Практическое занятие № 20

Настройка средств криптографической защиты сетевого трафика стандартного протокола ipSec в операционной системе MS Windows

Цель: Научиться защищать сетевой трафик средствами шифрования данных через ipSec (internet protocol security).

ПЗ № 20 Настройка средств криптографической защиты сетевого трафика стандартного протокола ipSec в операционной системе Windows.

Содержание:

Теоретическая часть

Методы проверки подлинности

Практическая часть

Для управления политикой безопасности **IPSec** с консоли управления Microsoft, выполните следующие действия. Нажмите кнопку **Пуск**, выберите команду **Выполнить**, введите **MMC** и нажмите кнопку **OK**.





В меню Консоль выберите команду Добавить или удалить оснастку, затем нажмите кнопку Добавить.





Выберите Управление политикой безопасности IP и нажмите кнопку Добавить.

оавить или удалит	B OCHACTRY	
золированная осна	Добавить изолированную оснастку	?
	Доступные изолированные оснастки:	
используется для т	Оснастка	Поставь 🔺
О <u>с</u> настки:	🙆 Службы компонентов	Microsof
	💽 Ссылка на веб-ресурс	Microsof
	🖓 Телефония	Microsof
	👜 Удаленные рабочие столы	Microsof
	😽 Управление дисками	Програм
	📃 Управление компьютером	Microsof
	😞 Управление политикой безопасности IP	Microsof-
	🔬 Управление съемными носителями	Microsof
	🖧 ประวาทสาวอานานข้าง สาวหาวาร (1/M)	Minrosof
	г Описание	
	A	
-0.0000000	Администрирование резопасностью протокола н Управление политиками IPSEC для безопасного	соединения с
описание	другими компьютерами.	
		-
	Добавить	<u>З</u> акрыты



Выберите компьютер, политиками **IPSec** которого требуется управлять.

ибор компьютера или домена	? >
Выберите управляемый компьютер или домен При сохранении консоли информация о расположении будет тоже сохранена	Ē
• Докальный компьютер	
Компьютер, на котором выполняется эта консоль	
C Домен с Active Directory, членом которого является этот компьютер	
🔿 Другой домен с Active Directory (его DNS-имя или IP-адрес):	
с другод компьютер.	
Tosob	
	_
< <u>Н</u> азад Готово	Отмена



Чтобы	Выполните следующее действие
Управлять только компьютером, на котором выполняется консоль	Выберите Локальный компьютер
Управлять политиками и IPSec для любого члена домена	Выберите Домен с Active Directory, членом которого является этот компьютер.
Управлять политиками IPSec для домена, членом которого компьютер, на котором выполняется консоль, не является	Выберите Другой домен с Active Directory.
Управлять удаленным компьютером	Выберите Другой компьютер



nom		112	<u>nmi</u>
UEIII	Кая		

золированная осна 1спользиется для і	астка Расширения	
1спользиется для і	п асширения [
TO T	добавления или удаления и	ізолированной оснастки.
Існастии		
<u>onderior</u>	Сорень консоли	
😞 Политики беза	опасности IP на "Локальны	й компьютер"
0		
Описание	ue безопасностью протоко	aa IP (IPSEC)
Описание Администрировані Управление полит	ие безопасностью протоко. иками IPSEC для безопасн	ла IP (IPSEC).
Описание Администрировані Управление полит другими компьюте	ие безопасностью протоко. иками IPSEC для безопасн зрами.	ла IP (IPSEC). юго соединения с
Описание Администрирован Управление полит другими компьюте	ие безопасностью протоко. иками IPSEC для безопасн грами.	ла IP (IPSEC).
Описание Администрировані Управление полит другими компьюте	ие безопасностью протоко. иками IPSEC для безопасн грами.	ла IP (IPSEC). юго соединения с
Описание Администрировані Управление полит другими компьюте	ие безопасностью протоко. иками IPSEC для безопасн грами.	ла IP (IPSEC). Юго соединения с
Описание Администрировані Управление полит другими компьюте Побавить	ие безопасностью протоко. иками IPSEC для безопасн арами.	ла IP (IPSEC). юго соединения с
Описание Администрировані Управление полит другими компьюте Добавить…	ие безопасностью протоко. чками IPSEC для безопасн зрами. <u>У</u> далить <u>О</u> пр	ла IP (IPSEC). юго соединения с
Описание Администрирован Управление полит другими компьюте Добавить	ие безопасностью протоко. иками IPSEC для безопасн арами. удалить	ла IP (IPSEC). юго соединения с

Сделать двойной клик на Политики безопасности на "Локальный компьютер"



im Консоль2	
Консоль Действие Вид Избранное Окно Справка	
← → 🔃 🕄 😫 🏦 🄁	
📕 Корень консоли	
🔄 Корень консоли Имя	
🔜 😓 Политики безопаснос 🛛 🕷 Политики безопасности IP на "Локальный компьютер"	

