**Packet Tracer. Настройка списков ACL для IP-адресов с целью нейтрализации атак**



Часть 1: Проверьте базовую связь по сети

Шаг 1: с компьютера PC-A проверьте связь с компьютером PC-C и маршрутизатором R2.

Шаг 2: с компьютера PC-C проверьте связь с компьютером PC-A и маршрутизатором R2.

Часть 2: Защитите доступ к маршрутизаторам

Шаг 1: Настройте ACL 10 для полной блокировки удаленного доступа к маршрутизаторам со всех систем, кроме PC-C.

Шаг 2: Примените список ACL 10 к входному трафику на линиях VTY.

Шаг 3: Проверьте монопольный доступ со станции управления PC-C.

Часть 3: Создайте нумерованный список ACL 120 для IP на маршрутизаторе R1

Шаг 1: Убедитесь, что компьютер PC-C может получать доступ к PC-A по протоколу HTTPS с помощью браузера.

Шаг 2: Настройте список ACL 120 для разрешения и отклонения указанного трафика.

Шаг 3: Примените список ACL к интерфейсу S0/0/0.

Шаг 4: Убедитесь, что компьютер PC-C не может получить доступ к PC-A по протоколу HTTPS с помощью браузера.

Часть 4: Измените существующий список ACL на маршрутизаторе R1

Шаг 1: Убедитесь, что компьютер PC-A не может успешно отправлять эхо-запросы на интерфейс loopback на маршрутизаторе R2.

Шаг 2: Внесите необходимые изменения в список ACL 120 для разрешения и отклонения указанного трафика.

Шаг 3: убедитесь, что компьютер PC-A может успешно отправлять эхо-запросы интерфейсу loopback на маршрутизаторе R2.

Часть 5: Создайте нумерованный список ACL 110 для IP на маршрутизаторе R3

Шаг 1: Настройте список ACL 110 для разрешения только трафика из внутренней сети.

Шаг 2: Примените список ACL к интерфейсу G0/1.

Часть 6: Создайте нумерованный список ACL 100 для IP на маршрутизаторе R3

Шаг 1: Настройте список ACL 100 для блокировки всего указанного трафика из внешней сети.

Шаг 2: Примените список ACL к интерфейсу Serial 0/0/1.

Шаг 3: Убедитесь, что указанный трафик, поступающий на последовательный интерфейс 0/0/1, обрабатывается правильно.



