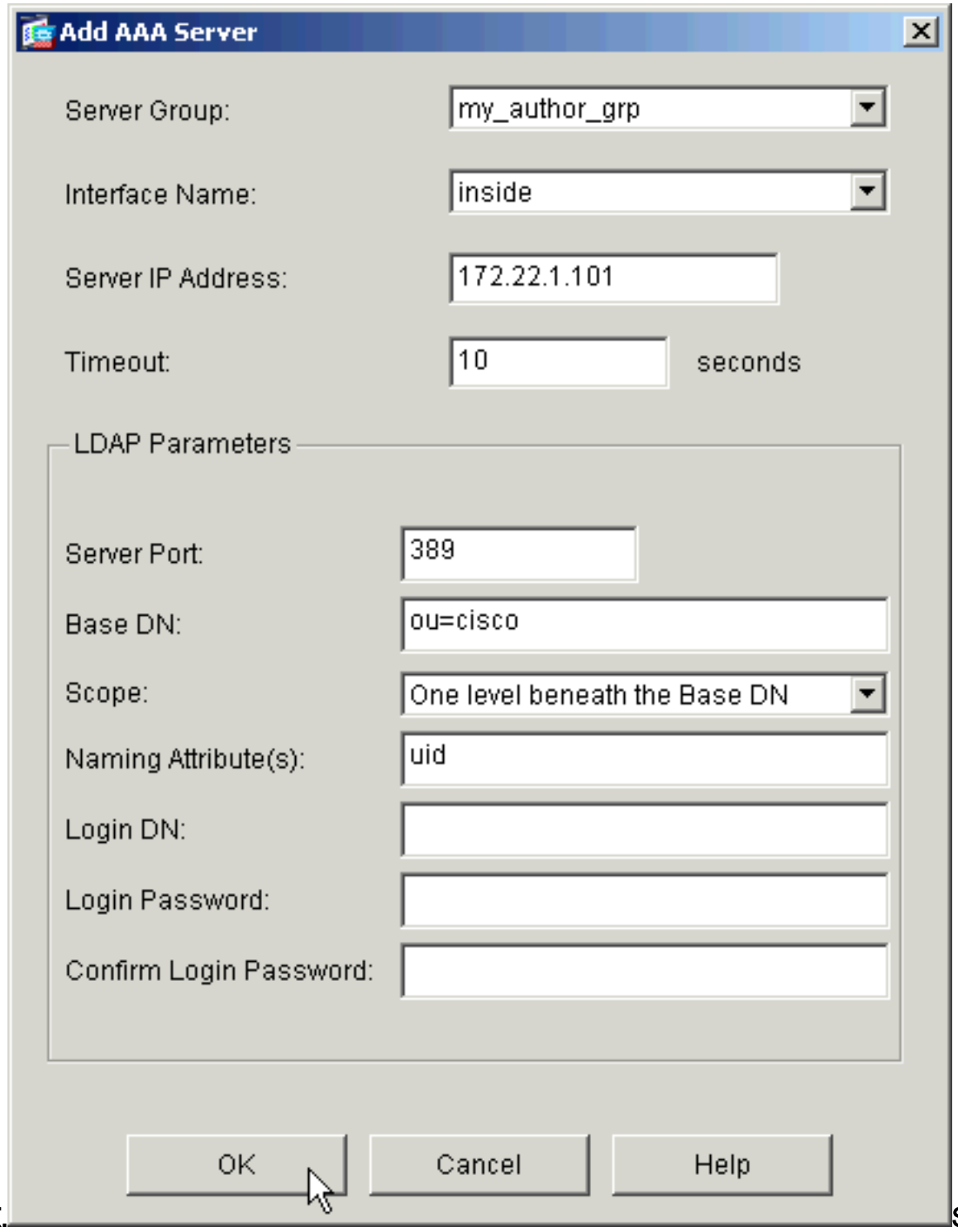


7. Настройте сервер аутентификации. **Закончив все действия, нажмите кнопку**



OK. **Server Group – выберите группу серверов аутентификации, настроенную в шаге 2.Interface Name – выберите интерфейс, на котором находится сервер.Server IP Address – указывает IP-адрес сервера аутентификации.Timeout – указывает максимальное время ожидания ответа с сервера в секундах.Параметры Kerberos:Server Port – 88 – это стандартный порт для Kerberos.Retry Interval – выберите необходимый интервал повтора.Kerberos Realm – введите имя области Kerberos.** Имя домена Windows зачастую пишется заглавными буквами.