Выбрать свойства "Сервер безопасности"



Корень консоли	Имя 🛆	Описание
🜏 Политики безопаснос	🛍 Сервер (Запрос без 🛍 Клиент (Ответ толь	Всегда требовать использ . Установить связь (небезо
	Сервер безопасност	Назначить
		Вс <u>е</u> задачи
		<u>У</u> далить
		Переименовать
		Сво <u>й</u> ства
	•	Справка

Во вкладке Общие указать настройки:

Общие свойства политики безопасности IP Имя: Сервер безопасности (Требуется безопасность) Описание: Всегда требовать использования средств безопасности Kerberos для IP трафика. Не разрешать небезопасную связь с ненадежными клиентами.] Провердть политику на наличие изменений каждые: 180 мин. Выполните обмен ключами, используя дополнительные параметры	Травила	Общие					
<u>И</u> мя: Сервер безопасности (Требуется безопасность) <u>О</u> писание: Всегда требовать использования средств безопасности Kerberos для IP трафика. Не разрешать небезопасную связь с ненадежными клиентами.] Провер <u>я</u> ть политику на наличие изменений каждые: 180 мин. Выполните обмен ключами, используя дополнительные параметры		Общие с	войства по	олитики безс	опасности IP		
Сервер безопасности (Требуется безопасность) Описание: Всегда требовать использования средств безопасности Kerberos для IP трафика. Не разрешать небезопасную связь с ненадежными клиентами.] Провердть политику на наличие изменений каждые: 180 мин. Выполните обмен ключами, используя дополнительные параметры: Параметры	<u>И</u> мя:						_
 Описание: Всегда требовать использования средств безопасности Kerberos ▲ для IP трафика. Не разрешать небезопасную связь с ненадежными клиентами. Провердть политику на наличие изменений каждые: 180 мин. Выполните обмен ключами, используя дополнительные параметры: араметры 	Сервер	безопасно	сти (Требу	ется безопа	сность)		
Всегда требовать использования средств безопасности Kerberos для IP трафика. Не разрешать небезопасную связь с ненадежными клиентами. Провердть политику на наличие изменений каждые: 180 мин. Выполните обмен ключами, используя дополнительные параметры: Параметры	Описани	1e:					
Провер <u>я</u> ть политику на наличие изменений каждые: 180 мин. Выполните обмен ключами, используя дополнительные параметры: <u>П</u> араметры	прсегда	TRODODDTL	LODOGLOOD				
Выполните обмен ключами, используя дополнительные параметры: Параметры	для IP т ненаде:	греооватв рафика. Не кными кли	использов е разрешат ентами.	ания средст ъ небезопас	в безопасности ную связь с	I Kelbelos	~
	для IP т ненаде: Провер <u>я</u> 180	треоовать рафика. Не кными кли ть политик мин.	использов е разрешат ентами. ку на налич	ания средст ъ небезопас ие изменени	в безопасности ную связь с ий каждые:	Reideros	-



Указать используемые методы шифрования данных

Параметры обмена ключами	? ×
🔲 Основной ключ безопасной <u>п</u> ересылки (PFS)	
	Методы безопасности при обмене ключами 🔋 🗙
480 <u>м</u> ин Проверять подлинность и создавать новый ключ через каж	Для защиты личных данных следует использовать указанные методы безопасности.
	М <u>е</u> тоды безопасности в порядке предпочтения:
Метопы	Тип Шифрование Целостность Г Добавить
	IKE 3DES SHA1 IKE 3DES MD5 С Изменить IKE DES SHA1 Н
	IKE DES MD5 - Удалить
МD5	Вверх
Алгоритм шифрования:	В <u>н</u> из
DES	
<u>Г</u> руппа Диффи-Хелмана:	
Низкая (1)	
ОК Отмена	ИК Отмена

После этого необходимо определить правила и фильтры **ipSec** Для создания новых правил или изменения старых необходимо выбрать вкладку **Правила** → **Список фильтров IP.**

