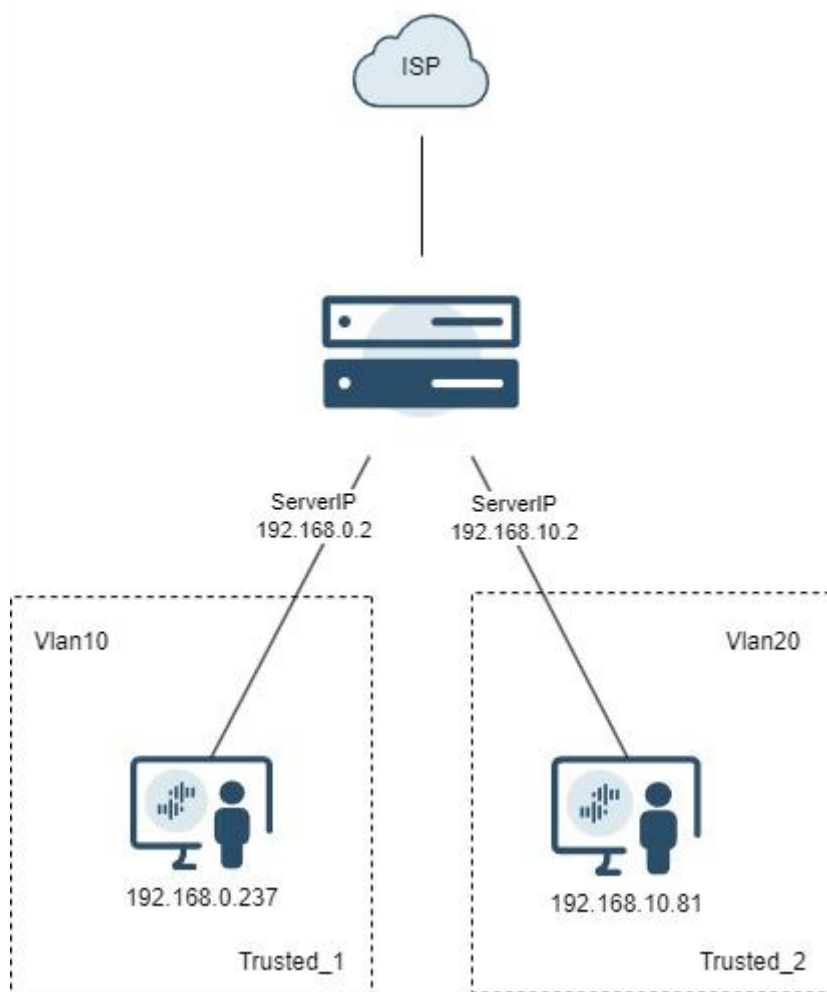


# ПОДКЛЮЧЕНИЕ АГЕНТОВ АУТЕНТИФИКАЦИИ ДЛЯ WINDOWS ИЗ РАЗНЫХ ПОДСЕТЕЙ

## Задача

Организовать соединение между агентами аутентификации, установленными в разных сегментах сети, и сервером UserGate в кластере отказоустойчивости **Актив-Пассив**, используя один адрес назначения.



## Решение

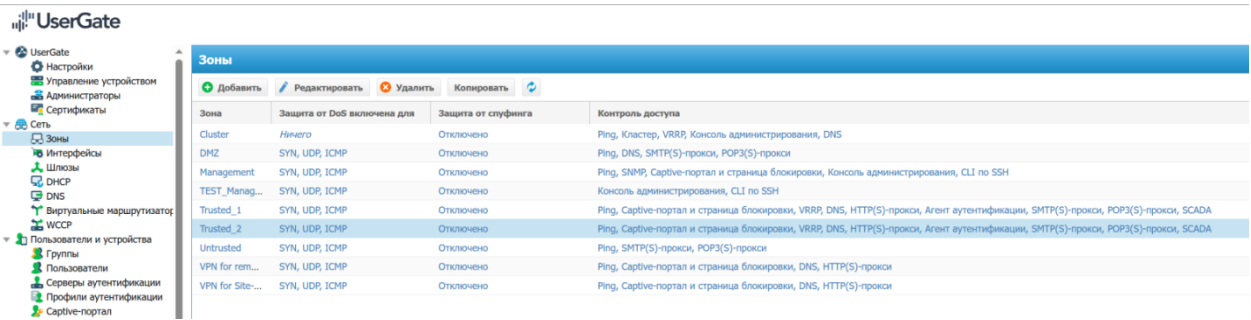
Для указания адреса интерфейса UserGate, на который приходят запросы агента аутентификации для Windows, используется параметр "ServerIP". NGFW принимает пакет только в том случае, если указанный в настройках агента адрес назначения ("ServerIP") совпадает с адресом интерфейса, куда пакет пришел; если [IP-адрес](#) принадлежит другому интерфейсу NGFW, то пакет будет отброшен.

