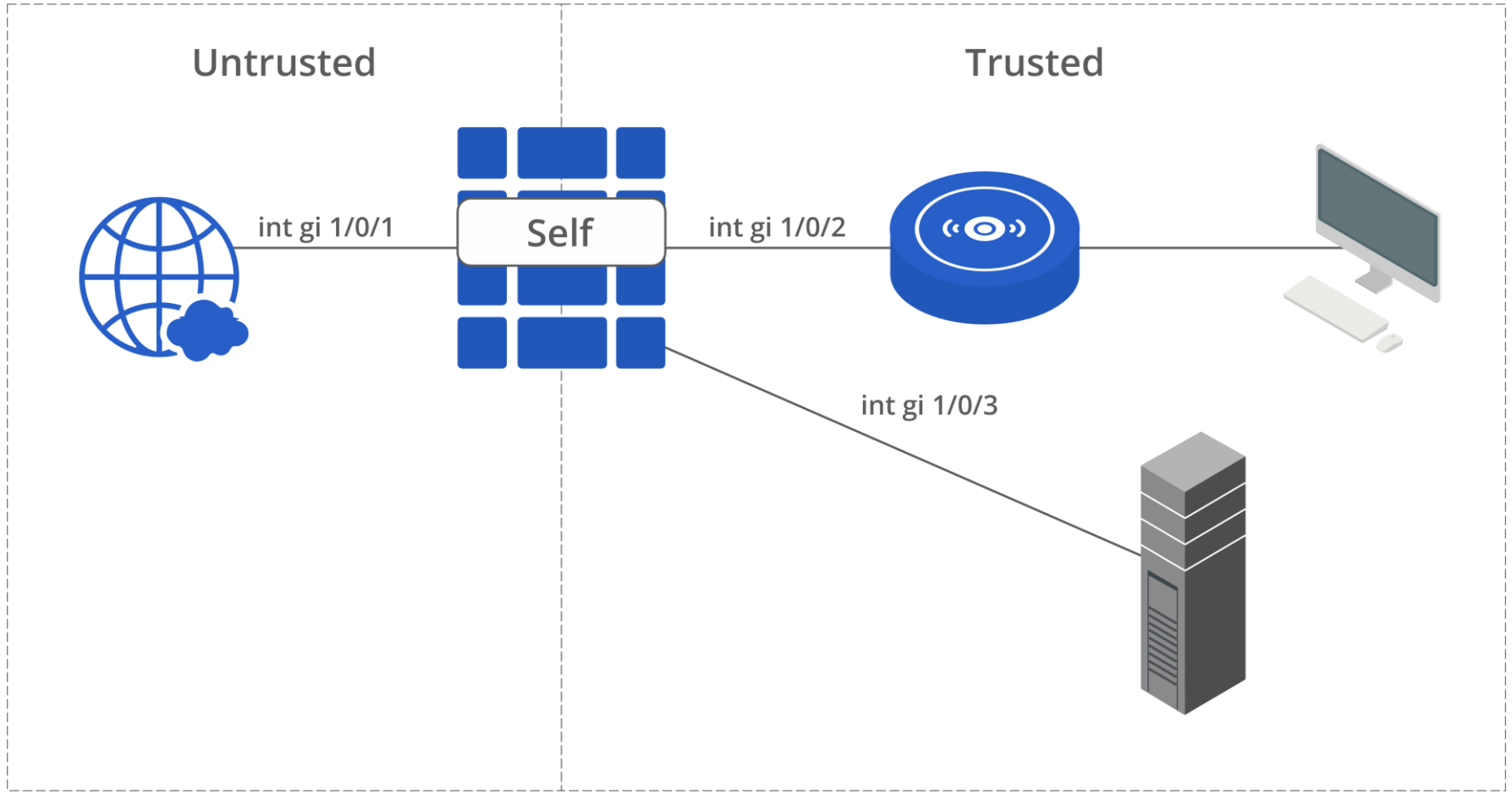
Принципы настройки Firewall на маршрутизаторах ESR

Докладчик: Госкаева Екатерина
Pre-sale инженер отдела
сервисных маршрутизаторов

План вебинара

- Принцип работы zone-based firewall
- Различия между statefull / stateless
- Порядок обработки трафика
- Функционал
- Демонстрации по кейсам
- Отличия от acl, итоги
- Вопрос - ответ
- Полезные ссылки

