# Best practice sugli ACL su un router serie RV34x

### Obiettivo

In questo articolo vengono descritte le best practice per la creazione di Access Control Lists (ACL) con il router serie RV34x.

### Dispositivi interessati | Versione firmware

- RV340 | 1.0.03.20 (scarica la versione più recente)
- RV340W | 1.0.03.20 (scarica la versione più recente)
- RV345 | 1.0.03.20 (scarica la versione più recente)
- RV345P | 1.0.03.20 (scarica la versione più recente)

## Introduzione

Si desidera un maggiore controllo sulla rete? Eseguire ulteriori operazioni per garantire la protezione della rete? In tal caso, un Access Control List (ACL) potrebbe essere proprio quello di cui avete bisogno.

Un ACL è costituito da una o più voci di controllo di accesso (ACE, Access Control Entries) che definiscono collettivamente il profilo del traffico di rete. A questo profilo possono quindi fare riferimento funzionalità software Cisco come il filtro del traffico, la priorità o le code personalizzate. Ogni ACL include un elemento action (allow o deny) e un elemento filter basato su criteri quali indirizzo di origine, indirizzo di destinazione, protocollo e parametri specifici del protocollo.

In base ai criteri immessi, è possibile controllare determinati traffici dall'ingresso e/o dall'uscita da una rete. Quando un router riceve un pacchetto, lo esamina per stabilire se inoltrarlo o eliminarlo in base all'elenco degli accessi.

L'implementazione di questo livello di protezione si basa su diversi scenari di utilizzo che considerano particolari scenari di rete ed esigenze di protezione.

Èimportante notare che il router può creare automaticamente un elenco degli accessi in base alle configurazioni del router. In questo caso, è possibile che vengano visualizzati elenchi degli accessi che non è possibile cancellare a meno che non si modifichino le configurazioni del router.

### Perché utilizzare gli elenchi di accesso

- Nella maggior parte dei casi, gli ACL vengono usati per fornire un livello di sicurezza di base per l'accesso alla rete. Ad esempio, se non si configurano gli ACL, per impostazione predefinita tutti i pacchetti che passano attraverso il router possono essere autorizzati a tutti i componenti della rete.
- Gli ACL possono consentire a un host e a un intervallo di indirizzi IP o di reti e impedire

a un altro host, a un intervallo di indirizzi IP o di reti di accedere alla stessa area (host o rete).
- Utilizzando gli ACL, è possibile decidere quali tipi di traffico inoltrare o bloccare sulle interfacce del router. Ad esempio, è possibile autorizzare il traffico SFTP (Secure Shell) e contemporaneamente bloccare tutto il traffico SIP (Session Initiation Protocol).