зойства: Сервер безоп	асности (Требуется	6eaonacuorm)	?) (1	<mark>⊻ </mark> зойства: Из	зменить правило	
правила Орщие					Методы провер	жи подлинности
\$				Пар	аметры туннеля	Тип подключени
Правила без компьютеран	опасности для связи с ; чи	аругими		Спи	сок фильтров IP	Действие фильт
Правила безопасности	IP:			HH	Выбранный список IP сетевой трафика буде	-фильтров указывает, како т затронут этим правилом
Список фильтров IP	Действие фильтра	Методы пров	Ko			
🗹 Полный IP трафик	Требуется безопас	Kerberos	He			
🛛 Полный ІСМР тр	Разрешить	<отсутствует>	Hε	С <u>п</u> иски фи	ильтров IP:	
Динамический>	Отклик по умолчан	Kerberos	<н	Имя	COMPANY AND A DESCRIPTION	Описание
				ОПолн	ый ІСМР трафик	Сравнение всех ІСМР-пак
				• Полн	ый IP трафик	Сравнение всех IP-пакет(
				О Созд	ание списка IP-фильтр	
			-			
4	ł		>			
1	1		-			
Добавить Измени	ть Идалить	Использовать	мастер			
	or 1	0		1		

Полный ІР трафик - отфильтровывать весь трафик



Вкладка Действие фильтра. Выбрать один из предлагаемых действий фильтра:

ства: Изм	енить правило	?
	Методы провери	ки подлинности
Пара	метры туннеля	Тип подключения
Списс	к фильтров IP	Действие фильтра
X	Выбранное действие ф необходимость и спосо сетевых данных.	эильтра определяет об согласования защиты потока
lействия ф Има	ильтра:	Описание
O Sanpoc	безопасности (Возмож	кн Принимать небезопаснию с
О Разреш	ить	Разрешение прохождение н
• Требуе	гся безопасность	Принимать небезопасную с
• [Þ
	Изменить. Удал	ить Использовать мастер
Добавить		

Запрос безопасности - Принимать небезопасную связь, но требовать от клиентов применения методов доверия и безопасности. Будет поддерживаться небезопасная связь с ненадежными клиентами, если клиенты не выполнят требование безопасности;

Разрешить - Разрешение прохождения небезопасных ір-пакетов; Требуется безопасность -Принимать небезопасную связь, но всегда требовать от клиентов применение методов доверия и безопасности. Не будет поддерживаться связь с ненадежными клиентами.

Тип подключения - вкладка, на которой указывается тип сетевого подключения, на которое распространяется данное правило.

войства: Изменить правило	<u>?</u> ×
Методы проверки	и подлинности
Список фильтров IP	Действие фильтра 🔰
Параметры туннеля	Тип подключения
📏 Это правило применяет 🗐 🗐 выбранного типа.	ся только к подключениям
• Все сетевые подключения	
🗌 🔿 <u>Л</u> окальное сетевое подключение	9
🔘 Удаленный доступ	

Для пары компьютеров необходимо установить одинаковый способ проверки подлинности, чтобы избежать конфликтов.

Список филь	TOOB IP	Пействие фильтра	
Параметры т	инела	Деистрие филотра	
Методь образо приним безопа	иетоды проверки подли и проверки подлинности м устанавливаются дов компьютерами. Эти мет аются в процессе согла сности с другим компью	нности определяют, каким ерительные отношения годы предлагаются и асования политики этером.	
орядок предпочте Метод	ния методов проверки г Сведения	юдлинности: Добавить	
Kerberos		Изменить	
		<u> </u>	
		Вверх	
		В <u>н</u> из	



Пример разрешения связи по протоколу http 1) Нажать Добавить

войства: Сервер безопасности (Требует	гся безопасность)	<u>?</u> ×
Правила Общие		
Правила безопасности для связ компьютерами	и с другими	
Правила безопасности IP:		_
Список фильтров IP	Действие фильтра	N
🗹 Полный IP трафик	Требуется безопас	K
🗹 Полный ІСМР трафик	Разрешить	<
✓ <Динамический>	Отклик по умолчан	ĸ
•	1	
Добавить <u>И</u> зменить <u>У</u> далить	🔽 Использовать ма	стер
OK	Отмена Прим	іенить

2) Запустить Мастер создания новых правил.

? X Мастер правил безопасности Мастер создания новых правил **ІР-безопасности** Правило безопасности определяет как и когда применяется действие по ее обеспечению на основе критерия из списка фильтров, такого как источник или место назначения, тип ІР-трафика. Правило безопасности содержит набор действий по обеспечению безопасности, которые выполняются, когда соединение подпадает под критерий в списке фильтров IP. Действия по обеспечению безопасности: атрибуты ІР-туннелей методы проверки подлинности действия фильтров Для продолжения нажмите кнопку "Далее". Далее > Отмена



3) Нажать Далее

тер правил безопасности	? ×
Конечная точка туннеля Конечной точкой туннеля является туннелированный компьютер, ближайший к местоположению трафика IP, что определяется списко фильтров IP.	
Туннель IPSEC позволяет пересылать пакеты в частной или общедос сети с уровнем безопасности прямого соединения двух компьютеров Укажите конечную точку туннеля для правила IP-безопасности: Это правило не определяет туннель	:тупной 3.
Конечная точка туннеля указана следующим IP-адресом:	
0.0.0.0	
	1