Для отправки пакетов со всех интерфейсов в один адрес назначения, принадлежащий одному интерфейсу NGFW, необходимо настроить правила DNAT.

Адрес назначения меняется правилом DNAT по адресу источника (для каждой локальной подсети в адрес своего интерфейса). "ServerIP" должен быть виртуальный, поэтому интерфейсы узлов должны быть в разных зонах (узлы разные, на одном сегменте сети одна зона). Необходимо настроить по 2 правила DNAT для каждой сети, соответственно во всех других правилах нужно будет указать по две зоны.

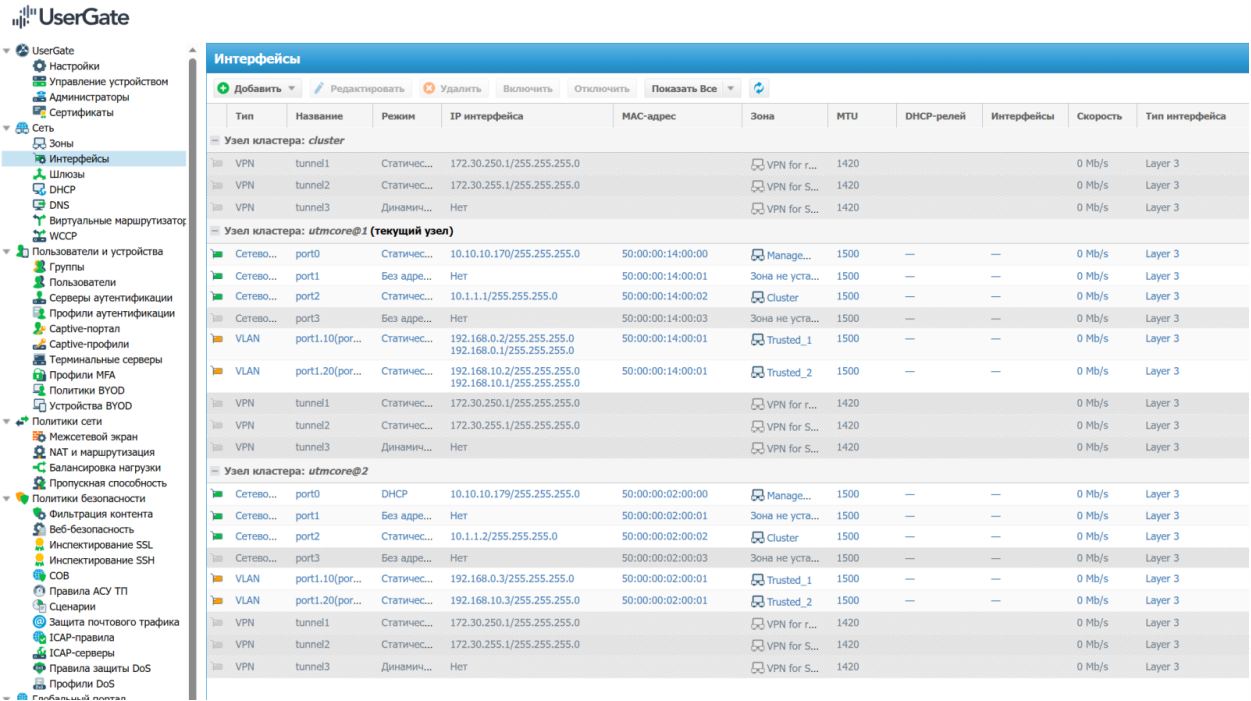
Для того чтобы использовать один адрес назначения для разных подсетей, необходимо произвести следующие настройки:

1. Перейдите в раздел **Сеть → Зоны** и создайте разные зоны для подсетей с пользователями.