### Quando utilizzare gli elenchi degli accessi

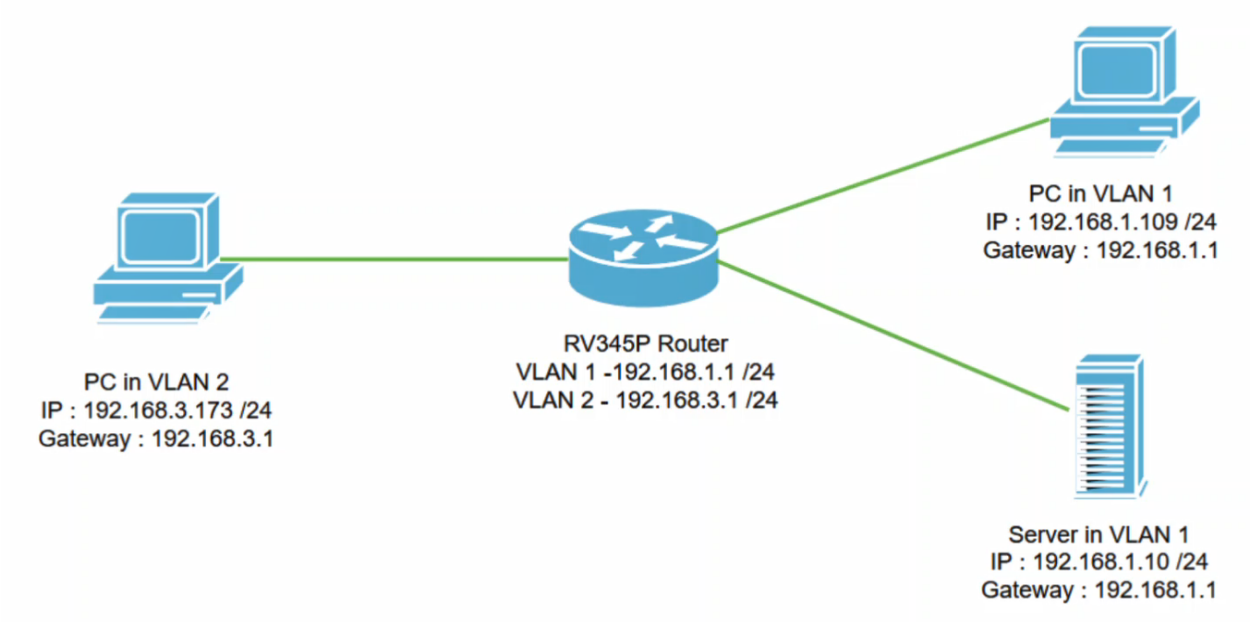
- Ènecessario configurare gli ACL nei router posizionati tra la rete interna e una rete esterna, ad esempio Internet.
- Gli ACL possono essere usati per controllare il traffico in entrata o in uscita da una parte specifica della rete interna.
- Quando è necessario filtrare il traffico in entrata o in uscita, o entrambi, su un'interfaccia.
- Per controllare il traffico, è necessario definire gli ACL in base al protocollo.

### Procedure consigliate per la configurazione della protezione di base con gli elenchi degli accessi

- Implementazione di ACL che consentano solo l'uso di protocolli, porte e indirizzi IP che negano tutto il resto.
- Bloccare i pacchetti in arrivo che affermano di avere la stessa destinazione e lo stesso indirizzo di origine (attacco terrestre sul router stesso).
- Attivare la funzionalità di registrazione degli ACL su un host Syslog interno (trusted).
- Se si usa il protocollo SNMP (Simple Network Management Protocol) sul router, è necessario configurare gli ACL SNMP e la stringa della community SNMP complessa.
- Consenti solo agli indirizzi interni di accedere al router dalle interfacce interne e solo al traffico destinato agli indirizzi interni di accedere al router dall'esterno (interfacce esterne).
- Blocca multicast se non utilizzato.
- Blocca alcuni tipi di messaggi ICMP (Internet Control Message Protocol) (reindirizzamento, eco).
- Considerare sempre l'ordine in cui si inseriscono gli ACL. Ad esempio, quando il router decide se inoltrare o bloccare un pacchetto, lo confronta con ciascuna istruzione ACL nell'ordine in cui sono stati creati gli ACL.

## Implementazione della lista accessi nei router Cisco serie RV34x

### Topologia di rete di esempio



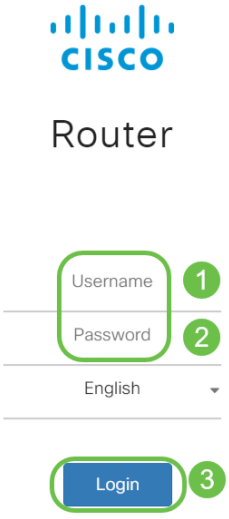

## Scenario di esempio

Questo diagramma di rete viene replicato con un router RV345P e due interfacce VLAN diverse. Abbiamo un PC nella VLAN 1 e nella VLAN 2 e un server nella VLAN 1. Il routing tra VLAN è abilitato, quindi gli utenti della VLAN 1 e della VLAN 2 possono comunicare tra loro. A questo punto si applicherà la regola di accesso per limitare la comunicazione tra l'utente VLAN 2 e questo server nella VLAN 1.

