

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

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Convenzioni](#)

[Configurazione VPN 3000](#)

[Filtri per un tunnel VPN da LAN a LAN](#)

[Configurazione VPN 3000 - Assegnazione filtro RADIUS](#)

[Configurazione server CSNT - Assegnazione filtro RADIUS](#)

[Debug - Assegnazione filtro RADIUS](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

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.

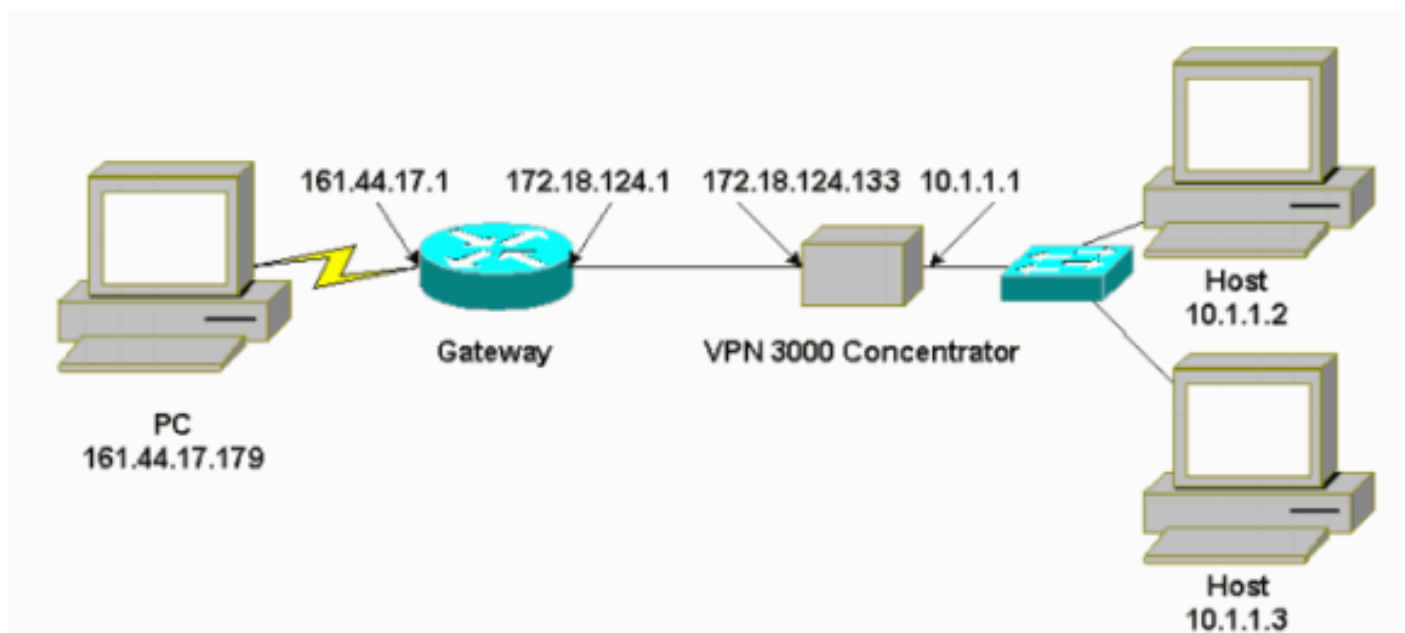
Componenti usati

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

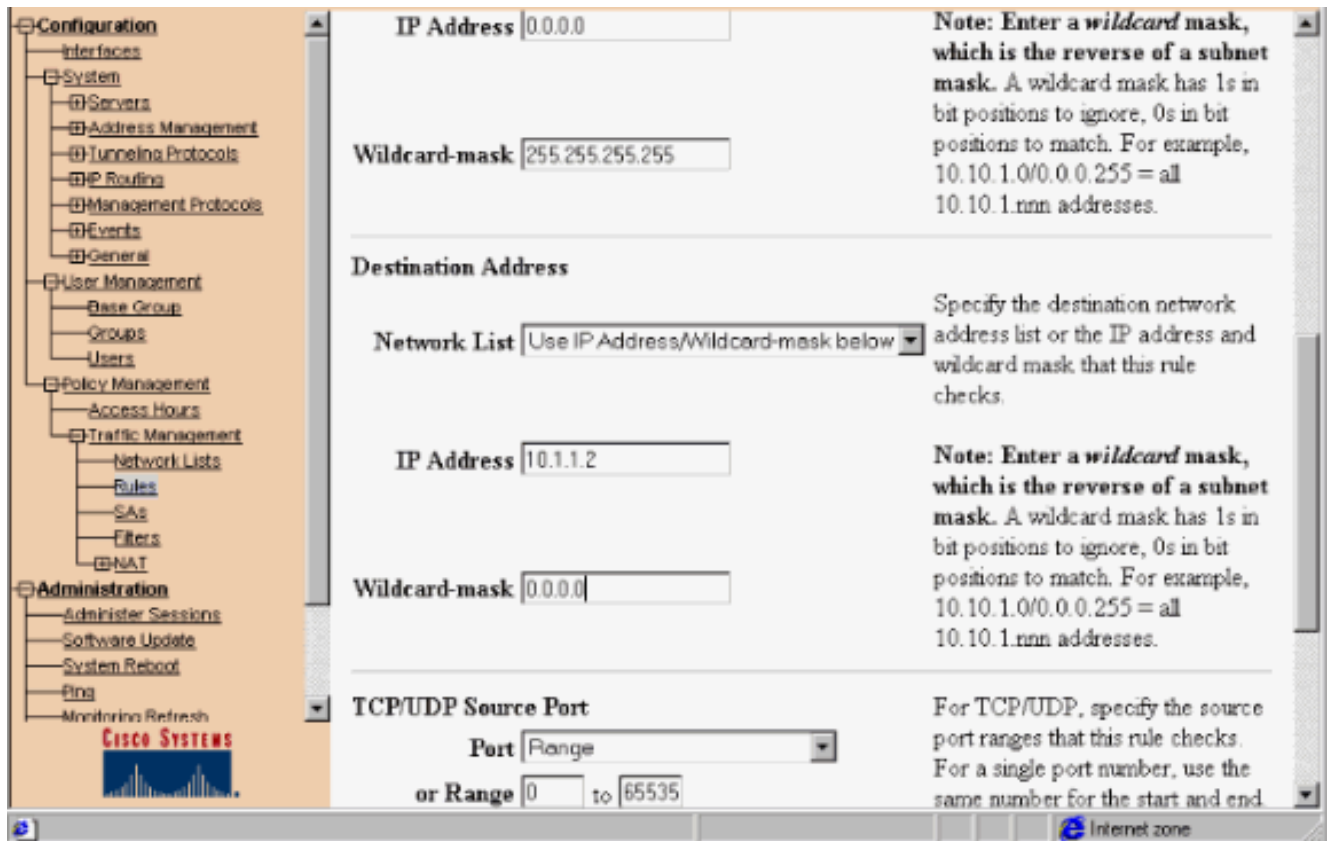
Completare questa procedura per configurare il concentratore VPN 3000.

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**

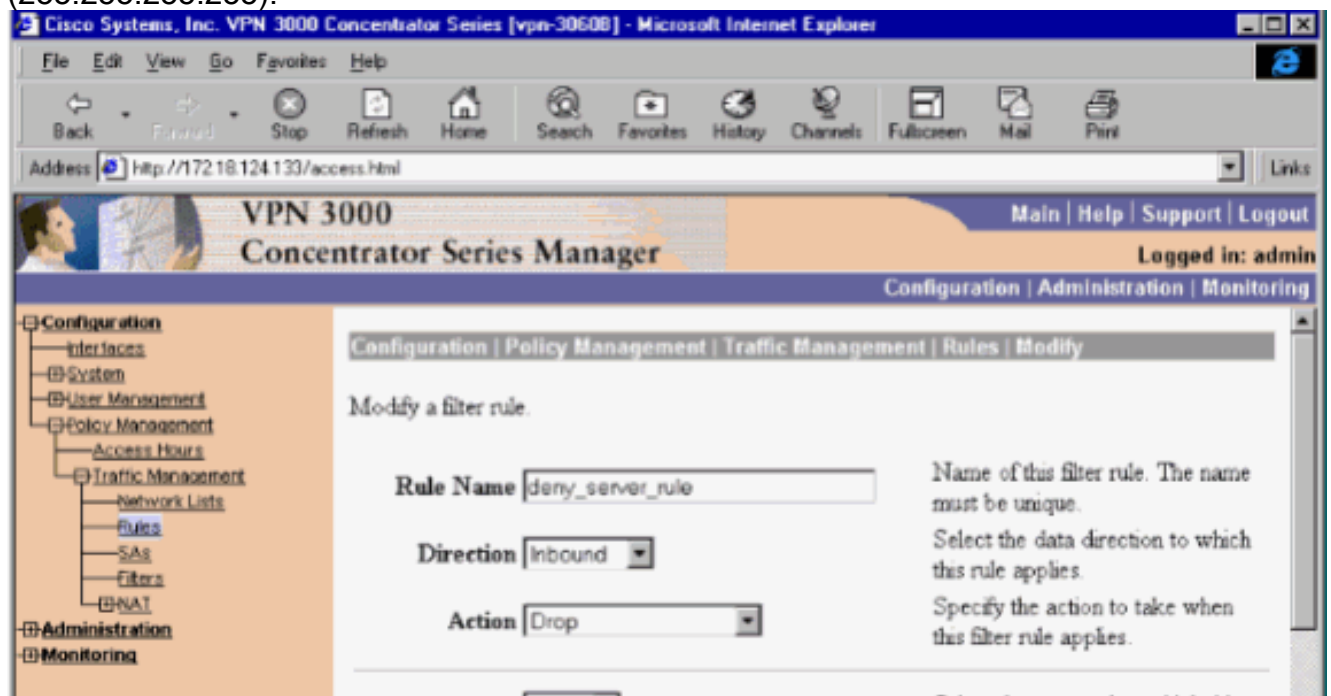
The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface in Microsoft Internet Explorer. The browser address bar shows `http://172.18.124.133/access.html`. The page title is "VPN 3000 Concentrator Series Manager" and the user is logged in as "admin". The navigation menu includes "Configuration", "Administration", and "Monitoring". The left sidebar shows a tree view with "Configuration" expanded to "Traffic Management" > "Rules". The main content area is titled "Configuration | Policy Management | Traffic Management | Rules | Add" and contains the following configuration fields:

- Rule Name:** `permit_server_rule` (Text input)
- Direction:** `Inbound` (Dropdown menu)
- Action:** `Forward` (Dropdown menu)
- Protocol:** `Any` (Dropdown menu)
- or Other:** (Text input)
- TCP Connection:** `Don't Care` (Dropdown menu)
- Source Address:** `Network List` (Dropdown menu)

Help text for each field is provided to the right of the input fields. The Cisco Systems logo is visible in the bottom left corner.



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**.

Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-30608] - Microsoft Internet Explorer

File Edit View Go Favorites Help

Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print

Address <http://172.18.124.133/access.html> Links

VPN 3000 Concentrator Series Manager Main | Help | Support | Log

Logged in: ac

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Filters | Add

Configure and add a new filter.

Filter Name Name of the filter you are adding. The name must be unique.

Default Action Select the default action to take when no rules on this filter apply.

Source Routing Check to have this filter allow IP source routed packets to pass.

Fragments Check to have this filter allow fragmented IP packets to pass.

Description

Add Cancel

CISCO SYSTEMS

Internet zone

4. Aggiungere le due regole a filter_with_2_rules:

Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-30608] - Microsoft Internet Explorer

File Edit View Go Favorites Help

Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print

Address http://172.18.124.133/access.html Links

VPN 3000 Concentrator Series Manager Main | Help | Support | Logout

Configuration | Administration | Monitoring

Save Needed

Configuration

- Interfaces
- System
- User Management
- Policy Management
 - Access Hours
 - Traffic Management
 - Network Lists
 - Rules
 - SAs
 - Filters
 - NAT
- Administration
- Monitoring

Add, remove, prioritize, and configure rules that apply to a filter.

Filter Name: filter_with_2_rules

Select an **Available Rule** and click **Add** to apply it to this filter.

Select a **Current Rule in Filter** and click **Remove**, **Move Up**, **Move Down**, or **Assign SA to Rule** as appropriate.

Select an **Available Rule**, then select a **Current Rule in Filter**, and click **Insert Above** to add the available rule above the current rule.

Current Rules in Filter	Actions	Available Rules
permit_server_rule (forward/in) deny_server_rule (drop/in)	<< Add << Insert Above Remove >> Move Up Move Down Assign SA to Rule Done	GRE In (forward/in) GRE Out (forward/out) IPSEC-ESP In (forward/in) IKE In (forward/in) IKE Out (forward/out) PPTP In (forward/in) PPTP Out (forward/out) L2TP In (forward/in) L2TP Out (forward/out) ICMP In (forward/in) ICMP Out (forward/out) RIP In (forward/in)

CISCO SYSTEMS

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

Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - Microsoft Internet Explorer

Address: http://172.16.124.133/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups | Modify servergroup

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow alphabetic-only passwords.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	filter_with_2_rules	<input type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the primary DNS server.
Secondary DNS		<input type="checkbox"/>	Enter the IP address of the secondary DNS server.

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**.



VPN 3000 Concentrator Series Manager

- Configuration
 - Interfaces
 - System
 - Servers
 - Address Management
 - Tunneling Protocols
 - PPTP
 - L2TP
 - IPSec
 - LAN-to-LAN
 - IKE Proposals
 - NAT Transparency
 - IP Routing
 - Management Protocols
 - Events
 - General
 - Client Update
 - Load Balancing
 - User Management
 - Policy Management
- Administration
- Monitoring

Configuration | System | Tunneling Protocols | IPSec | LAN-to-LAN | Modify

Modify an IPSec LAN-to-LAN connection.

Name

Interface

Peer

Digital Certificate

Certificate Entire certificate chain

Transmission Identity certificate only

Preshared Key

Authentication

Encryption

IKE Proposal

Filter

IPSec NAT-T

[Configurazione VPN 3000 - Assegnazione filtro RADIUS](#)

È inoltre 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:

Modify a configured filter.

Filter Name

101

Name of the filter. If the filter name is modified, the name must be unique.

Default Action

Drop

Select the default action to take when no rules are applied.

Source Routing

Check to allow the filter to allow routed packets to pass.

Fragments

Check to allow the filter to allow IP packets.

Description

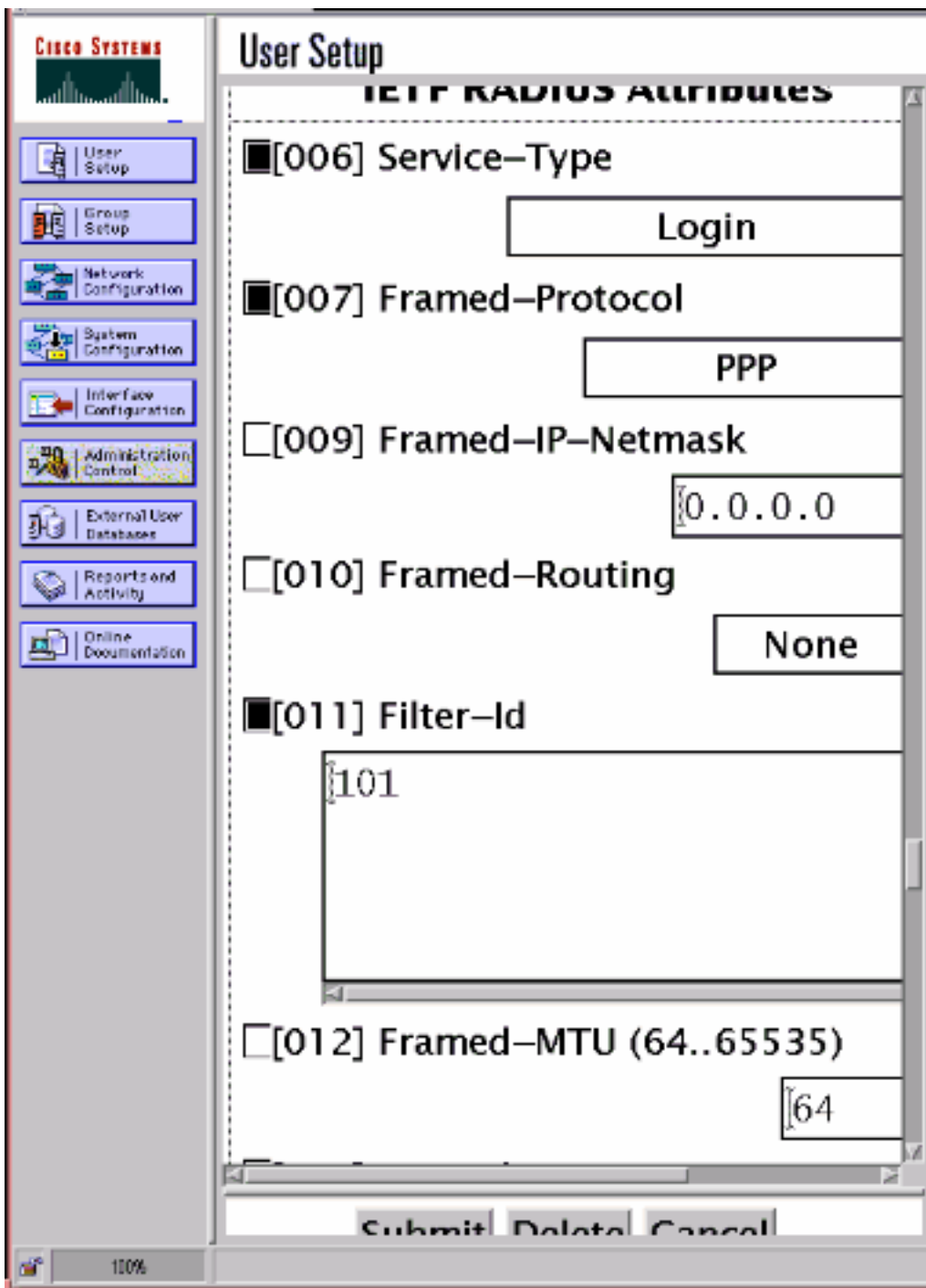
filter to allow access to 10.1.1.2

Apply

Cancel

[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 FFFFFFFF ..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](#)