Зона	Защита от DoS включена для	Защита от спуфинга	Контроль доступа
Cluster	Ничего	Отключено	Ping, Кластер, VRRP, Консоль администрирования, DNS
DMZ	SYN, UDP, ICMP	Отключено	Ping, DNS, SMTP(S)-прокси, POP3(S)-прокси
Management	SYN, UDP, ICMP	Отключено	Ping, SNMP, Captive-портал и страница блокировки, Консоль администрирования, CLI по SSH
TEST_Manag...	SYN, UDP, ICMP	Отключено	Консоль администрирования, CLI по SSH
Trusted_1	SYN, UDP, ICMP	Отключено	Ping, Captive-портал и страница блокировки, VRRP, DNS, HTTP(S)-прокси, Агент аутентификации, SMTP(S)-прокси, POP3(S)-прокси, SCADA
Trusted_2	SYN, UDP, ICMP	Отключено	Ping, Captive-портал и страница блокировки, VRRP, DNS, HTTP(S)-прокси, Агент аутентификации, SMTP(S)-прокси, POP3(S)-прокси, SCADA
Untrusted	SYN, UDP, ICMP	Отключено	Ping, SMTP(S)-прокси, POP3(S)-прокси
VPN for rem...	SYN, UDP, ICMP	Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси
VPN for Site...	SYN, UDP, ICMP	Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси

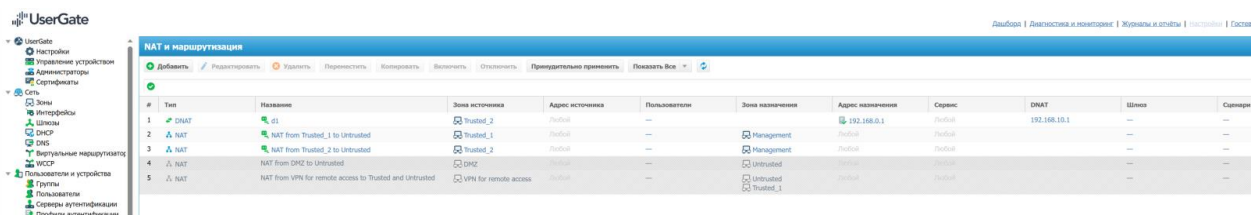
2. Перейдите в раздел **Сеть → Интерфейсы**, установите корректные IP-адреса, соответствующие вашим сетям, и назначьте зоны интерфейсам.