8. Настройте сервер авторизации. **По окончании нажмите**



OK.Server Group – выберите группу серверов авторизации, настроенную в шаге 3.Interface Name – выберите интерфейс, на котором находится сервер.Server IP Address – указывает IP-адрес сервера авторизации.Timeout – указывает максимальное время ожидания ответа с сервера в секундах.Параметры LDAP:Server Port – 389 – это порт по умолчанию для LDAP.Base DN – введите местоположение в иерархии LDAP, где сервер начнет поиск, как только получит запрос об авторизации.Scope – выберите пространство, где серверу необходимо начать поиск иерархии LDAP, как только он получит запрос об авторизации.Naming Attribute(s) – введите атрибут(ы) относительного отличительного имени, по которым были определены записи на сервере LDAP. Общими атрибутами наименования являются общее имя (cn) и идентификатор пользователя (uid).**Login DN – для некоторых серверов LDAP, включая сервер активных каталогов Microsoft, необходимо установить подтверждение связи с помощью аутентифицированного связывания до того, как принять запросы для других операций LDAP.** С помощью поля

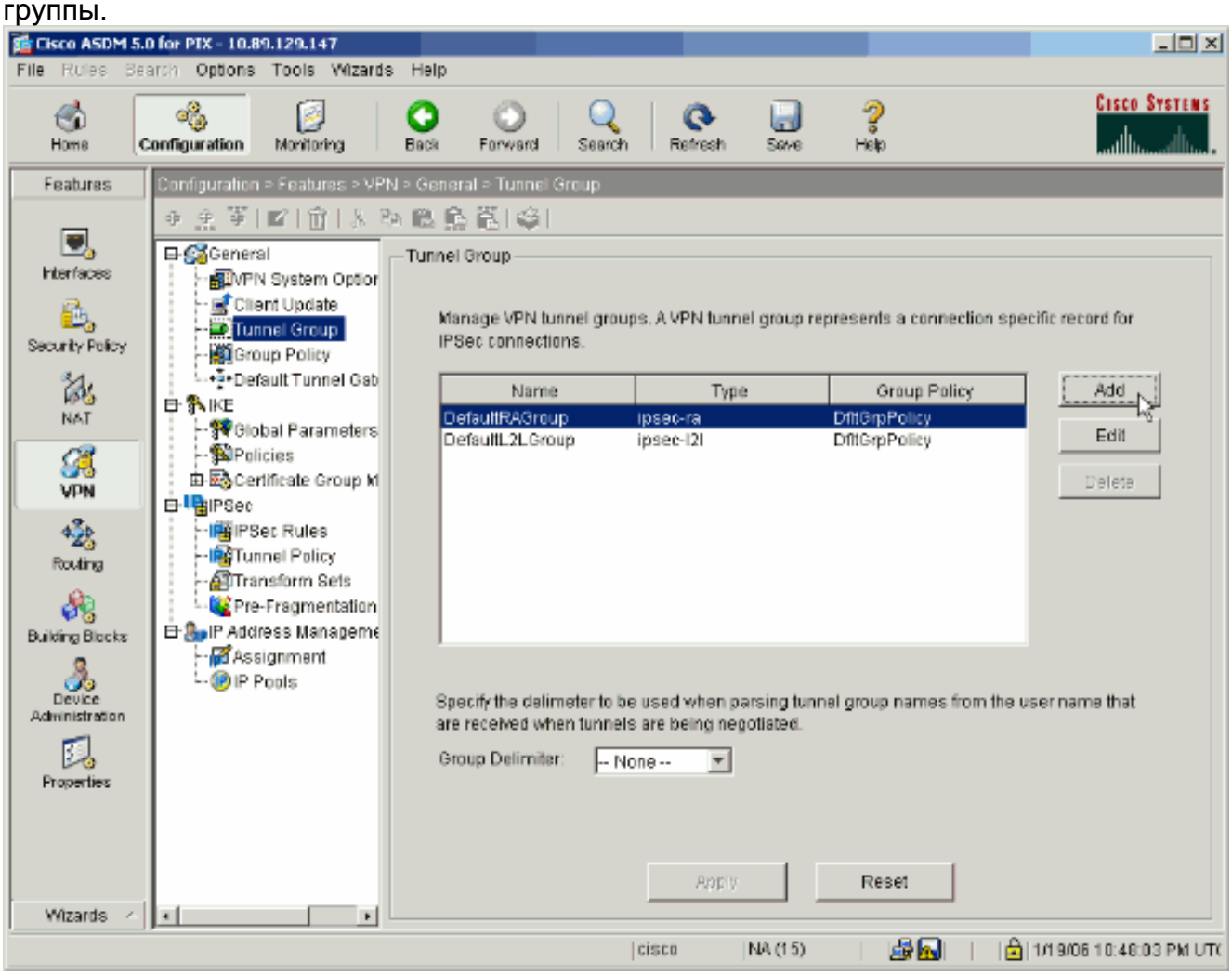
Login DN можно определить характеристики аутентификации устройства, которые должны соответствовать характеристикам пользователя с полномочиями администрирования. Например, cn=administrator. Для анонимного доступа оставьте данное поле пустым.**Login Password – введите пароль для Login DN.Confirm Login Password – подтвердите пароль для Login DN.**

