Block IP addresses on the core switch

Overview

Step 1: Review the switch configuration to verify that an ingress ACL is applied to all external or CE-facing interfaces. The Cisco PE switch must be configured to block any traffic that is destined to the IP core infrastructure. Core network elements must not be accessible from any external host. Protecting the core from any attack is vital for the integrity and privacy of customer. There is a DMP receiver on our network that is receiving messages predictably one hour a week. I believe the messages are coming from a panel on our network. The classic Access Control List (ACL) is the core mechanism on Cisco network devices (routers, switches etc) which is mainly used for traffic filtering. In this article we will examine a different type of ACL, called the Vlan Access.

Block IP addresses on the core switch

Here''s the Cisco CLI Switch Command cheat sheet you need for configuring and managing Cisco switches The Cisco Command-Line Interface (CLI) is a core tool used by network ...

Setting up VLAN ACLs on your Cisco switch involves a series of strategic commands and steps. We will cover these essential commands and guide you through the configuration process ...

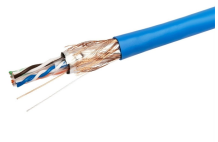
Configure protection for the IP core to be implemented at the edges by blocking any traffic with a destination address assigned to the IP core infrastructure. Step 1: Configure an ingress ACL to ...

To demonstrate how you can use ACL filtering, I will block the telnet session from Host1 to Host2 using an ACL applied inbound on the SVI interface for VLAN10 of the switch.

In this article, I''ll walk you through the steps to configure access profiles and profiles rules for your Cisco switch. Note: The following method I am going to describe also allows you to restrict ...

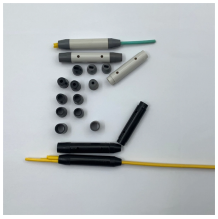
Step 1: Configure an ingress ACL to discard and log packets destined to the IP core address space. Step 2: Apply the ACL inbound to all external or CE-facing interfaces. IP addresses ...

You can have a hybrid environment where some VLANs are routed on the switch, and others on the firewall. Use a trunk port to connect the switch to the firewall, and then you can have all ...

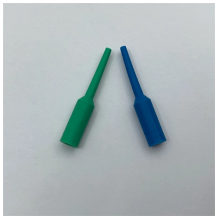


The switch is doing layer 2 forwarding, looks at the destination mac address, and forwards the packet to the receiver. So you need something that operates at layer 2.

We can set the configuration (as you''ll see below) to IP filter traffic in Cisco layer 3 switches, such as the Nexus switches, between two different SIV''s/VLANs. Let''s dive in! The ACLs work by blocking ...



Is this a catalyst or nexus switch? Basically you will create a ACL (access list) either allowing or denying IPs and you apply the ACL to the VLAN interface.



Here''s the Cisco CLI Switch Command cheat sheet you need for ...

Contact Us

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

Website: https://www.indzawo.co.za
Email: sales@indzawo.co.za
Phone: +27 71 296 8473
Address: 22 Quantum Street, Midrand, 1685, Gauteng, South Africa

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