Тип	Название	Режим	IP интерфейса	MAC-адрес	Зона	MTU	DHCP-релей	Интерфейсы	Скорость	Тип интерфейса
Узел кластера: cluster										
VPN	tunnel1	Статичес...	172.30.250.1/255.255.255.0		VPN for r...	1420			0 Mb/s	Layer 3
VPN	tunnel2	Статичес...	172.30.255.1/255.255.255.0		VPN for S...	1420			0 Mb/s	Layer 3
VPN	tunnel3	Динамич...	Нет		VPN for S...	1420			0 Mb/s	Layer 3
Узел кластера: utmscore@1 (текущий узел)										
Cetevo...	port0	Статичес...	10.10.10.170/255.255.255.0	50:00:00:14:00:00	Manage...	1500			0 Mb/s	Layer 3
Cetevo...	port1	Без адре...	Нет	50:00:00:14:00:01	Зона не уста...	1500			0 Mb/s	Layer 3
Cetevo...	port2	Статичес...	10.1.1.1/255.255.255.0	50:00:00:14:00:02	Cluster	1500			0 Mb/s	Layer 3
Cetevo...	port3	Без адре...	Нет	50:00:00:14:00:03	Зона не уста...	1500			0 Mb/s	Layer 3
VLAN	port1.10(port...	Статичес...	192.168.0.2/255.255.255.0	50:00:00:14:00:01	Trusted_1	1500			0 Mb/s	Layer 3
VLAN	port1.20(port...	Статичес...	192.168.10.2/255.255.255.0	50:00:00:14:00:01	Trusted_2	1500			0 Mb/s	Layer 3
VLAN	port1.30(port...	Статичес...	192.168.10.3/255.255.255.0	50:00:00:14:00:01	Trusted_2	1500			0 Mb/s	Layer 3
VPN	tunnel1	Статичес...	172.30.250.1/255.255.255.0		VPN for r...	1420			0 Mb/s	Layer 3
VPN	tunnel2	Статичес...	172.30.255.1/255.255.255.0		VPN for S...	1420			0 Mb/s	Layer 3
VPN	tunnel3	Динамич...	Нет		VPN for S...	1420			0 Mb/s	Layer 3
Узел кластера: utmscore@2										
Cetevo...	port0	DHCP	10.10.10.179/255.255.255.0	50:00:00:02:00:00	Manage...	1500			0 Mb/s	Layer 3
Cetevo...	port1	Без адре...	Нет	50:00:00:02:00:01	Зона не уста...	1500			0 Mb/s	Layer 3
Cetevo...	port2	Статичес...	10.1.1.2/255.255.255.0	50:00:00:02:00:02	Cluster	1500			0 Mb/s	Layer 3
Cetevo...	port3	Без адре...	Нет	50:00:00:02:00:03	Зона не уста...	1500			0 Mb/s	Layer 3
VLAN	port1.10(port...	Статичес...	192.168.0.3/255.255.255.0	50:00:00:02:00:01	Trusted_1	1500			0 Mb/s	Layer 3
VLAN	port1.20(port...	Статичес...	192.168.10.3/255.255.255.0	50:00:00:02:00:01	Trusted_2	1500			0 Mb/s	Layer 3
VPN	tunnel1	Статичес...	172.30.250.1/255.255.255.0		VPN for r...	1420			0 Mb/s	Layer 3
VPN	tunnel2	Статичес...	172.30.255.1/255.255.255.0		VPN for S...	1420			0 Mb/s	Layer 3
VPN	tunnel3	Динамич...	Нет		VPN for S...	1420			0 Mb/s	Layer 3

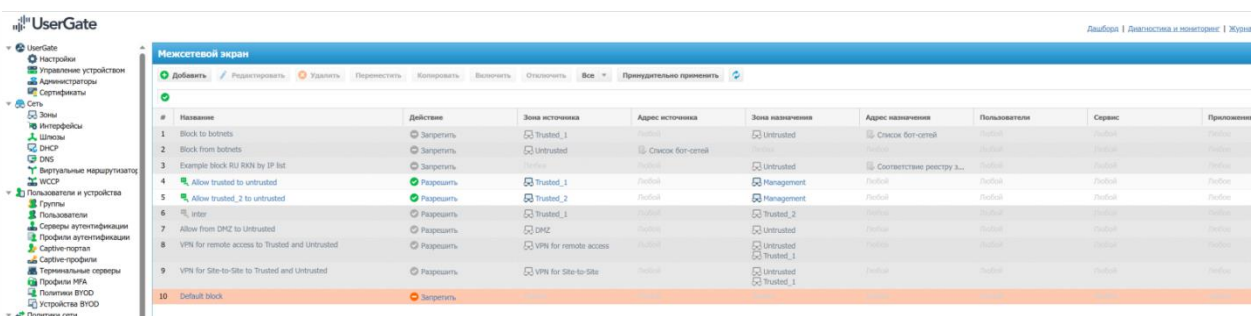
3. Перейдите в раздел **Политики сети → NAT и маршрутизация**. Поменяйте адрес назначения правилом DNAT по адресу источника (для каждой локальной подсети в адрес своего интерфейса). Адрес должен быть не виртуальным, поэтому интерфейсы узлов должны быть в разных зонах.

## Создайте правило DNAT согласно инструкции



#	Тип	Название	Зона источника	Адрес источника	Пользователи	Зона назначения	Адрес назначения	Сервис	DNAT	Штат	Состояние
1	DNAT	80	Trusted_2	Any	—	Management	192.168.0.1	HTTP	192.168.1.1	—	—
2	Δ NAT	NAT from Trusted_1 to Untrusted	Trusted_1	Any	—	Management	Any	Any	—	—	—
3	Δ NAT	NAT from Trusted_2 to Untrusted	Trusted_2	Any	—	Management	Any	Any	—	—	—
4	Δ NAT	NAT from DMZ to Untrusted	DMZ	Any	—	Untrusted	Any	Any	—	—	—
5	Δ NAT	NAT from VPN for remote access to Trusted and Untrusted	VPN for remote access	Any	—	Untrusted	Any	Any	—	—	—

4. Перейдите в раздел **Политики сети** → **Межсетевой экран**, в случае если пользователям локальных подсетей требуется в выход в интернет, создайте правило межсетевого экрана указав зоны, присвоенные подсетям.