9. Нажмите **Apply** для передачи изменений к устройству после того, как добавлены все серверы проверки подлинности и авторизация.Если PIX уже настроен, в нем предварительно можно просмотреть команды, которые добавляются к текущей конфигурации.
10. Нажмите **Send** для передачи команд к устройству.

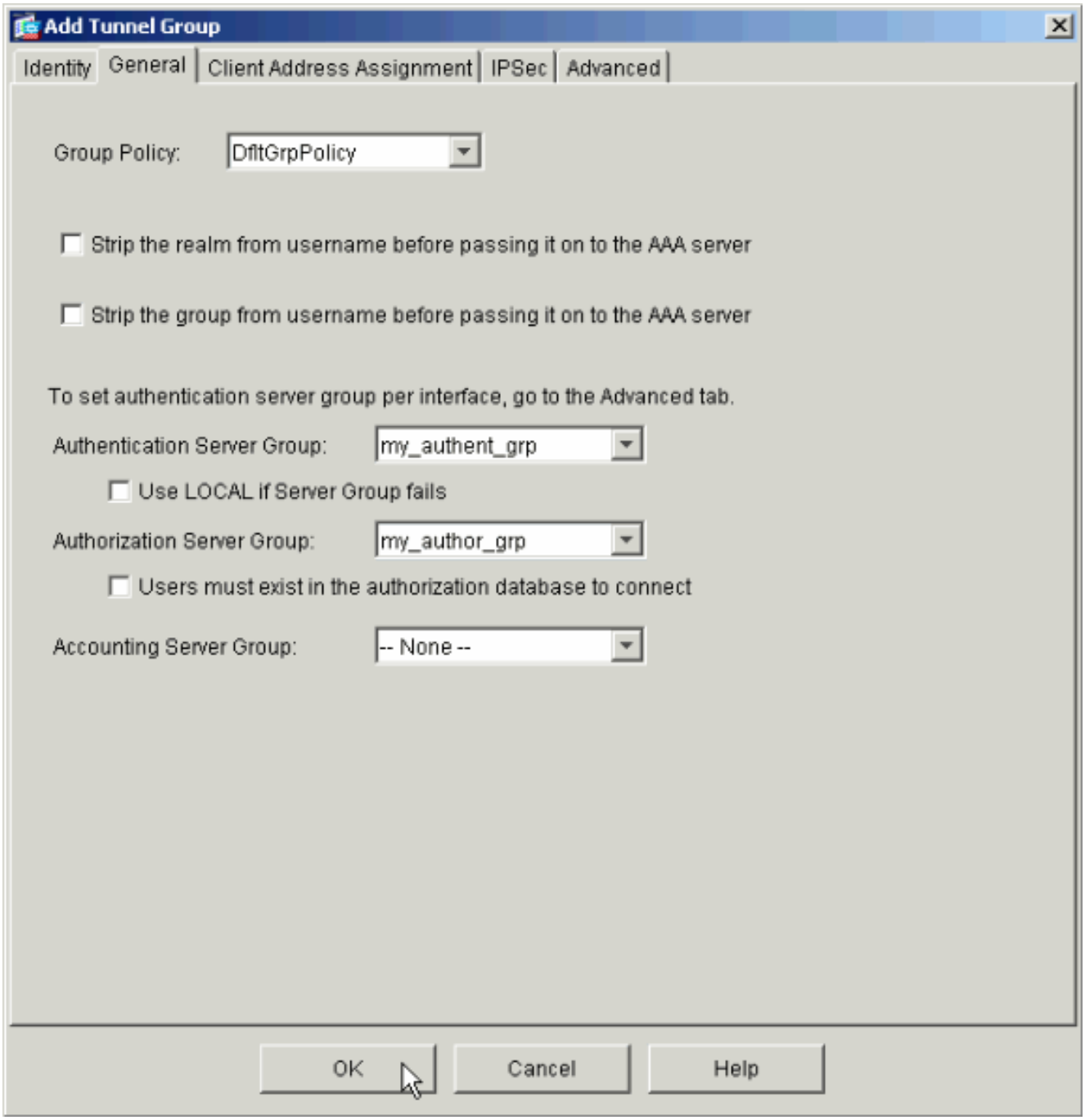
Конфигурация туннельной группы VPN для аутентификации и авторизации