Zone-based firewall - по умочанию не разрешено



Statefull режим

```
esr# show ip firewall sessions
Codes: E - expected, U - unreplied, A - assured, C - confirmed

Port Aging Inside source       Inside destination  Outside source      Outside destination  Pkts  Bytes  Status
---- ----- ------------------  ------------------  ------------------  -------------------  ----  -----  ------
tcp   78   192.168.1.15:54366  192.168.25.7:22     192.168.1.15:54366  192.168.25.7:22       --     --     --
```

1. По таблице маршрутизации определяется, в какой интерфейс должен будет отправиться обрабатываемый в данный момент пакет

```
esr# configure
esr(config)# security zone LAN
esr(config-security-zone)# exit
esr(config)# security zone WAN
esr(config-security-zone)# exit
```

2. В качестве source-zone принимается зона безопасности, сконфигурированная на интерфейсе через который пакет поступил на маршрутизатор. В качестве destination-zone принимается зона безопасности, сконфигурированная на интерфейсе из 1п.

```
esr(config)# interface gi 1/0/2
esr(config-if-gi)# ip address 192.168.12.2/24
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# exit
esr(config)# interface gi 1/0/3
esr(config-if-gi)# ip address 192.168.12.2/24
esr(config-if-gi)# security-zone LAN
esr(config-if-gi)# exit
```

Statefull режим

3 Просматривается набор правил между source-zone и destination-zone начиная с правила с меньшим номером. Неактивированные правила не просматриваются. Если пакет подпадает под все условия прописанные в правиле ("match") выполняется действие прописанное в правиле ("action") и дальнейший просмотр прекращается

```
esr(config)# security zone-pair LAN WAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# match protocol icmp
esr(config-zone-pair-rule)# match destination-address object-group WAN_Gateway
esr(config-zone-pair-rule)# match source-address object-group LAN_Gateway
esr(config-zone-pair-rule)# enable
```

4 Если пакет попал под правило с "action permit" кроме маршрутизации пакета в таблицу зарегистрированных сессий добавляется информация о сессии, в рамках которой был смаршрутизирован проверенный пакет

```
esr(config)# security zone-pair LAN LAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

Stateless режим

- В режиме stateless происходит проверка каждого пакета. «Прямой» и «ответный» трафики требуется разрешать в соответствующих zone-pair
- Средство для dpi

Порядок обработки трафика правилами

Транзитного

- Трафик проверяется набором правил zone-pair <user-zone> any
- Если трафик передаётся с одного интерфейса на другой в пределах настраеваемых зон, то он будет проверяться набором правил <user-zone1> <user-zone2>
  (Эти зоны могут совпадать)
- Трафик проверяется набором правил zone-pair any any

Если трафик не попал ни под одно из правил текущей zone-pair, он отбрасывается

Терминируемого на ESR

- Трафик проверяется набором правил zone-pair any self
- Трафик проверяется набором правил zone-pair <user-zone> self

Если трафик не попал ни под одно из правил текущей zone-pair, он отбрасывается

Можно ли отключить firewall?

```
esr(config-if-gi)# ip firewall
disable
```

При применении команды

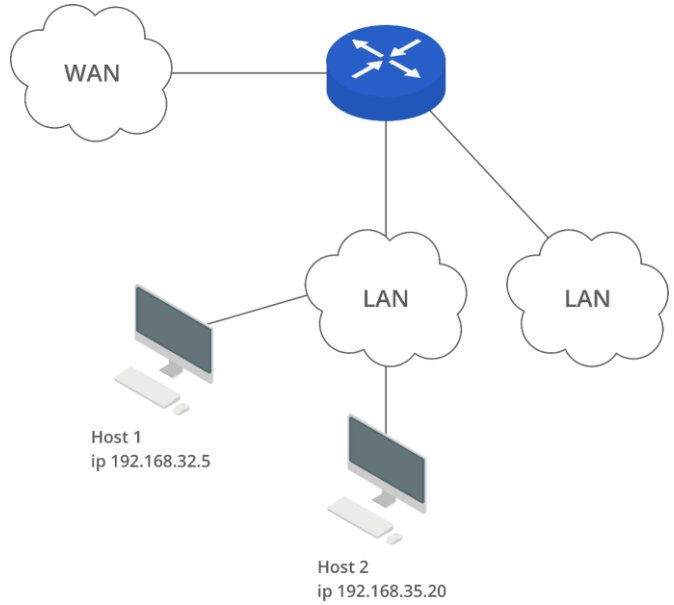
- Маршрутизатор продолжает регистрировать маршрутизируемые сессии
- Firewall не отключается полностью, но перестаёт просматриваться соответствующий набор правил межзонного взаимодействия даже если одновременно с "ip firewall disable" на интерфейсе указана зона безопасности
- Все пакеты поступающие через данный интерфейс считаются разрешенными

WAN LAN

LAN to WAN LAN to WAN LAN to WAN LAN to LAN