#	Название	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Пользователи	Сервис	Приложение
1	Block to botnets	Запретить	Untrusted	Any	Untrusted	Список bot-сетей	Any	Any	Any
2	Block from botnets	Запретить	Untrusted	Список bot-сетей	Any	Any	Any	Any	Any
3	Example block RU RKN by IP list	Запретить	Any	Any	Untrusted	Список RU RKN	Any	Any	Any
4	Allow trusted to untrusted	Разрешить	Trusted_1	Any	Management	Any	Any	Any	Any
5	Allow trusted_2 to untrusted	Разрешить	Trusted_2	Any	Management	Any	Any	Any	Any
6	Inter	Разрешить	Trusted_1	Any	Trusted_2	Any	Any	Any	Any
7	Allow from DMZ to Untrusted	Разрешить	DMZ	Any	Untrusted	Any	Any	Any	Any
8	VPN for remote access to Trusted and Untrusted	Разрешить	VPN for remote access	Any	Untrusted	Any	Any	Any	Any
9	VPN for Site-to-Site to Trusted and Untrusted	Разрешить	VPN for Site-to-Site	Any	Untrusted	Any	Any	Any	Any
10	Default block	Запретить	Any	Any	Untrusted	Any	Any	Any	Any

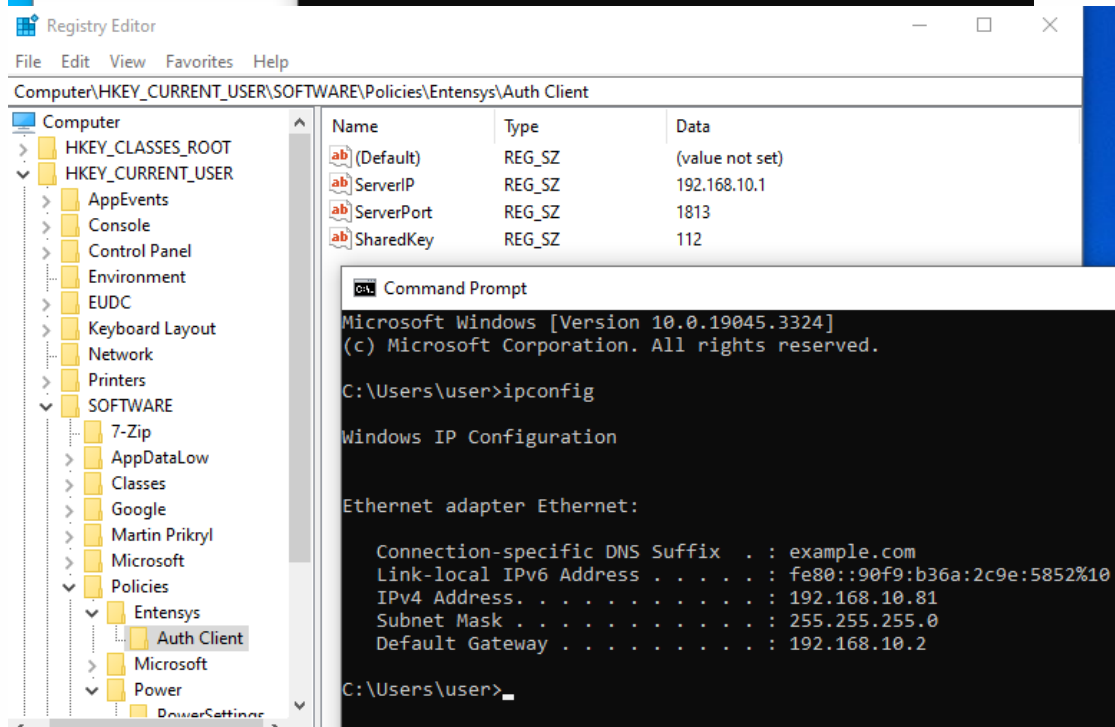
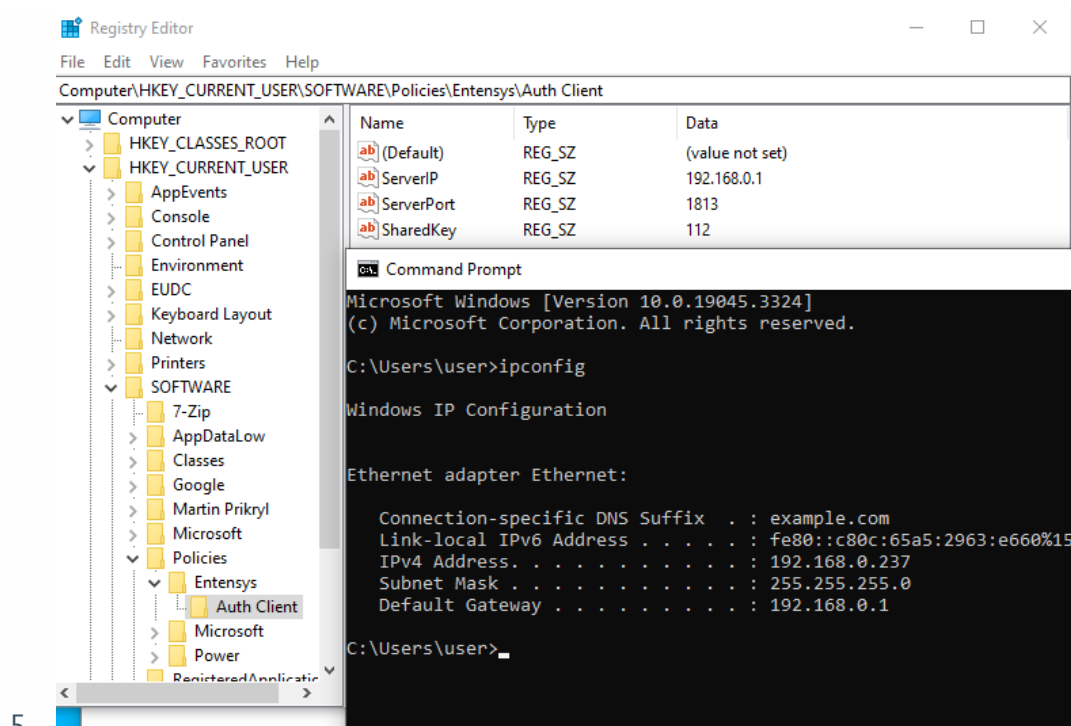
## Установите агент аутентификации АГЕНТ АУТЕНТИФИКАЦИИ ДЛЯ WINDOWS

Для пользователей, работающих на операционной системе Windows, входящих в домен Active Directory, существует еще один способ аутентификации - использовать специальный агент аутентификации. Агент представляет собой сервис, который передает на сервер UserGate информацию о пользователе, его имя и **IP-адрес**, соответственно, UserGate будет однозначно определять все сетевые подключения данного пользователя, и **аутентификация** другими методами не требуется. Чтобы начать работу с идентификацией пользователей с помощью агента авторизации, необходимо выполнить следующие шаги:

Наименование	Описание
<b>Шаг 1.</b> Разрешить сервис агент авторизации на необходимой зоне.	В разделе <b>Сеть</b> → <b>Зоны</b> разрешить сервис <b>Агент аутентификации</b> для той зоны, со стороны которой находятся пользователи.
<b>Шаг 2.</b> Задать пароль агентов терминального сервера.	В консоли UserGate в разделе <b>UserGate</b> → <b>Настройки</b> → <b>Модули</b> напротив записи <b>Пароль агентов терминального сервиса</b> нажать на кнопку <b>Настроить</b> и задать пароль агентов терминального сервера.

