Configurazione di Cisco VPN 3000 Concentrator per il blocco con filtri e l'assegnazione di filtri RADIUS

Sommario

Introduzione

In questa configurazione di esempio, si desidera utilizzare i filtri per consentire a un utente di accedere a un solo server (10.1.1.2) all'interno della rete e bloccare l'accesso a tutte le altre risorse. Cisco VPN 3000 Concentrator può essere configurato per controllare l'accesso dei client IPsec, Point-to-Point Tunneling Protocol (PPTP) e L2TP alle risorse di rete tramite filtri. I filtri sono costituiti da regole simili agli elenchi degli accessi di un router. Se un router è stato configurato per:

```
access-list 101 permit ip any host 10.1.1.2
access-list 101 deny ip any any
```

l'equivalente di VPN Concentrator consiste nell'impostare un filtro basato su regole.

La prima regola di VPN Concentrator è **allow_server_rule**, equivalente al comando **allow ip any host 10.1.1.2** del router. La seconda regola di VPN Concentrator è **deny_server_rule**, equivalente al comando **deny ip any** del router.

Il nostro filtro VPN Concentrator è **filter_with_2_rules**, equivalente all'elenco degli accessi 101 del router; vengono utilizzate le regole **allow_server_rule** e **deny_server_rule** (nell'ordine indicato). Si presume che i client possano connettersi correttamente prima di aggiungere i filtri; ricevono gli indirizzi IP da un pool sul concentratore VPN.

Per ulteriori informazioni, fare riferimento al documento PIX/ASA 7.x ASDM: Limitare l'accesso alla rete degli utenti VPN di accesso remoto per ulteriori informazioni sullo scenario in cui PIX/ASA 7.x blocca l'accesso degli utenti VPN.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

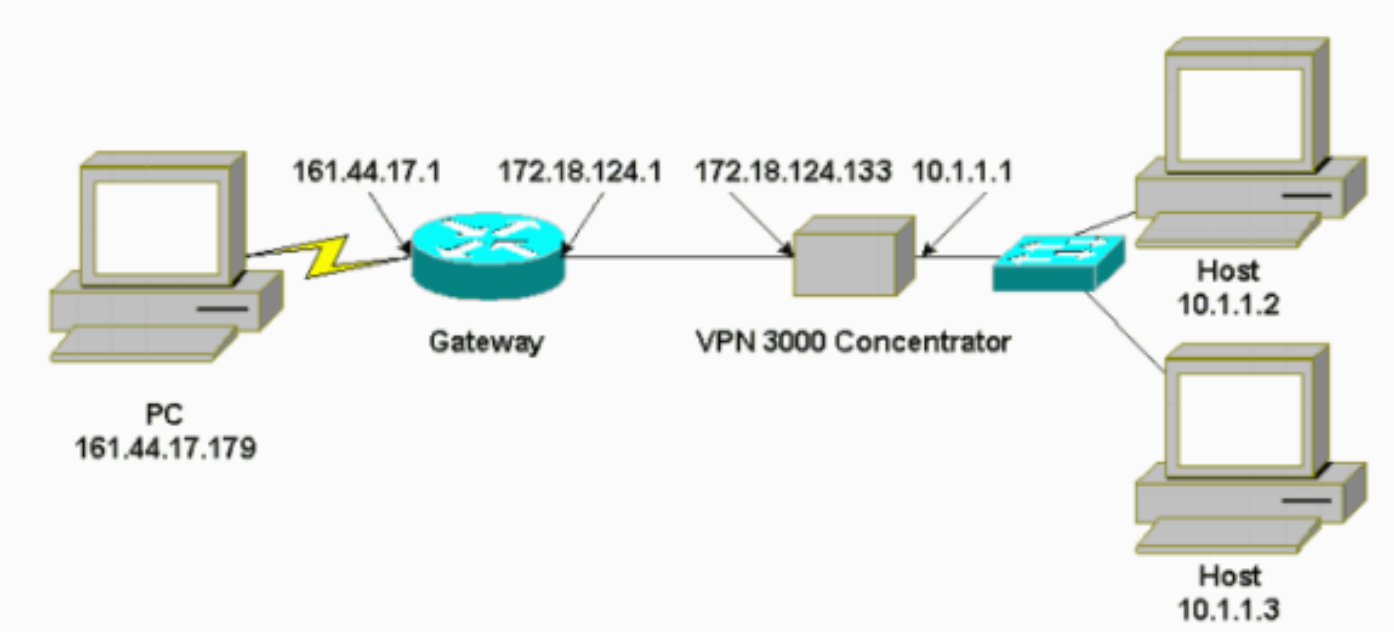
Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco VPN 3000 Concentrator versione 2.5.2.D.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