```
esr(config)#object-group network host_1
esr(config-object-group-network)# ip address-range 192.168.32.1-192.168.32.10
esr(config)#object-group service Black_ports
esr(config-object-group-service)# port-range 80,443
esr(config)# security zone-pair any WAN
esr(config-security-zone-pair)# rule 10
esr(config-security-zone-pair-rule)# action deny
esr(config-security-zone-pair-rule)# match protocol tcp
esr(config-security-zone-pair-rule)# match destination-port object-group
Black_ports
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# rule 2
esr(config-security-zone-pair-rule)# action permit
esr(config-security-zone-pair-rule)# match protocol tcp
esr(config-security-zone-pair-rule)# match source-address object-group host_1
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# rule 30
esr(config-security-zone-pair-rule)# action permit
esr(config-security-zone-pair-rule)# enable
esr(config-security-zone-pair-rule)# exit
esr(config-security-zone-pair)# exit
esr(config)# security zone-pair LAN LAN
esr(config-zone-pair)# rule 1
esr(config-zone-pair-rule)# action permit
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
```

```
esr(config-security-zone-pair)# rearange <>
esr(config-security-zone-pair)# renumber
rule <CUR_ORDER> <NEW_ORDER>
```



trusted self

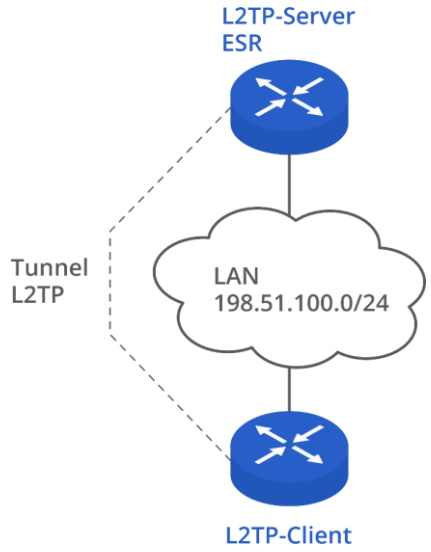
```
object-group service IKE
  port-range 500
  port-range 4500
exit
object-group service L2TP
  port-range 1701
exit

security zone trusted
exit
security zone untrusted
exit

interface gigabitethernet 1/0/1
  security-zone untrusted
  ip address 198.51.100.1/24
exit
security zone-pair untrusted self
  rule 1
    action permit
    match protocol udp
    match destination-port object-
group L2TP
    enable
  exit
rule 2
    action permit
    match protocol udp
    match destination-port object-
group IKE
    enable
  exit
```

```
rule 3
    action permit
    match protocol esp
    enable
  exit
exit
security zone-pair trusted trusted
  rule 1
    action permit
    enable
  exit
exit
security zone-pair trusted self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
exit
security ike proposal l2tp
  encryption algorithm aes256
  dh-group 14
exit
security ipsec proposal l2tp
  encryption algorithm aes256
exit
remote-access l2tp server
  authentication mode local
  local-address ip-address
192.0.2.1
  remote-address address-range
192.0.2.2-192.0.2.10
  outside-address ip-address
198.51.100.1
```

