

Switches restrict access terminal IPs

Article Overview

Switches can restrict access to specific terminal IP addresses using IP-based access control lists (ACLs) or port security features to enhance network security.

Methods to Restrict Access

1. IP Limit / Management ACLs Many switches allow you to configure an IP Limit or management ACL to control which IP addresses can access the device. This involves first blocking all IP addresses and then explicitly allowing only authorized IPs. For example, Cisco devices can restrict Telnet, SSH, or web access to specific IPs by defining allowed addresses and applying them to management services . Juniper devices use firewall filters applied to the loopback interface to permit only certain IPs for management access . 2. Port Security Port security restricts which devices can connect to a specific switch port based on MAC addresses. You can configure a port to allow only one or a limited number of devices, either statically or dynamically using sticky MAC addresses. Unauthorized devices attempting to connect can be blocked, logged, or trigger a port shutdown . This method complements IP-based restrictions by controlling physical access at the port level. 3. UniFi Switch ACLs UniFi switches support IP and MAC ACLs to isolate devices within the same VLAN or manage inter-VLAN traffic. ACL rules are processed top-to-bottom, with specific allow rules placed before general block rules. MAC ACLs are applied before IP ACLs, and these can be used to enforce device isolation or performance-driven traffic control .

Best Practices

- o Apply "deny all" first, then allow specific IPs to prevent accidental access.
- o Use commit confirmed (on Juniper) or equivalent rollback features to avoid locking yourself out.
- o Combine IP ACLs with port security for layered protection.
- o Monitor logs for security violations to detect unauthorized access attempts.
- o Limit management services (SSH, Telnet, HTTP/HTTPS) to only those required for administration . By implementing these methods, you can ensure that only authorized terminals with specific IP addresses can access your switches, significantly improving network security.

Secret password type 4 is not supported. Information About Controlling Switch Access with Passwords and Privileges

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password

Switches restrict access terminal IPs

Controlling Access to a VTY via SSH to a specific IP helps improve security to your Cisco Switches or Routers. You

We will learn Switch Port Security, how to configure port security on Cisco switches, violation modes: Shutdown, Protect, Restrict

In an environment where all users are known to you, you can use a switch with the default configuration. However,

This module allows you to limit the packet per second (pps) rate on a per destination IP or per destination port base. As opposed to

Typically, you want network administrators to have access to your switch while you restrict access to users who dial

This example shows how to limit management access to Juniper Networking devices based on a specific set of allowed IP

The SSH Terminal-Line Access feature enables users to configure their router with secure access and perform the

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

Introduction This document describes information to secure your Cisco IOS XE Software system devices, which increases the overall

An Access Control List (ACL) is a list of rules that control and filter traffic based on source and destination IP addresses or Port

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

Limiting access to vty lines based on source IP with access list To configure basic access control on switches (like

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

I thought I had IP restrictions set to my 3750G Cisco switch to my single IP, but I just accessed it from another IP and

Switches restrict access terminal IPs

Web: <https://www.kremgroup.co.za>