Наименование	Описание
<p><b>Шаг 3.</b> Установить агент аутентификации.</p>	<p>Установить агент авторизации на все компьютеры, для которых необходимо идентифицировать пользователей.</p> <p><b>Важно!</b> Агент аутентификации совместим со всеми версиями ОС Windows, кроме Windows XP.</p> <p>Агент авторизации поставляется вместе с административным шаблоном для распространения через политики Active Directory. Используя этот шаблон, администратор может развернуть корректно настроенный агент на большое количество пользовательских компьютеров. С помощью административного шаблона администратор может задать <a href="#">IP-адрес</a> и порт сервера UserGate, и заданный на предыдущем шаге пароль. Более подробно о разворачивании ПО с использованием политик Active Directory вы можете прочитать в документации Microsoft.</p> <p>Агент может быть установлен и без использования групповых политик. Для этого необходимо установить агент из инсталлятора и указать необходимые параметры для подключения к серверу UserGate в следующих ключах реестра:</p> <pre>[HKEY_CURRENT_USER\Software\Policies\Entensys\Auth Client] "ServerIP"="" "ServerPort"="1813" "SharedKey"=""</pre>

UserGate теперь будет получать информацию о пользователях. В политиках безопасности можно использовать имена пользователей, как они указаны в Active Directory, для этого необходим настроенный LDAP-коннектор. Если коннектор не настроен, то можно использовать пользователей **Known** и **Unknown**.



6. Перейдите в раздел **Журналы и отчеты** → **Журнал трафика**. В окне журнала будут отражены активные соединения между ПК и NGFW и записи об аутентификации пользователей.

- Журналы
  - Журнал событий
  - Журнал веб-доступа
  - Журнал трафика
  - Журнал COB
  - Журнал ASU TPI
  - Журнал инвентаризации SSH
  - История поиска
  - Экспорт журналов
- Отчёты
  - Шаблоны
  - Правила отчётов
  - Созданные отчёты