Выполните эти шаги для добавления групп серверов, которые вы просто настроили группе VPN-туннеля.

1. Выберите **Configuration> VPN> Tunnel Group** и **нажмите Add**, чтобы создать новую туннельную группу или **Отредактировать** для изменения существующей группы.



2. Откроется окно с вкладкой General. Выберите ранее настроенную группу серверов.



3. *Дополнительно:* Настройте оставшиеся параметры на других вкладках при добавлении новой туннельной группы.
4. **Закончив все действия, нажмите кнопку OK.**
5. Нажмите **Apply** для передачи изменений к устройству после того, как конфигурация туннельной группы завершена.Если PIX уже настроен, в нем предварительно можно просмотреть команды, которые добавляются к текущей конфигурации.
6. Нажмите **Send** для передачи команд к устройству.

Настройка аутентификации и авторизации для пользователей VPN с помощью CLI

Конфигурация CLI эквивалентна группе серверов аутентификации и авторизации для пользователей VPN.

Конфигурация устройства обеспечения безопасности

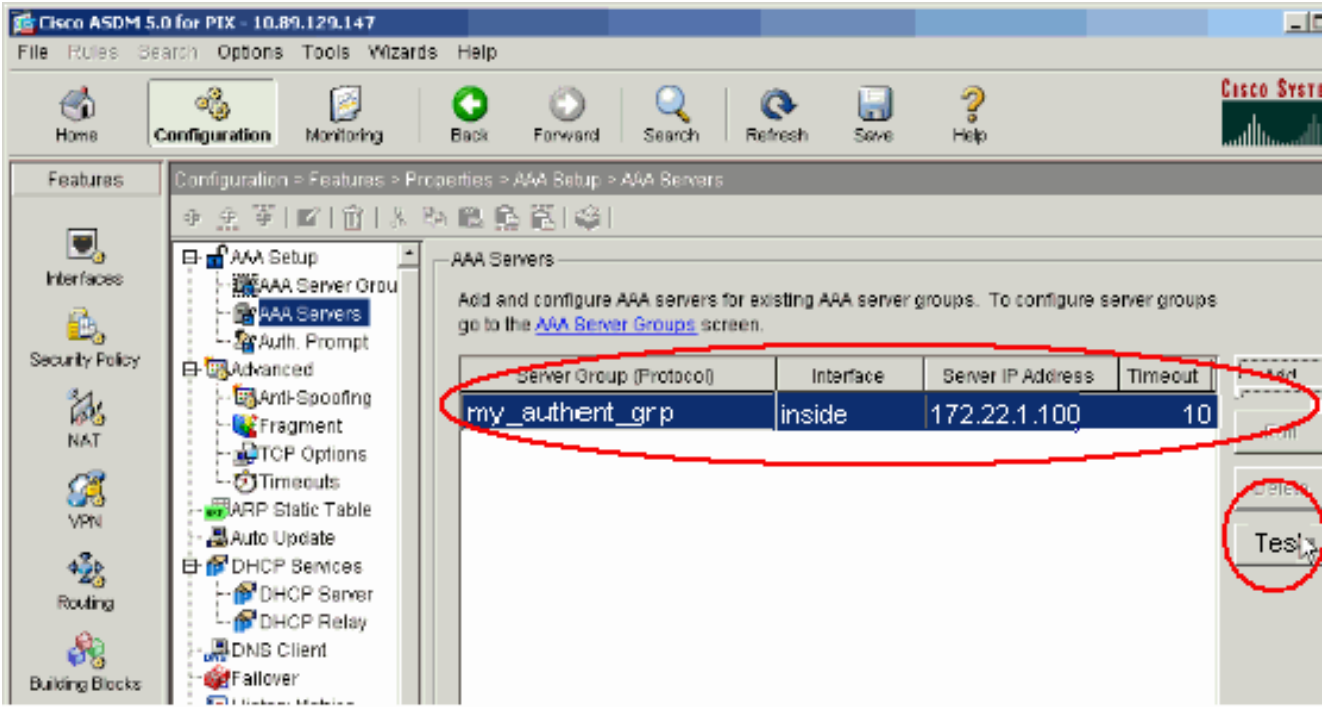
CLI

```
pixfirewall#show run : Saved : PIX Version 7.2(2) !
hostname pixfirewall domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface Ethernet0 shutdown no nameif no security-level
no ip address ! interface Ethernet1 nameif inside
security-level 100 ip address 172.22.1.105 255.255.255.0
! !--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid pager lines 24 mtu
inside 1500 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image flash:/asdm-522.bin !--- Output
is suppressed. aaa-server my_authent_grp protocol
kerberos aaa-server my_authent_grp host 172.22.1.100
kerberos-realm REALM.CISCO.COM aaa-server my_author_grp
protocol ldap aaa-server my_author_grp host 172.22.1.101
ldap-base-dn ou=cisco ldap-scope onelevel ldap-naming-
attribute uid http server enable http 0.0.0.0 0.0.0.0
inside no snmp-server location no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart tunnel-group DefaultRAGroup general-
attributes authentication-server-group my_authent_grp
authorization-server-group my_author_grp ! !--- Output
is suppressed.
```