```
security-zone trusted
ipsec authentication method pre-shared-
key
  ipsec authentication pre-shared-key
ascii-text encrypted 8CB5107EA7005AFF
  ipsec ike rekey enable
  ipsec ike proposal l2tp
  ipsec proposal l2tp
username user2
    password ascii-text encrypted
8CB5107EA7005AFF
    enable
  exit
  enable
exit
```



Функционал

Логирование

```
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 10000
esr(config-zone-pair-rule)# action deny log
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

2022-11-21T12:27:31+00:00 %FIREWALL-I-LOG: zone-pair 'untrusted self' rule 10000 denied tcp 192.168.1.15:40900 (gi1/0/1 60:e3:27:00:ee:e9) -> 192.168.1.1:23 dscp 4, 1 packets

```
esr(config)# security zone-pair untrusted self
esr(config-zone-pair)# rule 10
esr(config-zone-pair-rule)# action permit log
esr(config-zone-pair-rule)# match destination-port SSH
esr(config-zone-pair-rule)# match source-address SSH_TRUSTED_PERMIT
esr(config-zone-pair-rule)# enable
esr(config-zone-pair-rule)# exit
esr(config-zone-pair)# exit
```

2022-11-21T12:28:25+00:00 %FIREWALL-I-LOG: zone-pair 'untrusted self' rule 100 permitted tcp 192.168.1.15:43596 (gi1/0/1 60:e3:27:00:ee:e9) -> 192.168.1.1:22 dscp 0, 1 packets

Счетчики

```
esr(config)#ip firewall sessions counters

Zone-pair                  Rule        Action           Pkts        Bytes       Description
-------------------------  ----------  ---------------  ----------  ----------  --------------------
any/any                    default     deny             0           0           --
trusted/self                 1         permit           0           0           From local to router
trusted/trusted              1         permit           0           0           --
```

Критерии

Protocol type/id

Профиль ip адресов

mac адреса

match [not] destination - nat

match [not] fragment – any self

match [not] ip-option - any self

Профиль tcp/udp портов

По умолчанию любой match - any, можно явно не указывать

Профиль приложений (dpi)

Тип и код сообщений протокола ICMP

Action

permit - прохождение трафика разрешается

deny - прохождение трафика запрещается

reject - дополнительно посылает ответ об ошибке

rate-limit total pps <RATE>

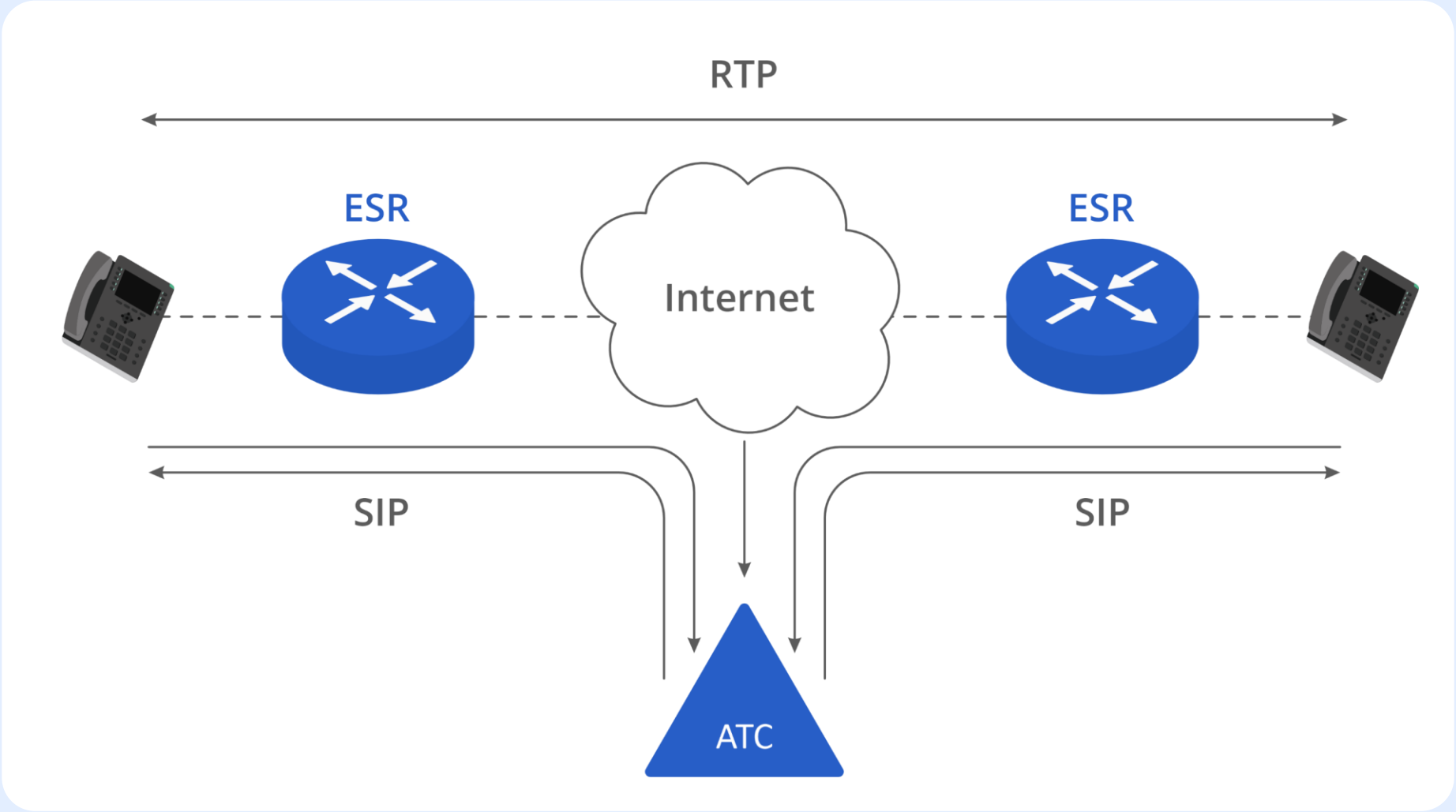
Команда применима только в правилах между зонами any self