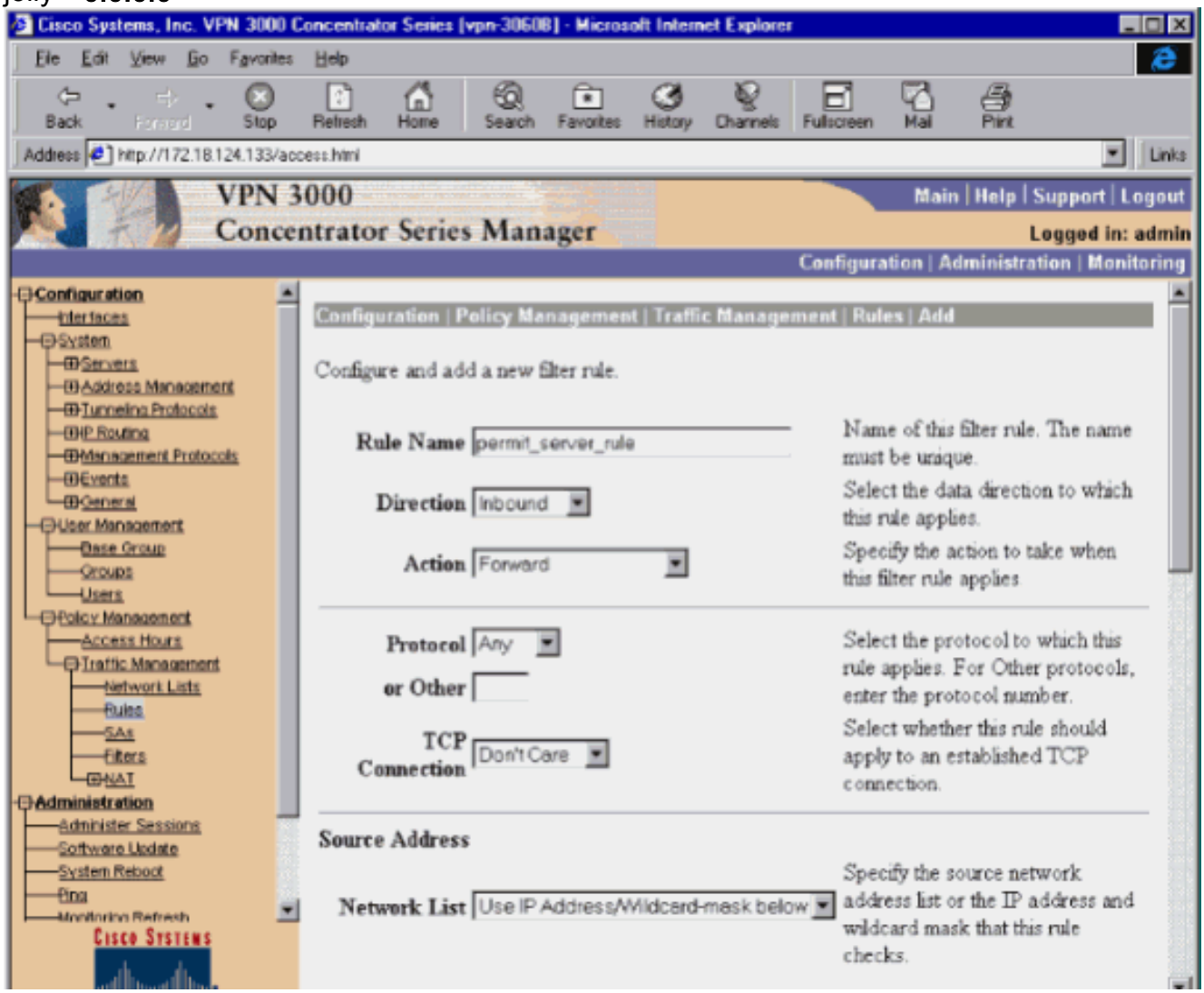
Convenzioni

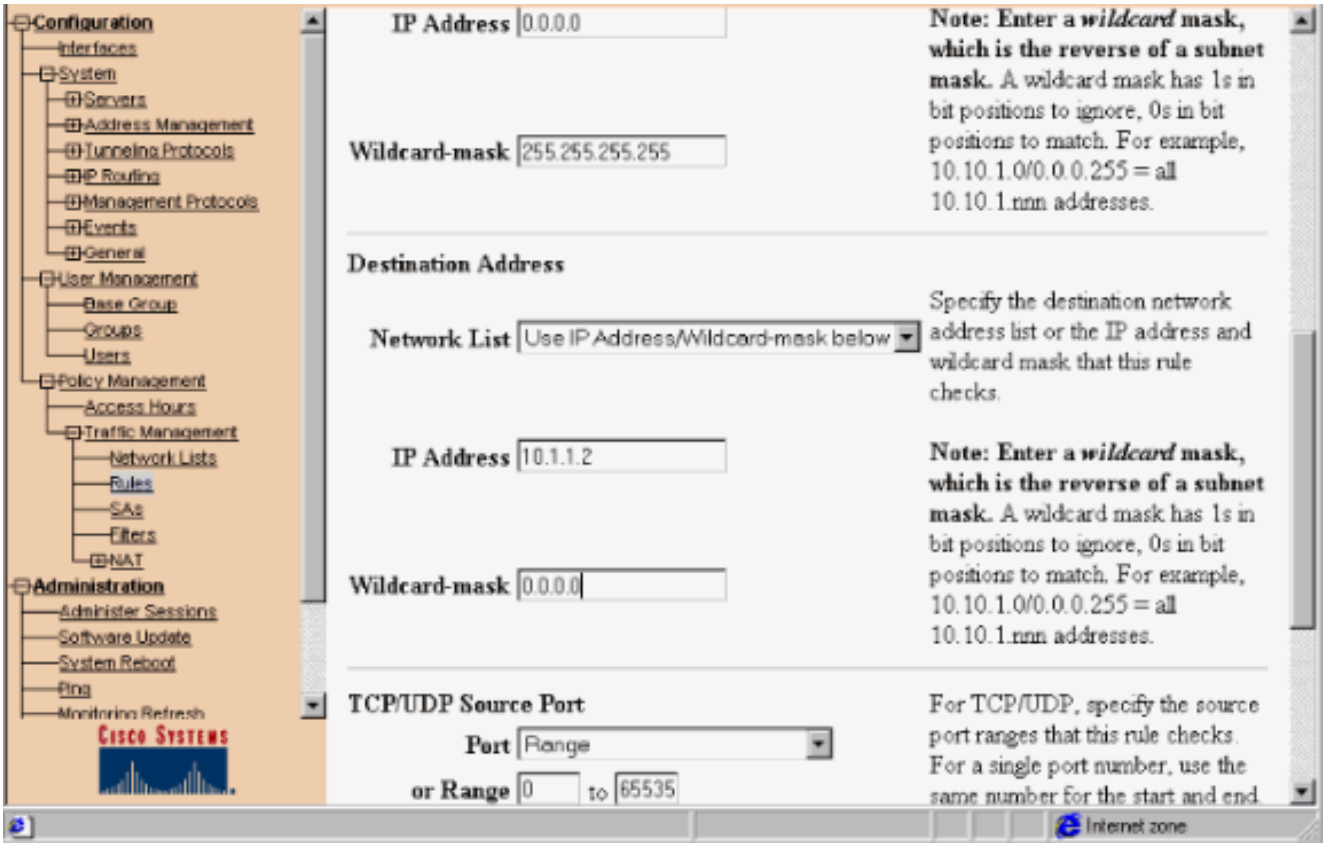
Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione VPN 3000

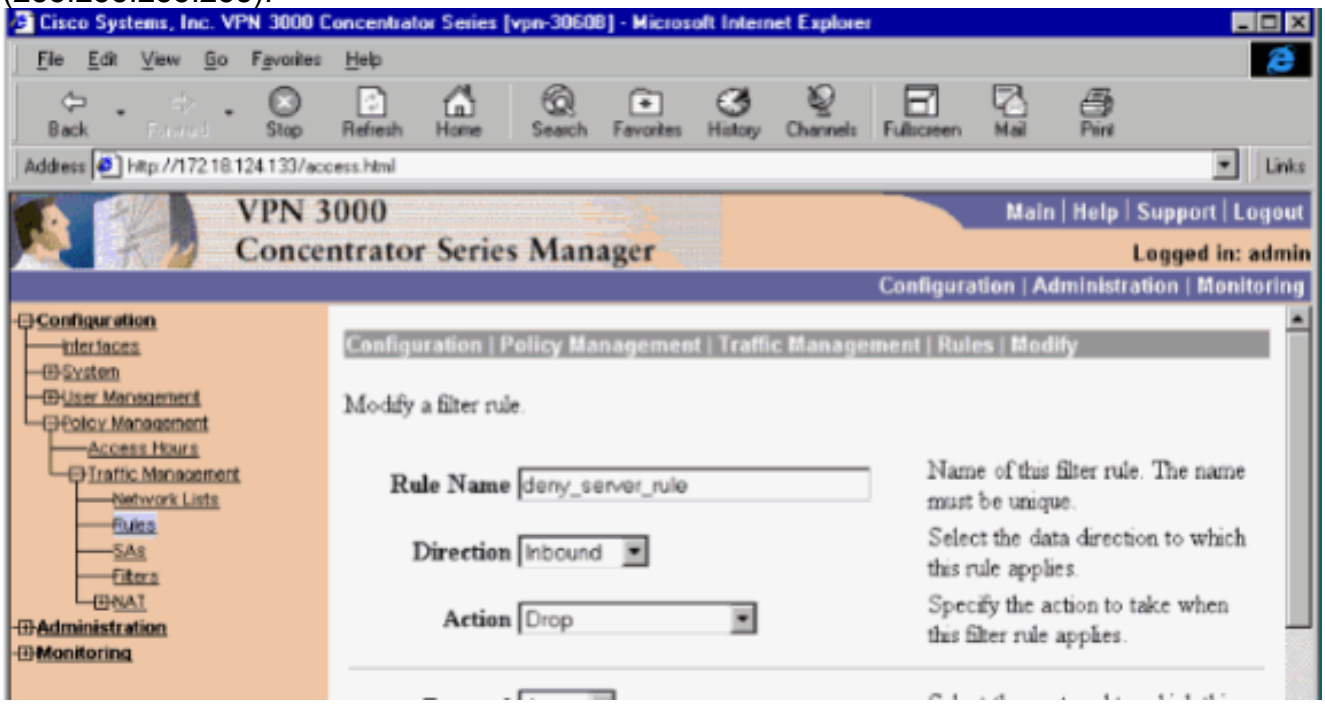
Completare questa procedura per configurare il concentratore VPN 3000.

1. Scegliere **Configurazione > Gestione criteri > Gestione traffico > Regole > Aggiungi** e definire la prima regola di Concentrator VPN denominata **allow_server_rule** con queste impostazioni:Direzione—**In entrata**Azione—**Avanti**Indirizzo di origine—**255.255.255.255**Indirizzo di destinazione—**10.1.1.2**Maschera con caratteri jolly—**0.0.0.0**

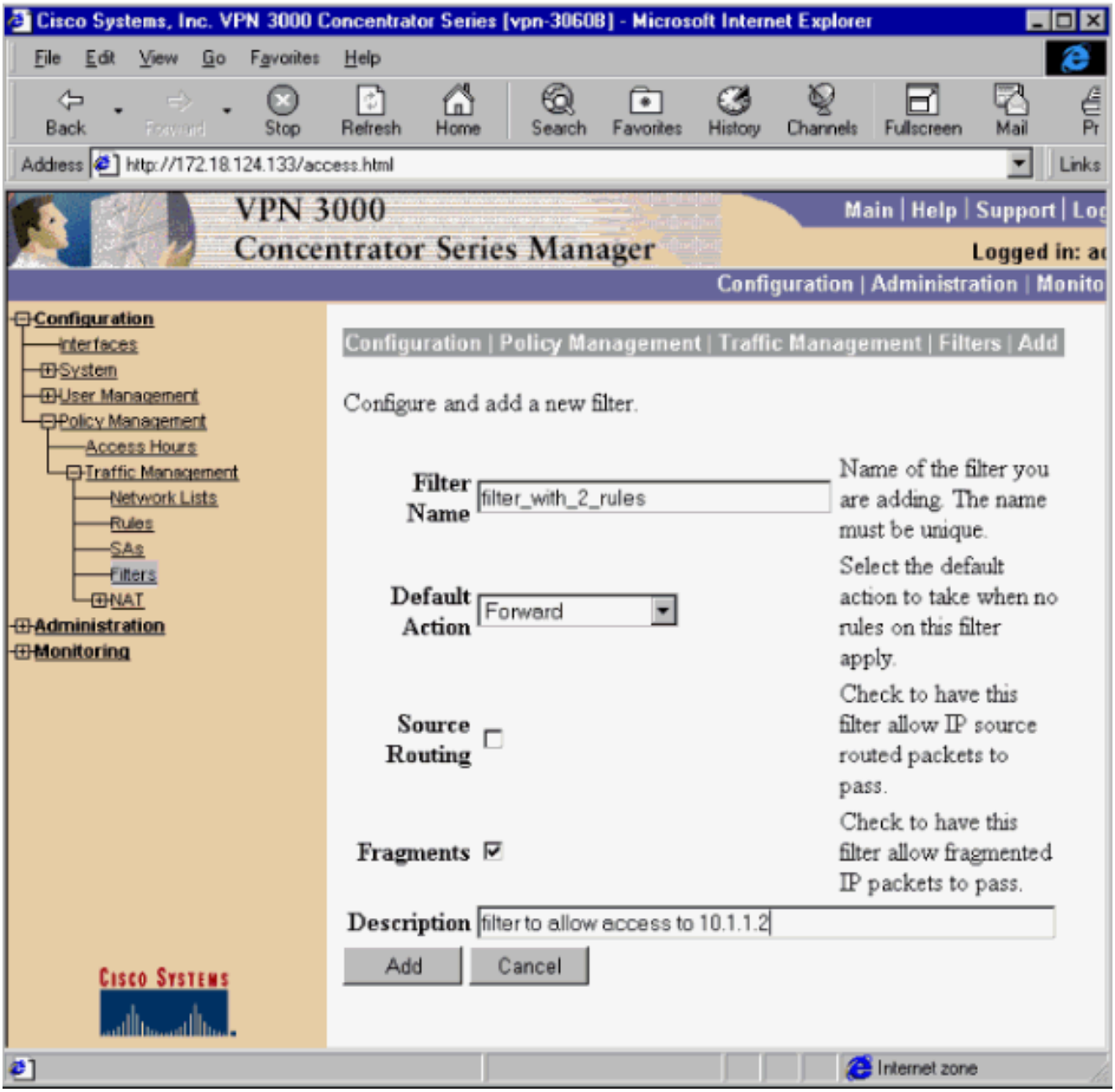




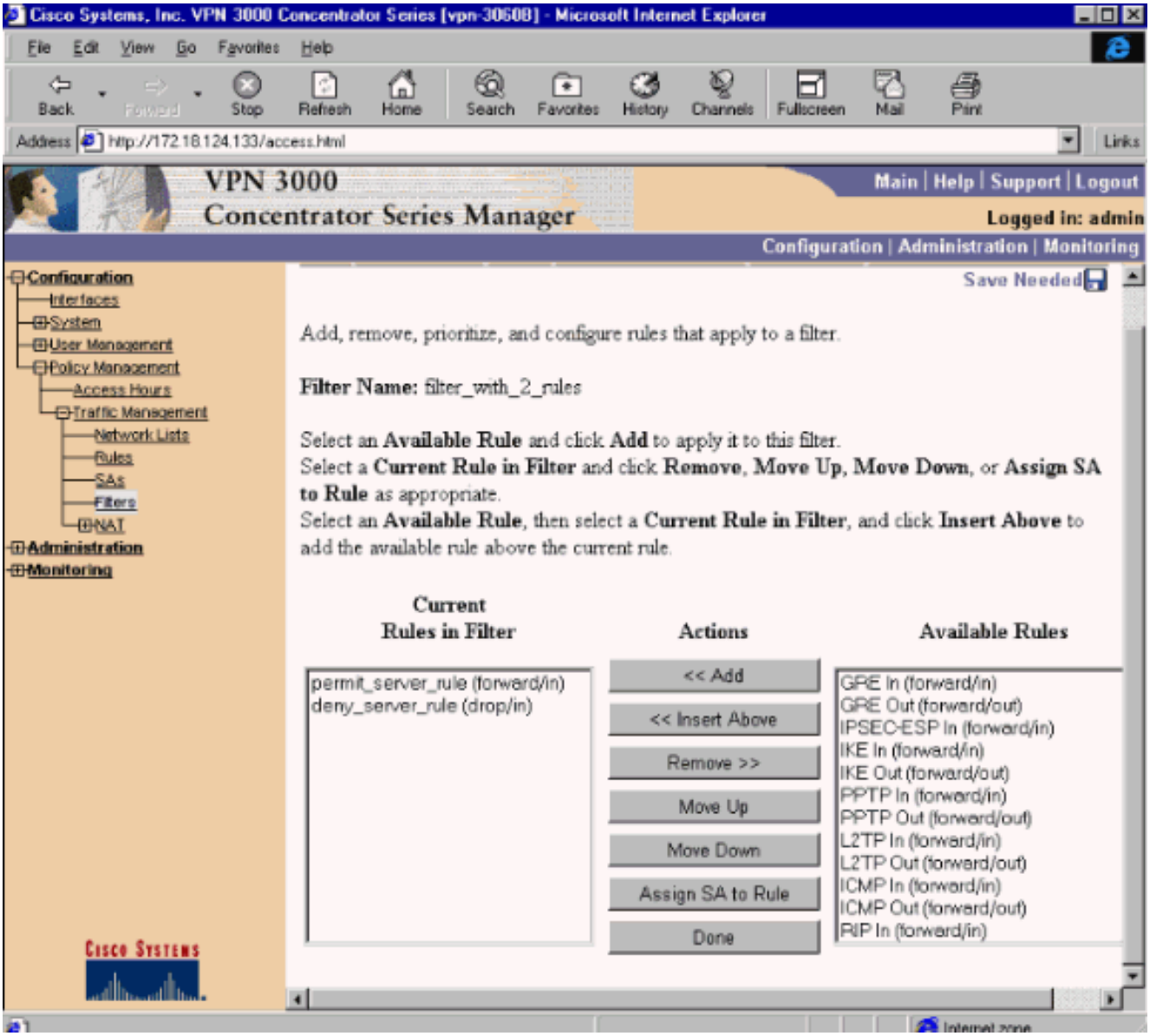
2. Nella stessa area, definire la seconda regola di Concentrator VPN denominata **deny_server_rule** con le impostazioni predefinite seguenti:Direzione—**In entrata**Azione—**Elimina**Indirizzi di origine e di destinazione di qualsiasi elemento (255.255.255.255):



3. Scegliere **Configurazione > Gestione criteri > Gestione traffico > Filtri** e aggiungere il filtro **filter_with_2_rules**.



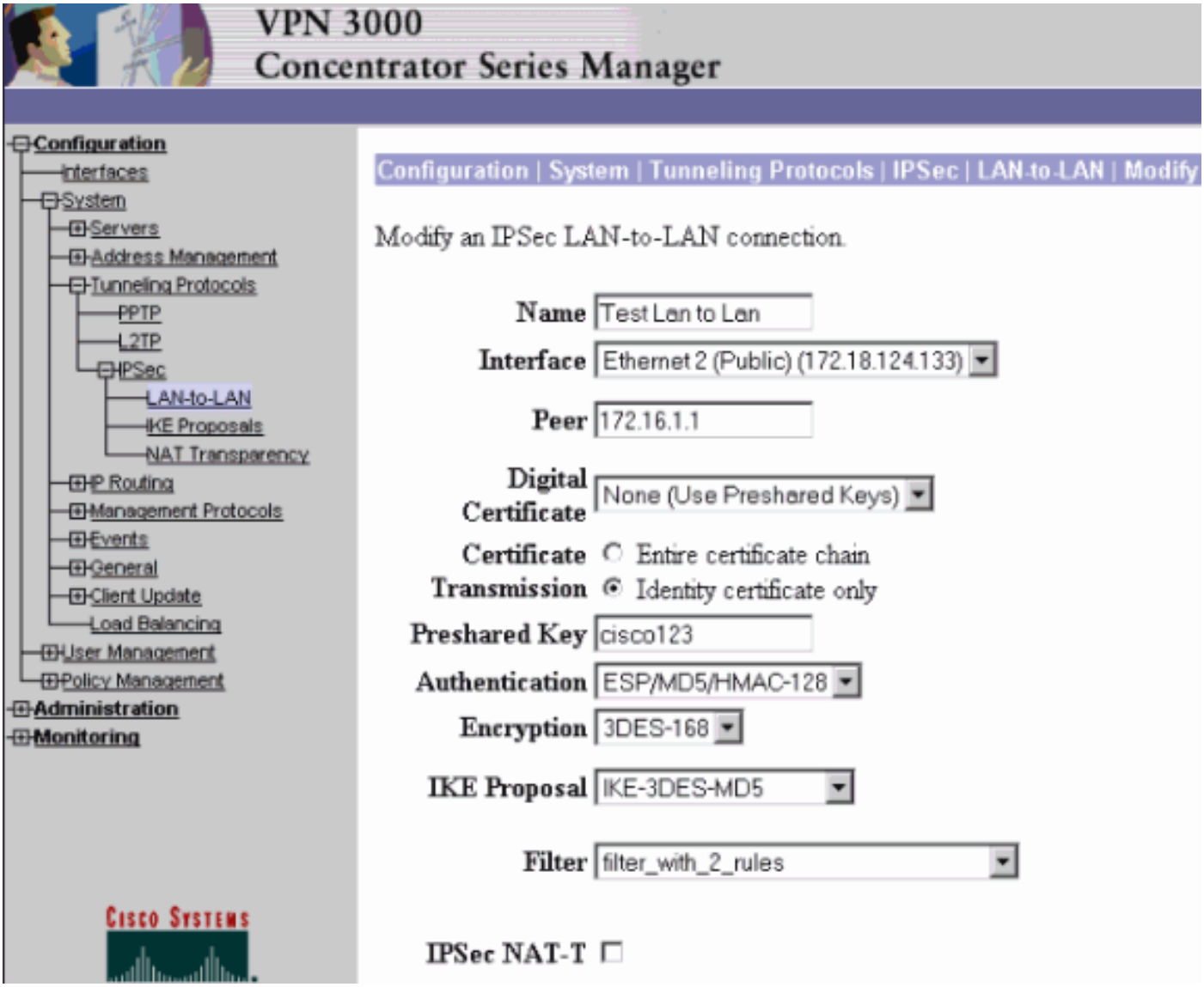
4. Aggiungere le due regole a filter_with_2_rules:



5. Scegliere **Configurazione > Gestione utente > Gruppi** e applicare il filtro al gruppo:

Filtri per un tunnel VPN da LAN a LAN

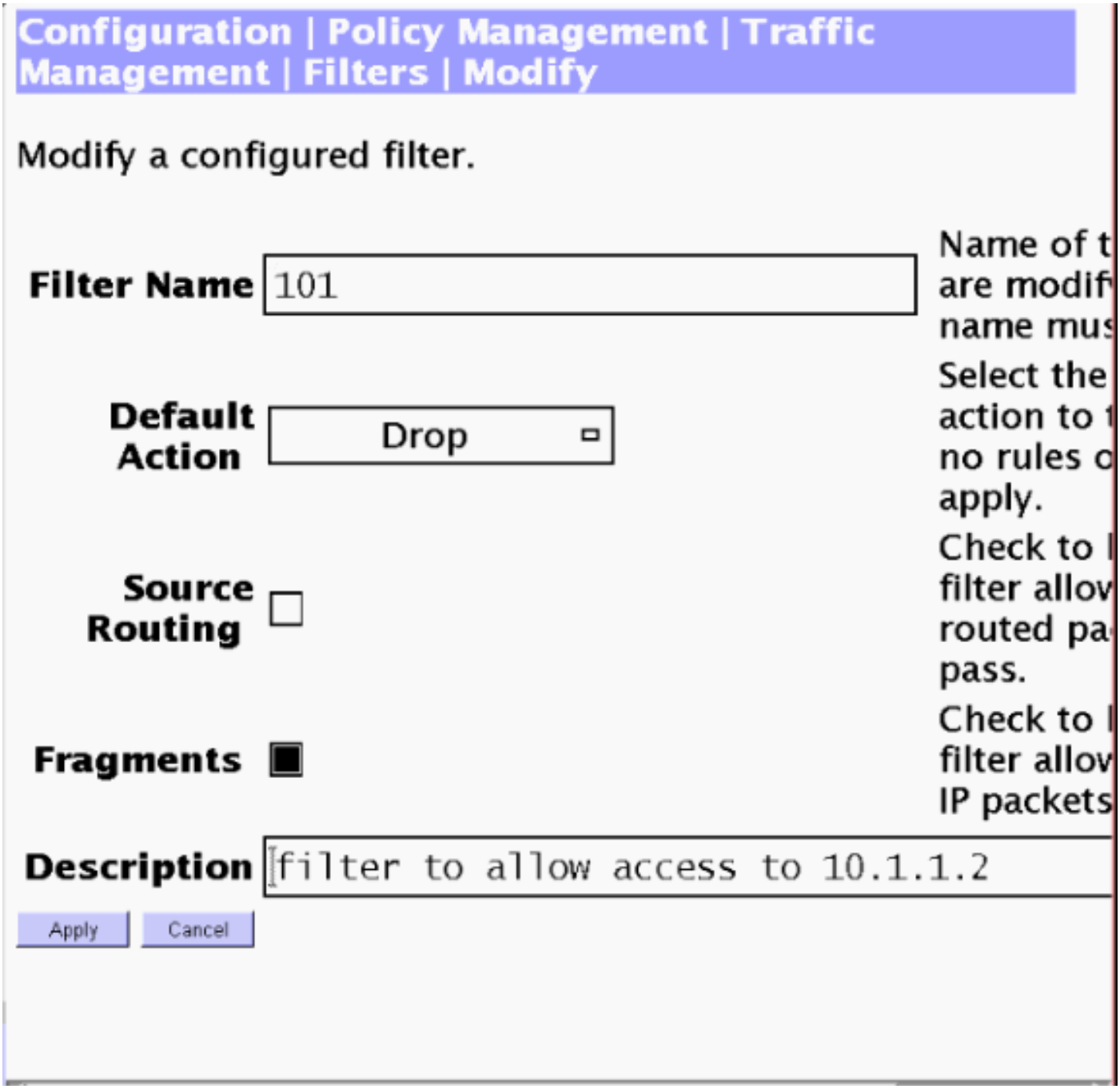
Da VPN Concentrator code 3.6 e versioni successive, è possibile filtrare il traffico per ogni tunnel VPN IPsec da LAN a LAN. Ad esempio, se si costruisce un tunnel da LAN a LAN su un altro concentratore VPN con indirizzo 172.16.1.1 e si desidera consentire all'host 10.1.1.2 l'accesso al tunnel mentre si nega tutto il resto del traffico, è possibile applicare **filter_with_2_rules** quando si sceglie **Configurazione > Sistema > Protocolli di tunneling > IPSec > Da LAN a LAN > Modifica** e si seleziona **filter_with_2_rules** in **Filtro**.



Configurazione VPN 3000 - Assegnazione filtro RADIUS

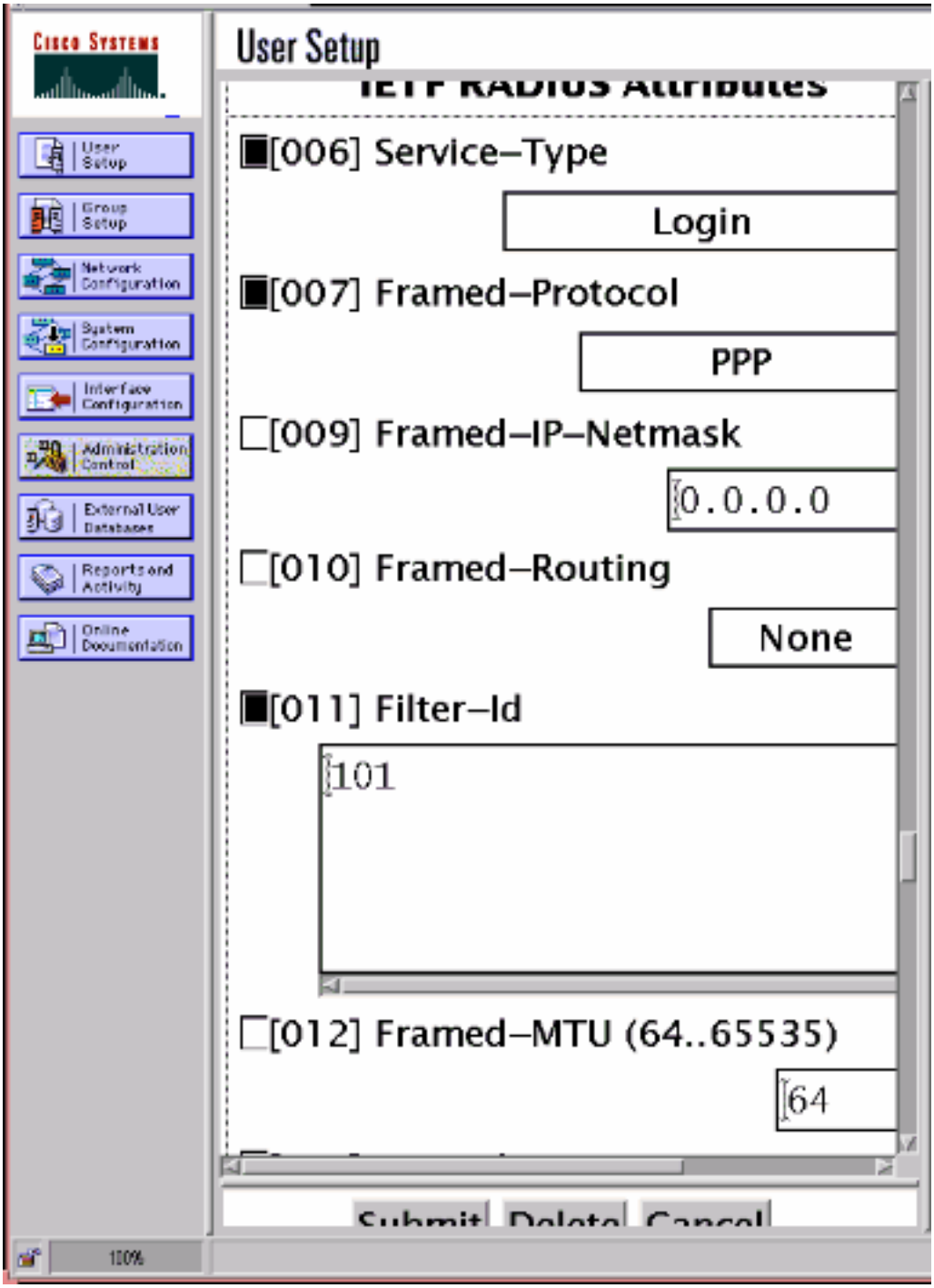
Èinoltre possibile definire un filtro nel concentratore VPN e quindi passare il numero di filtro da un server RADIUS (in termini RADIUS, l'attributo 11 è Filter-id), in modo che quando l'utente viene autenticato sul server RADIUS, il Filter-id venga associato a tale connessione. In questo esempio si presume che l'autenticazione RADIUS per gli utenti di VPN Concentrator sia già operativa e che sia necessario aggiungere solo l'ID filtro.

Definire il filtro su VPN Concentrator come nell'esempio precedente:



Configurazione server CSNT - Assegnazione filtro RADIUS

Configurare l'attributo 11, Filter-id sul server Cisco Secure NT su **101**:



Debug - Assegnazione filtro RADIUS

Se AUTHDECODE (1-13 Gravità) è attivato in VPN Concentrator, il log mostra che il server Cisco Secure NT invia l'elenco degli accessi 101 in basso nell'attributo 11 (0x0B):

```
207 01/24/2001 11:27:58.100 SEV=13 AUTHDECODE/0 RPT=228
0000: 020C002B 768825C5 C29E439F 4C8A727A     ...+v.%...C.L.rz
0010: EA7606C5 06060000 00020706 00000001     .v..............
0020: 0B053130 310806FF FFFFFF                   ..101......
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Solo a scopo di risoluzione dei problemi, è possibile attivare il debug del filtro quando si sceglie **Configurazione > Sistema > Eventi > Classi** e aggiungere la classe **FILTERDBG** con **Gravità a Registro = 13**. Nelle regole, modificare l'azione predefinita da Avanti (o Rilascia) a **Avanti e Registro** (o Rilascia e Registro). Quando il registro eventi viene recuperato in **Monitoraggio > Registro eventi**, dovrebbe contenere voci quali:

```
221 12/21/2000 14:20:17.190 SEV=9 FILTERDBG/1 RPT=62
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8

222 12/21/2000 14:20:18.690 SEV=9 FILTERDBG/1 RPT=63
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8
```

Informazioni correlate

- Negoziazione IPSec/protocolli IKE
- Domande frequenti su VPN 3000 Concentrator
- Supporto RADIUS
- Supporto Cisco VPN 3000 Concentrator
- Supporto client Cisco VPN 3000
- Supporto Cisco Secure ACS per Windows
- RFC (Request for Comments)
- Documentazione e supporto tecnico – Cisco Systems