## Configurazione di esempio

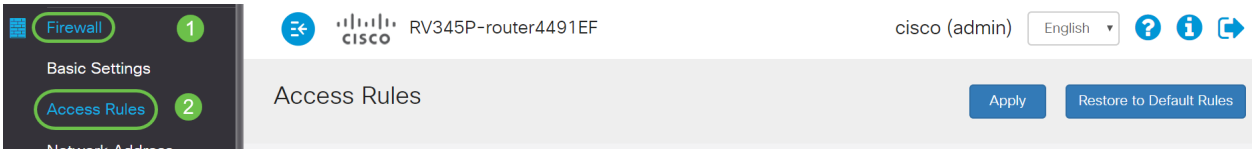
### Passaggio 1

Accedere all'interfaccia utente Web del router utilizzando le credenziali configurate.




### Passaggio 2

Per configurare l'ACL, selezionare **Firewall > Regole di accesso** e fare clic sull'**icona con il segno più** per aggiungere una nuova regola.



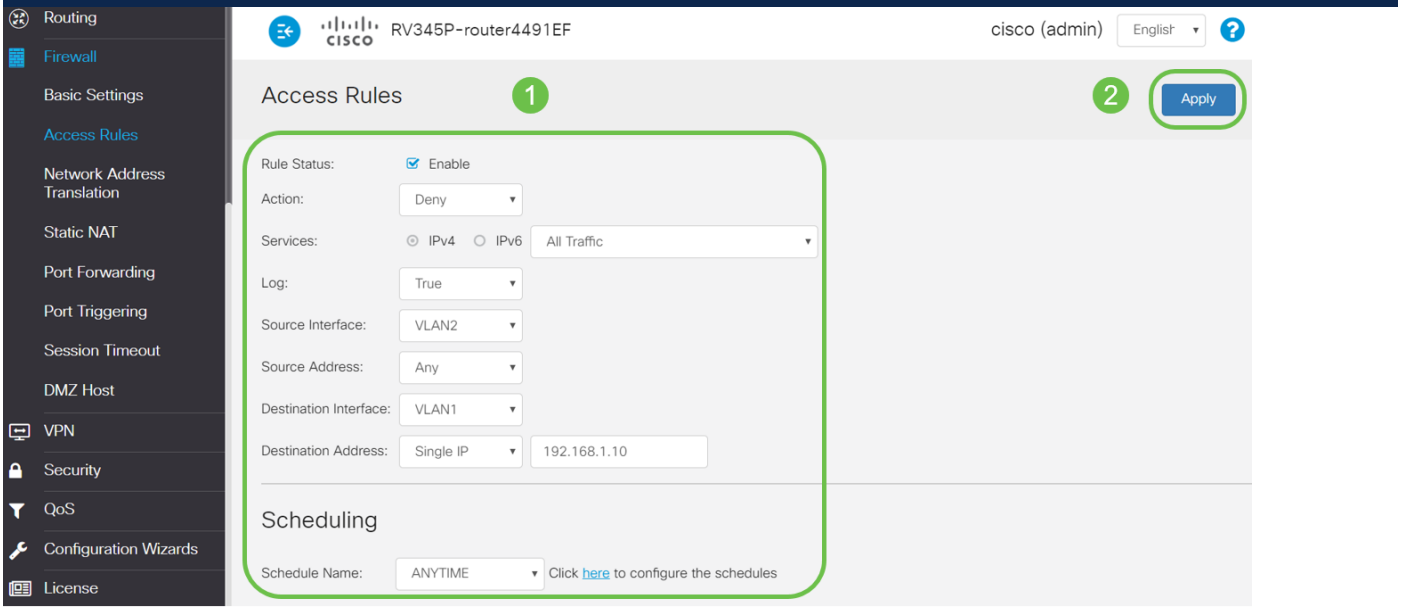
## Passaggio 3

Configurare i parametri *delle regole di accesso*. Applicare l'ACL per limitare il server (IPv4: 192.168.1.10/24) da parte degli utenti VLAN2. Per questo scenario, i parametri saranno i seguenti:

- *Stato regola: Attiva*
- *Azione: Nega*
- *Servizi Tutto il traffico*
- *Registro: Vero*
- *Interfaccia di origine: VLAN2*
- *Source address: Qualsiasi*
- *Interfaccia di destinazione: VLAN1*
- *Indirizzo di destinazione: IP 192.168.1.10 singolo*
- *Nome pianificazione: In qualsiasi momento*

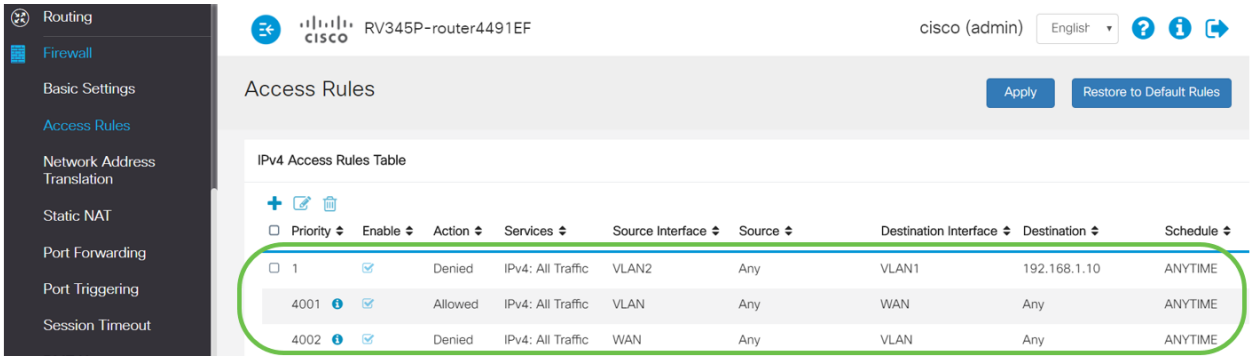
Fare clic su **Apply** (Applica).

Nell'esempio, è stato negato l'accesso al server da qualsiasi dispositivo della VLAN2 e quindi è stato consentito l'accesso agli altri dispositivi della VLAN1. Le esigenze dell'utente potrebbero variare.




## Passaggio 4

Nell'elenco *Regole di accesso* verrà visualizzato quanto segue:




## Verifica

Per verificare il servizio, aprire il prompt dei comandi. Nelle piattaforme Windows, per ottenere questo risultato, fare clic sul pulsante Windows e quindi digitare **cmd** nella casella di ricerca in basso a sinistra del computer e selezionare **Prompt dei comandi** dal menu.

Immettere i seguenti comandi:

- Sul PC (192.168.3.173) nella VLAN2, eseguire il ping del server (IP: 192.168.1.10). Si riceverà una notifica di *timeout della richiesta* che indica che la comunicazione non è consentita.
- Sul PC (192.168.3.173) della VLAN2, eseguire il ping sull'altro PC (192.168.1.109) della VLAN1. La risposta verrà accettata.

```
C:\Users\Cisco>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Cisco>ping 192.168.1.109

Pinging 192.168.1.109 with 32 bytes of data:
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time<1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Cisco>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::249b:cf42:b4fc:384f%20
   IPv4 Address. . . . . . . . . . . : 192.168.3.173
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1
```

## Conclusioni

In tutti i passaggi necessari per configurare la regola di accesso su un router Cisco serie RV34x, Ora è possibile applicarlo per creare una regola di accesso nella rete che soddisfi le proprie esigenze.