

Can a core switch restrict a specific IP address



Article Overview

Yes, a core switch can restrict a specific IP address using IP-based Access Control Lists (ACLs) or access profiles.

Using IP Access Control Lists (ACLs)

A common method to restrict a specific IP address is to configure an IP ACL on the switch. ACLs allow you to define rules that permit or deny traffic from specific IP addresses or subnets. On a Layer 3 switch, you can create an ACL that denies traffic from the target IP and apply it inbound on the relevant VLAN interface or port. For example, on a Cisco switch, you could use:

```
ip access-list extended BLOCK_IP deny ip host 192.168.1.100 any permit ip any  
anyinterface vlan 10 ip access-group BLOCK_IP in
```

This configuration blocks all traffic from 192.168.1.100 while allowing other IPs to communicate normally .

Access Profiles and Management Restrictions

Some managed switches, like Cisco SG series, allow access profiles to restrict management access to specific IP addresses. You can create a profile that permits only the desired IP and apply it to services such as SSH, HTTP, or Telnet. This method is particularly useful for securing switch management interfaces

Article Content

How to create a Access list on core switch to bloxk all

Helpp Everyone, I am trying to create a Access-List on my Core Switch, in which I want to

Restricting a VLAN to only access one IP address on other VLAN

Hello, I currently have an SG200-26 26-Port Gigabit Smart Switch using all default settings and I am trying to gather

Mac filtering - How do you block a MAC address on your network.

I have a Cisco network with multiple Layer-2 switches (CAT & IOS) connecting back to Core Layer-3 switches.

Solved: Restricting vlan access

They minute we would restrict access, all other vlans would lose connectivity to this particular vlan (services). Is there

Restrict Access to Cisco Switch Based on IP Address

In this article, I'll walk you through the steps to configure access profiles and profiles rules for your Cisco switch. Note:

Azure Storage firewall rules and network access control

Configure Azure Storage firewall rules to control network access. Restrict traffic by IP address, virtual network, or

Solved: Core switch ACL question

I have a core switch with around 20 vlans connected. I need to be able to do the following: 1) Permit access from a

Limit SSH access to specific clients by IP address

You can limit which hosts can connect by configuring TCP wrappers or filtering network

Cisco switch limiting SSH access to specific SVI interface

Dear All, we've Cisco core switch and wanted to limit ssh access to specific SVI interface, at the moment we've a

Port Security on Switches | Shutdown | Protect | Restrict ★ CCNA

Switch Port Security is the security mechanism used in switches. With this mechanism, a specific port of a switch can be protected

How to Restrict Access to IPs

Why Do You Need IP Restriction? Here's the deal: some folks are constantly up to no good, snooping about in places

only permit specific ip address on a switch port

I'm looking for a solution to only permit a specific ip address on a port that I connect a client to. For example, I give a

Solved: SSH Access On Specific IP

Hi, I have configured 10 interface vlan on my cisco core switch 6509. However I want my users SSH it on

UniFi Switch Settings - Ubiquiti Help Center

UniFi Switch Settings let you configure how your network switches handle traffic, VLANs, port behavior, and Layer 3 isolation. These

Switch ACLs: how to config ACL to permit internet access but restrict ...

You can have a hybrid environment where some VLANs are routed on the switch, and others on the firewall. Use a

Configuring Access Policies on Aruba Switches

To restrict certain types of traffic on physical ports of Aruba switches, you can configure ACLs from the Aruba Central UI. To create

How to Lock Down Cisco Switch Ports with Port Security (2025 Guide ...

Port Security is a Layer 2 security feature used on Cisco switches to restrict input to an interface by limiting and

Using a Cisco Core Switch I want to block a specific range of IP ...

I have two VLANs defined in the core switch: VLAN 504 - 10.10.10.0 255.255.255.0
VLAN 700 - 192.168.0.0 255.255.255.0 Both

Securing the network by using IP access control lists

If you want to be taken seriously as a Cisco network administrator, you have to know how to configure your switches and routers to

Switchport Port Security Explained With Examples

You have two options for mapping MAC addresses to switch ports: static and dynamic. The static method is more

Only allow Specific Traffic to a VLAN

Have a quick question regarding inter-vlan routing on a 3750. Overview of network is ISP --> ASA --> 3750 (acting as

VLAN Access Control Lists

All non-IP protocols are access-controlled through MAC addresses and Ethertype using MAC VLAN maps. (IP traffic is not access

Filtering traffic between ports on an ethernet switch

Switching is Layer 2 functionality and the kind of ACL you want to create should be acting on Layer 3, the IP layer

Google Translate

Google's service, offered free of charge, instantly translates words, phrases, and web pages between English and over 100 other

ACL to block management on all but one VLAN interface

Our core switch handles all our VLAN interfaces and you can telnet to the switch using any one of the VLAN interface

Solved: Block a Single IP address

I seem to have a rogue DHCP server on the network and have not been able to locate it. The switch shows it

Contact Us

For more information, pricing, or custom solutions, please contact us:

Website: <https://www.thebucketlistbook.co.za>

Email: sales@thebucketlistbook.co.za

Phone: +33 1 42 78 39 16

Address: 10 Rue de la Paix, 75002 Paris, France

This document is for informational purposes only. Specifications subject to change without notice.