Журнал трафика																		
Сегмент (10 Aug 2023) ▾		Действие: Все ▾		Тип: Все ▾		Сбл: *		Расширенный		Сохранить как		Получаемые фильтры ▾						
IP назначения: Все ▾																		
Узел	Время	Пользователь	Правило	Протокол	Протокол	Зона источника	IP источника	Порт	Зона назначения	IP назначения	Порт...	NAT адрес...	NAT ...	NAT адрес...	NAT ...	Байт отправлено...	Пакетов отпра...	
utmcor...	09:01:59	User2	NAT from...	Q...	UDP	Trusted_2	192.168.10.81	53588	Manage...	142.250.150.94	443	10.10.10.170	53588	142.250.150...	443	1.2 KB / 0 bytes	1 / 0	
utmcor...	09:01:59	User2	Allow tru...	Q...	UDP	Trusted_2	192.168.10.81	53588	Manage...	142.250.150.94	443	Not	Not	Not	Not	1.2 KB / 0 bytes	1 / 0	
utmcor...	09:01:58	User2	Allow tru...	SSL	SSL	Trusted_2	192.168.10.81	49692	Manage...	64.233.162.94	443	Not	Not	Not	Not	649 bytes / 52 b...	3 / 1	
utmcor...	09:01:58	User2	NAT from...	Not...	TCP	Trusted_2	192.168.10.81	49692	Manage...	64.233.162.94	443	10.10.10.170	49692	64.233.162.94	443	52 bytes / 0 bytes	1 / 0	
utmcor...	09:01:58	User2	Allow tru...	Not...	TCP	Trusted_2	192.168.10.81	49692	Manage...	64.233.162.94	443	Not	Not	Not	Not	52 bytes / 0 bytes	1 / 0	
utmcor...	09:01:58	System	NAT from...	DNS	UDP	Trusted_2	10.10.10.170	6997	Manage...	8.8.8.8	53	Not	Not	Not	Not	62 bytes / 0 bytes	1 / 0	
utmcor...	09:01:57	User2	Allow tru...	ML...	SSL	Trusted_2	192.168.10.81	49691	Manage...	20.190.181.4	443	Not	Not	Not	Not	313 bytes / 52 b...	3 / 1	
utmcor...	09:01:57	User2	NAT from...	Not...	TCP	Trusted_2	192.168.10.81	49691	Manage...	20.190.181.4	443	10.10.10.170	49691	20.190.181.4	443	52 bytes / 0 bytes	1 / 0	
utmcor...	09:01:57	User2	Allow tru...	Not...	TCP	Trusted_2	192.168.10.81	49691	Manage...	20.190.181.4	443	Not	Not	Not	Not	52 bytes / 0 bytes	1 / 0	
utmcor...	09:01:56	System	NAT from...	DNS	UDP	Trusted_2	10.10.10.170	45680	Manage...	8.8.8.8	53	Not	Not	Not	Not	60 bytes / 0 bytes	1 / 0	
utmcor...	09:01:54	User2	NAT from...	Q...	UDP	Trusted_2	192.168.10.81	57162	Manage...	209.85.233.103	443	10.10.10.170	57162	209.85.233.1...	443	1.2 KB / 0 bytes	1 / 0	
utmcor...	09:01:54	User2	Allow tru...	Q...	UDP	Trusted_2	192.168.10.81	57162	Manage...	209.85.233.103	443	Not	Not	Not	Not	1.2 KB / 0 bytes	1 / 0	
utmcor...	09:01:49	User2	Allow tru...	SSL	SSL	Trusted_2	192.168.10.81	49690	Manage...	64.233.164.154	443	Not	Not	Not	Not	649 bytes / 52 b...	3 / 1	
utmcor...	09:01:49	User2	NAT from...	Not...	TCP	Trusted_2	192.168.10.81	49690	Manage...	64.233.164.154	443	10.10.10.170	49690	64.233.164.1...	443	52 bytes / 0 bytes	1 / 0	
utmcor...	09:01:49	User2	Allow tru...	Not...	TCP	Trusted_2	192.168.10.81	49690	Manage...	64.233.164.154	443	Not	Not	Not	Not	52 bytes / 0 bytes	1 / 0	
utmcor...	09:01:40	User	Allow tru...	HTTP	TCP	Trusted_1	192.168.0.237	49720	Manage...	95.173.136.78	80	Not	Not	Not	Not	554 bytes / 52 b...	3 / 1	
utmcor...	09:01:40	User	Allow tru...	HTTP	TCP	Trusted_1	192.168.0.237	49722	Manage...	95.173.136.78	80	Not	Not	Not	Not	554 bytes / 52 b...	3 / 1	
utmcor...	09:01:40	User	Allow tru...	HTTP	TCP	Trusted_1	192.168.0.237	49721	Manage...	95.173.136.78	80	Not	Not	Not	Not	555 bytes / 52 b...	3 / 1	
utmcor...	09:01:40	User	Allow tru...	HTTP	TCP	Trusted_1	192.168.0.237	49723	Manage...	95.173.136.78	80	Not	Not	Not	Not	564 bytes / 52 b...	3 / 1	
utmcor...	09:01:40	User	NAT from...	Not...	TCP	Trusted_1	192.168.0.237	49723	Manage...	95.173.136.78	80	10.10.10.170	49723	95.173.136.78	80	52 bytes / 0 bytes	1 / 0	
utmcor...	09:01:40	User	Allow tru...	Not...	TCP	Trusted_1	192.168.0.237	49723	Manage...	95.173.136.78	80	Not	Not	Not	Not	52 bytes / 0 bytes	1 / 0	
utmcor...	09:01:40	User	NAT from...	Not...	TCP	Trusted_1	192.168.0.237	49722	Manage...	95.173.136.78	80	10.10.10.170	49722	95.173.136.78	80	52 bytes / 0 bytes	1 / 0	
utmcor...	09:01:40	User	Allow tru...	Not...	TCP	Trusted_1	192.168.0.237	49722	Manage...	95.173.136.78	80	Not	Not	Not	Not	52 bytes / 0 bytes	1 / 0	
utmcor...	09:01:40	User	NAT from...	Not...	TCP	Trusted_1	192.168.0.237	49721	Manage...	95.173.136.78	80	10.10.10.170	49721	95.173.136.78	80	52 bytes / 0 bytes	1 / 0	
utmcor...	09:01:40	User	Allow tru...	Not...	TCP	Trusted_1	192.168.0.237	49721	Manage...	95.173.136.78	80	Not	Not	Not	Not	52 bytes / 0 bytes	1 / 0	

В случае использования кластера отказоустойчивости **Актив-Актив**: адрес назначения меняется правилом DNAT по адресу источника (для каждой локальной подсети в адрес своего интерфейса), но адрес должен быть **не виртуальный**, а физический, поэтому интерфейсы узлов должны быть в разных зонах (у каждого интерфейса своя зона). Должно быть создано по два правила DNAT для каждой сети, соответственно во всех других правилах нужно будет указать по две зоны.