4) Нажать Добавить

1астер правил безопасности		<u>? ×</u>
Список фильтров IP Выберите список IP-фильтров дл применено правило безопасност	пя того типа IP-трафика, к котој ти.	оому будет
Если ни один из нижеприведенни кнопку "Добавить" для создания <u>С</u> писки фильтров IP:	ых фильтров IP вам не подходи я нового фильтра.	т, нажмите
Имя	Описание	Добавить
О Полный ІСМР трафик	Сравнение всех ІСМР-пакет	<u></u>
О Полный IP трафик О Создание списка IP-филь	Сравнение всех IP-пакетов	<u>И</u> зменить <u>У</u> далить
	< <u>Н</u> азад Дале	е> Отмена



5) Создать новый фильтр через Мастер, нажав кнопку Добавить

)к фильтров IP (о скомпоновать			
колов.	ь в один IP-фильтр	ножества фильтров. Та несколько подсетей, IF	ким образом Р-адресов и
		18	
жа IP-фильтров	(1)		(
			Добавить
			Изменить
		T	Удалить
		Исполь	зовать мастер
сание	Протокол	Порт источника	Порт назн
	ска IP-фильтров исание	ска IP-фильтров (1) исание Протокол	ска IP-фильтров (1)



6) Нажать Далее, если нужно, можно указать Описание.

стер ІР-фильтров	? ×
Описание IP-фильтра и свойство "Отраженный" Поле описания используется для указания имени или пояснения к IP-фильтру. Флажок "Отраженный" используется для указания фильтра в каждом из направлений.	Ē
<u>О</u> писание:	
Internet Explorer	
I	
противоположными адресами источника и назначения.	
< <u>Н</u> азад Далее> (Этмена



7) Указать Адрес источника пакетов, нажать Далее.

Мастер IP-фильтров			? ×
Источник IP-трафика Указание адреса источника IP-трафика.			Ē
Адрес <u>и</u> сточника пакетов:			
Мой IP-адрес			
	< <u>Н</u> азад Да	алее >	Отмена



8) По аналогии с Адресом источника указать Адрес назначения.

9) Указать номер порта, используемый для протокола, в нашем случае 80.

Мастер IP-фильтров	<u>? ×</u>
Тип протокола IP Выберите тип протокола IP. Если это TCP или UDP протокол, укажите также исходный и конечный порты.	Ĩ
Выберите тип протокола: Другое 80	
< <u>Н</u> азад Далее>	Отмена



10) Завершить работу с Мастером.

Мастер фильтров IP		<u>? ×</u>
A	Завершение мастера IP-фильтра	
	Работа мастера IP-фильтра успешно завершена.	
1	Чтобы изменить спецификацию IP-фильтра, установите флажок "Изменить свойства" и затем нажмите кнопку "Готово".	
	□ Изменить свойства	
	Чтобы закрыть мастер, нажмите кнопку "Готово".	
	< <u>Н</u> азад Готово Отме	ia



11) Убедиться, что правило появилось в списке фильтров.

Список	фильтров IP			?)
	Список фильтров I можно скомпонов протоколов.	Р формируется из м ать в один IP-фильтр	ножества фильтров. Та несколько подсетей, If	ким образом ⁹ -адресов и
1м <u>я</u> :				
Создани	е списка IP-фильтр	юв (1)		
Описание	9)			Добавить
7				Изменить
			*	<u>У</u> далить
Р-фильтр	оы:		Исполь	зовать мастер
Отра	Описание	Протокол	Порт источника	Порт назн
Дa	Internet Explorer	80	ANY	ANY
Да		ANY	ANY	ANY
•				
			OK	Отмена



12) Разрешить передачу данных данному протоколу.

	юерите деиствие фильтра для	н фильтрат оезопасности.	E
Еслин "Доба помоц Ле	никакие действия фильтра не вить" для создания нового де цью мастера, установите фла ействия фильтра:	соответствуют необходимым, на эйствия. Чтобы создать новое де жок "Использовать мастер". Г Испол	эжмите кнопку йствие фильтра с ьзовать м <u>а</u> стер
Ī	метрия фильтра. Імя	Описание	Добавить
	Э Запрос безопасности (Во Разрешить	Принимать небезопасную с Разрешение прохождение н	Изменить
C) Требуется безопасность	Принимать небезопасную с	<u>У</u> далить



Практическая часть

Подготовьте Internet Explorer для безопасной работы через proxy server, адрес которого 192.168.0.16 порт 8080.

Результат: Выполнив работу, вы научитесь управлять защитой сетевого трафика с помощью средств стандартного протокола IPSec операционной системы Microsoft Windows.