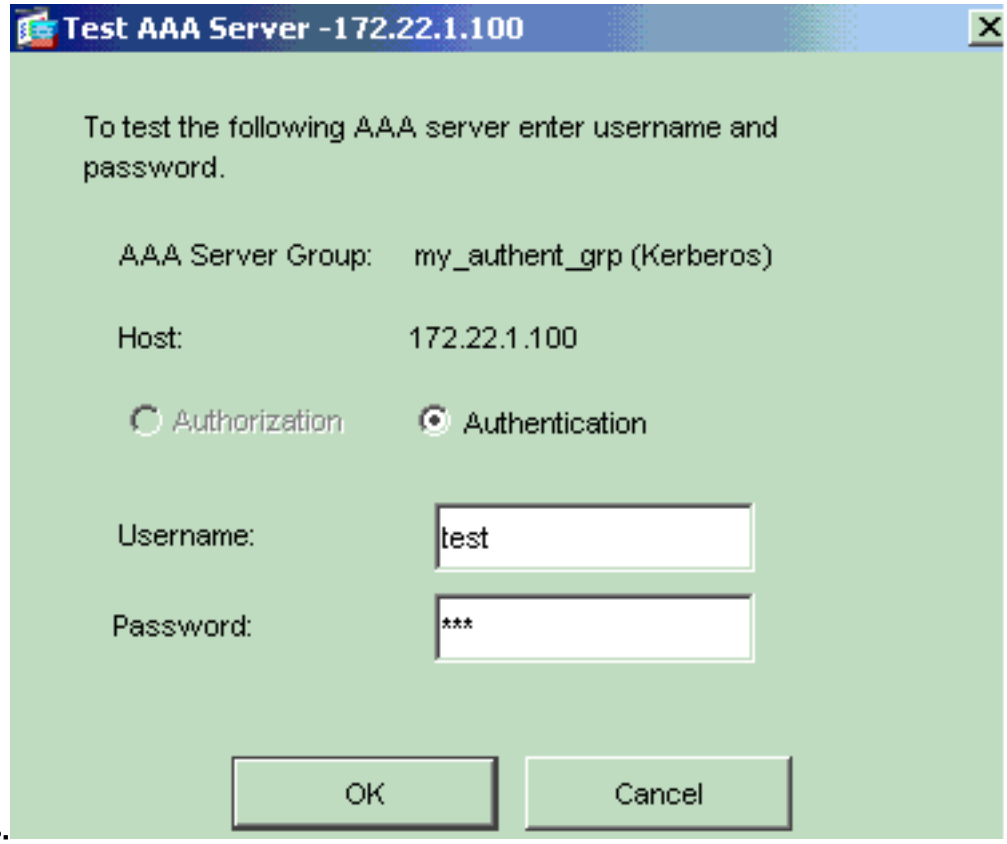
Проверка

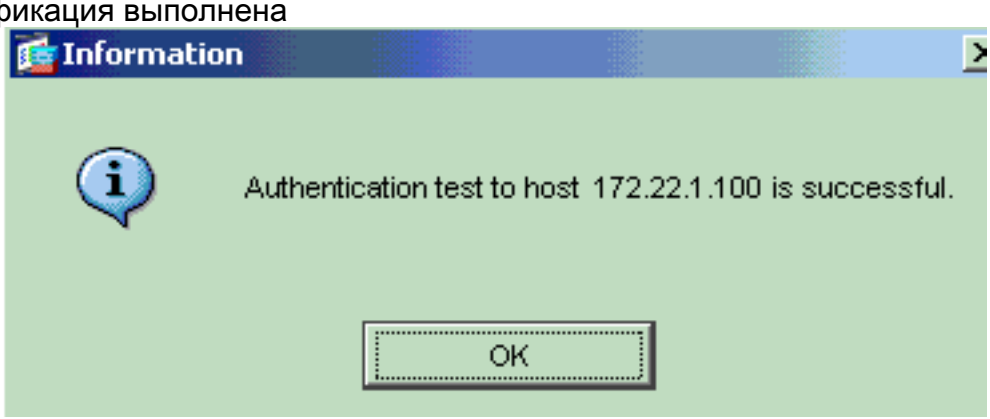
Чтобы проверить аутентификацию пользователей между серверами PIX/ASA и AAA, выполните следующие действия:

1. **Выберите Configuration > Properties > AAA Setup > AAA Server Groups и выберите группу серверов (my_authent_grp).** Затем нажмите **Test** для проверки учетных данных пользователя.



2. Предоставьте имя пользователя и пароль (например имя пользователя: test и пароль: **test) и нажмите OK, чтобы**

проверить. 

3. Аутентификация выполнена успешно. 

Устранение неполадок

1. Одной из наиболее частых причин ошибки аутентификации является потеря времени. Убедитесь, что часы на PIX или ASA и сервере конфигурации синхронизированы.Когда аутентификация отказывает из-за Расфазировки тактовых сигналов, можно получить это сообщение об ошибках: `:- ERROR: Authentication Rejected: Clock skew greater than 300 seconds.`. Кроме того, это сообщение журнала появляется:`%PIX|ASA-3-113020: Kerberos error : Clock skew with server ip_address greater than 300 seconds` `iP-` IP-адрес сервера Kerberos.Это сообщение отображено, когда аутентификация для IPSec или пользователя WebVPN через сервер Kerberos отказывает, потому что часы на устройстве безопасности и сервер составляют больше чем пять минут (300 секунд) независимо. Когда это происходит, попытка подключения отклонена.Для решения этого вопроса синхронизируйте часы на устройстве безопасности и сервере Kerberos.
2. Предварительная проверка подлинности на Active Directory (AD) должна быть отключена, или это может привести к ошибке аутентификации пользователя.
3. Пользователи VPN-клиента неспособны аутентифицироваться против Сервера

сертификатов Microsoft. Это сообщение об ошибках появляется:`"Error processing payload" (Error 14)` Для решения этого вопроса снимите флажок **с не, требуют kerberose** флажка **процедур, предшествующих аутентификации** на сервере проверки подлинности.

Дополнительные сведения

- Конфигурация серверов AAA и локальной базы данных
- Поддержка устройств адаптивной безопасности Cisco ASA серии 5500
- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация