

필터 및 RADIUS 필터 할당을 사용하여 차단을 위한 Cisco VPN 3000 Concentrator 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[네트워크 다이어그램](#)

[표기 규칙](#)

[VPN 3000 구성](#)

[LAN-to-LAN VPN 터널용 필터](#)

[VPN 3000 구성 - RADIUS 필터 할당](#)

[CSNT 서버 구성 - RADIUS 필터 할당](#)

[디버그 - RADIUS 필터 할당](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 샘플 컨피그레이션에서는 필터를 사용하여 사용자가 네트워크 내에서 하나의 서버(10.1.1.2)에만 액세스하고 다른 모든 리소스에 대한 액세스를 차단하도록 허용하고자 합니다. Cisco VPN 3000 Concentrator는 필터를 사용하여 네트워크 리소스에 대한 IPsec, PPTP(Point-to-Point Tunneling Protocol) 및 L2TP 클라이언트 액세스를 제어하도록 설정할 수 있습니다. 필터는 라우터의 액세스 목록과 유사한 규칙으로 구성됩니다. 라우터가 구성된 경우:

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

VPN Concentrator는 규칙을 사용하여 필터를 설정하는 것과 같습니다.

첫 번째 VPN Concentrator 규칙은 **permit_server_rule**이며, 이는 라우터의 `permit ip any host 10.1.1.2` 명령과 같습니다. 두 번째 VPN Concentrator 규칙은 **deny_server_rule**이며 이는 라우터의 `deny ip any` 명령과 같습니다.

VPN Concentrator 필터는 **filter_with_2_rules**이며, 라우터의 101 액세스 목록과 같습니다. **permit_server_rule** 및 **deny_server_rule**(그 순서대로)을 사용합니다. 필터를 추가하기 전에 클라이언트가 제대로 연결할 수 있다고 가정합니다. VPN Concentrator의 풀에서 IP 주소를 수신합니다.

[PIX/ASA 7.x ASDM을 참조하십시오. PIX/ASA 7.x가 VPN 사용자의 액세스를 차단하는 시나리오에 대해 자세히 알아보려면 \[Network Access of Remote Access VPN Users\\(원격 액세스 VPN 사용자\\)의 네트워크 액세스\]\(#\)를 제한합니다.](#)

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

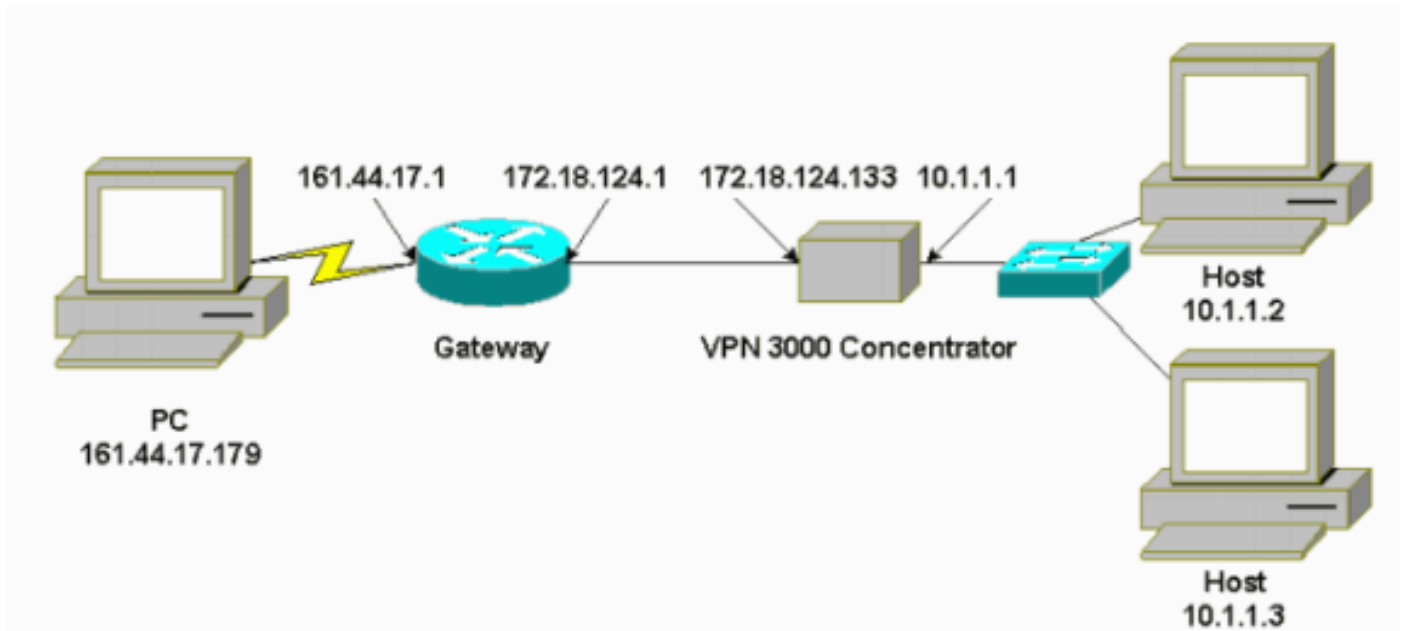
사용되는 구성 요소

이 문서의 정보는 Cisco VPN 3000 Concentrator 버전 2.5.2.D를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

VPN 3000 구성

VPN 3000 Concentrator를 구성하려면 다음 단계를 완료하십시오.

1. Configuration(구성) > Policy Management(정책 관리) > Traffic Management(트래픽 관리) > Rules(규칙) > Add(추가)를 선택하고 다음 설정으로 permit_server_rule이라는 첫 번째 VPN Concentrator 규칙을 정의합니다. 방향 - 인바운드 작업 - 전달소스 주소 - 255.255.255.255 대상 주소 - 10.1.1.2와일드카드 마스크 - 0.0.0.0

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The browser title is "Cisco Systems, Inc. VPN 3000 Concentrator Series [vpn-3060B] - Microsoft Internet Explorer". The 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 "Configuration" menu is expanded to show "Policy Management" > "Traffic Management" > "Rules" > "Add". The main content area is titled "Configuration | Policy Management | Traffic Management | Rules | Add".

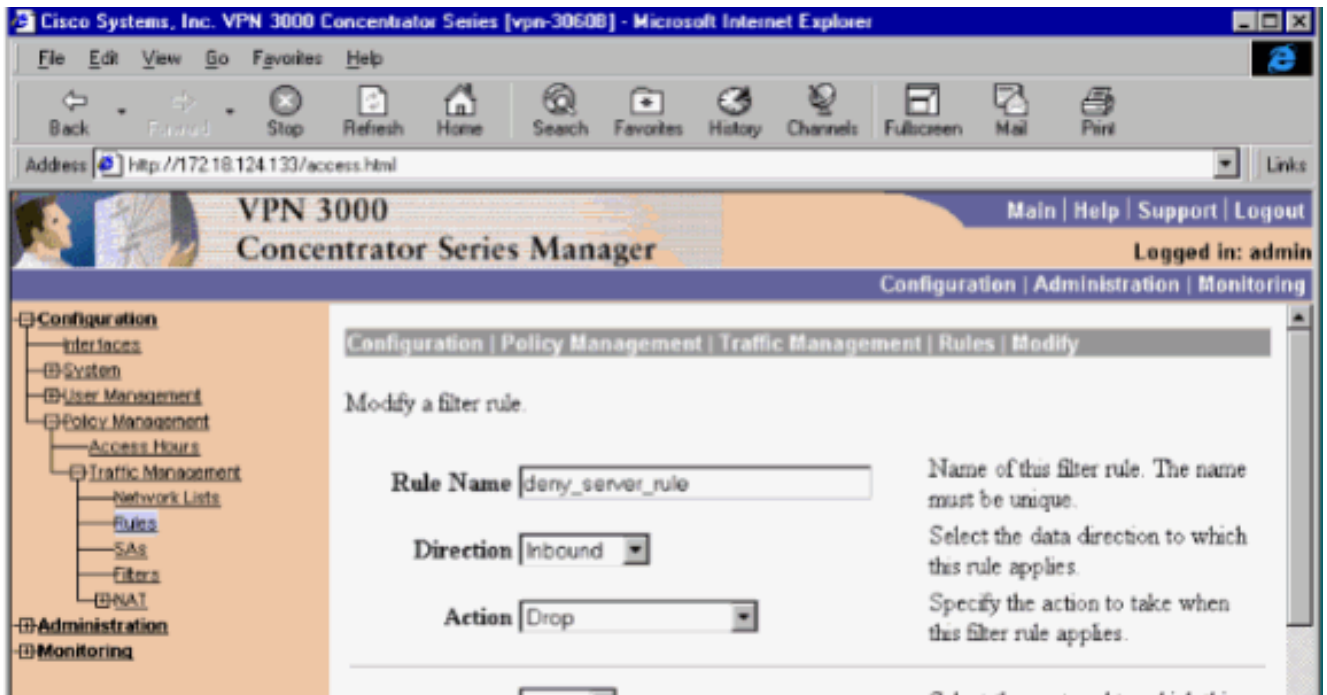
The configuration form for adding a new filter rule is displayed. The rule name is "deny_server_rule". The direction is "Inbound". The action is "Deny". The protocol is "Any". The TCP connection is "Don't Care".

The "Source Address" section is expanded to show the "Network List" dropdown set to "Use IP Address/Wildcard-mask below". The "IP Address" field is "0.0.0.0" and the "Wildcard-mask" field is "255.255.255.255". A note states: "Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses."

The "Destination Address" section is expanded to show the "Network List" dropdown set to "Use IP Address/Wildcard-mask below". The "IP Address" field is "10.1.1.2" and the "Wildcard-mask" field is "0.0.0.0". A note states: "Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses."

The "TCP/UDP Source Port" section is expanded to show the "Port" dropdown set to "Range". The "or Range" field is "0" to "65535". A note states: "For TCP/UDP, specify the source port ranges that this rule checks. For a single port number, use the same number for the start and end."

2. 동일한 영역에서 다음 기본값으로 deny_server_rule이라는 두 번째 VPN Concentrator 규칙을 정의합니다. 방향 - 인바운드작업 - 삭제모든 항목의 소스 및 대상 주소 (255.255.255.255):



3. Configuration > Policy Management > Traffic Management > Filters를 선택하고 filter_with_2_rules 필터를 추가합니다

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

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

CISCO SYSTEMS

Internet zone

4. filter_with_2_rules에 두 규칙을 추가합니다

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

Configuration

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

Save Needed

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. Configuration > User Management > Groups를 선택하고 그룹에 필터를 적용합니다

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

LAN-to-LAN VPN 터널용 필터

VPN Concentrator 코드 3.6 이상에서 각 LAN-to-LAN IPsec VPN 터널에 대한 트래픽을 필터링할 수 있습니다. 예를 들어, 172.16.1.1 주소를 사용하여 다른 VPN Concentrator에 LAN-to-LAN 터널을 구축하고 다른 모든 트래픽을 거부하는 동시에 호스트 10.1.1.2 터널 액세스를 허용하려는 경우 Configuration(구성) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPsec > LAN-to-LAN > Modify(수정)를 선택하고 **Filter(필터)** 아래에서 filter_with_2_rules를 선택할 수 있습니다.



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

VPN 3000 구성 - RADIUS 필터 할당

또한 VPN Concentrator에서 필터를 정의한 다음 RADIUS 서버에서 필터 번호(RADIUS 용어로 특성 11은 필터 ID)를 전달하여 사용자가 RADIUS 서버에서 인증되면 필터 ID가 해당 연결과 연결될 수 있습니다. 이 예에서는 VPN Concentrator 사용자에게 대한 RADIUS 인증이 이미 작동 중이며 Filter-id만 추가되어야 한다고 가정합니다.

이전 예와 같이 VPN Concentrator에서 필터를 정의합니다.

Modify a configured filter.

Filter Name

101

Name of the filter to be modified. The name must be unique.

Default Action

Drop

Select the action to be applied to traffic when no rules are found.

Source Routing

Check to allow the filter to apply to source-routed packets.

Fragments

Check to allow the filter to apply to IP packet fragments.

Description

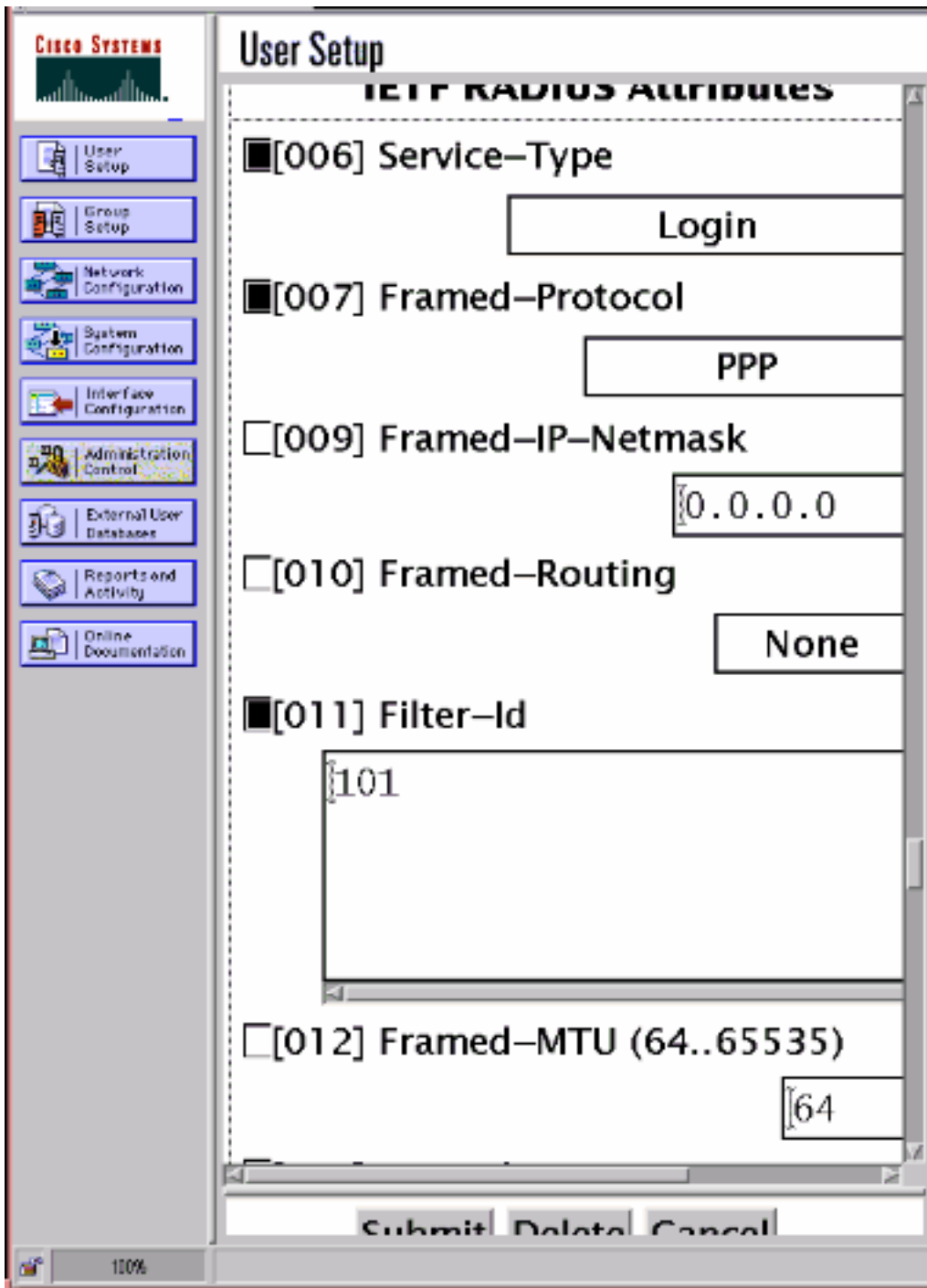
filter to allow access to 10.1.1.2

Apply

Cancel

[CSNT 서버 구성 - RADIUS 필터 할당](#)

Cisco Secure NT 서버에서 특성 11, Filter-id를 101로 구성합니다.



디버그 - RADIUS 필터 할당

AUTHDECODE(1-13 Severity)가 VPN Concentrator에 있는 경우, 로그에 Cisco Secure NT 서버가 11(0x0B) 특성:

```
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.....
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

문제 해결 목적으로만, 구성 > 시스템 > 이벤트 > 클래스를 선택하고 심각도 = 13인 FILTERDBG 클래스를 로그에 추가할 수 있습니다. 규칙에서 기본 작업을 전달(또는 삭제)에서 전달 및 로그(또는 삭제 및 로그)로 변경합니다. 이벤트 로그가 Monitoring(모니터링) > Event Log(이벤트 로그)에서 검색되면 다음과 같은 항목이 표시되어야 합니다.

```
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
```

관련 정보

- [IPSec 협상/IKE 프로토콜](#)
- [VPN 3000 Concentrator FAQ](#)
- [RADIUS 지원](#)
- [Cisco VPN 3000 Concentrator 지원](#)
- [Cisco VPN 3000 클라이언트 지원](#)
- [Windows용 Cisco Secure ACS 지원](#)
- [RFC\(Request for Comments\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)