session-limit [total <SESSION>] [per-source-host <SESSION>]

Управление защитой от сетевых атак

ip firewall screen	logging firewall screen
dos-defense icmp-threshold	Защита от ICMP flood атак
dos-defense land	Защита от land-атак
dos-defense syn-flood	Защита от SYN flood атак
dos-defense udp-threshold	Защита от UDP flood атак
dos-defense winnuke	Защита от winnuke-атак
spy-blocking ip-sweep	Защита от IP-sweep атак
spy-blocking port-scan	Защита от port scan атак
spy-blocking spoofing	Защита от IP spoofing атак

ip firewall sessions tracking sip



nat alg sip - для конфигурации с натом

Итоги

- Firewall - средство, осуществляющее контроль и фильтрацию
- Достаточно разрешить первый пакет
- Назначение на все виды интерфейсов
- Средство технологий
- Возможность инспектировать трафик в несколько этапов
- Отслеживание сессий
- ACL - список правил, определяющих прохождение пакетов через интерфейс
- Проверяет каждый пакет
- Можно использовать только на физических интерфейсах
- Краткий список match
- Используется для организации политик QoS и pbr
- Только запрет, без ограничений полосы или pps
- Первый режет пакеты

Match

	Firewall	ACL
application	+	-
cos	-	+
dscp	-	+
source/destination-address-port	+	-
source/destination-nat	+	-
fragment	+	-
icmp	+	-
ip-option	+	-
protocol	+	-
vlan	-	+

Action

	Firewall	ACL
permit	+	+
deny	+	+
reject	+	-
rate-limit	+	-
session-limit	+	-

F.A.Q.

- Как firewall нагружает системы?
- Чем и как обрабатываются правила ACL и Firewall?
- Что если на интерфейсе не настроена security-zone и не отключен Firewall?
- Что если на входящем интерфейсе настроена security-zone, а на исходящем интерфейсе security-zone не определена и отключен firewall?

Полезные ссылки

- База знаний
- Руководство для пользователя
- Справочник команд cli

Курсы

Вебинары

Спасибо за внимание!

Мы всегда готовы к диалогу, разработке и доработке решений под ваше техническое задание

630020, г. Новосибирск, ул. Окружная 29В
09:00 — 18:00 (GMT+7)
Понедельник - пятница

+7 (383) 274-10-01, 274-48-48
eltex@eltex-co.ru; eltex-co.ru