Huawei Core Switch Blacklist

Overview

Run the blacklistblacklist-idaclacl-number1 command to create an IPv4 blacklist. The ACL referenced by the IPv4 blacklist can be a basic ACL, an advanced ACL, or a Layer 2 ACL.

Key Takeaways

Huawei core switches use blacklists to block traffic from untrusted IP addresses or interfaces, leveraging ACLs to filter packets dynamically or manually.

Overview of Blacklist Functionality

A blacklist on Huawei switches is a security feature that discards packets from or destined for specified IP addresses, interfaces, or VLANs to protect the network from malicious or untrusted sources. Blacklists can be applied to both IPv4 and IPv6 traffic, and they work in conjunction with Access Control Lists (ACLs) to define which packets are blocked. Packets matching the ACL rules are discarded regardless of permit or deny rules in the ACL.

Types of BlacklistsIPv4 Blacklist: Can reference basic, advanced, or Layer 2 ACLs. It can also be configured to discard packets directly in the forwarding chip for supported models. IPv6 Blacklist: Only advanced ACLs can be applied, and in some models, only the source IP address can be matched.

Dynamic Blacklist: Automatically adds IP addresses to the blacklist when a packet matches an intrusion prevention signature. The timeout interval for removal is determined by the IPS signature database. Manual Blacklist: Administrators can manually add or remove IP addresses, interfaces, or VLANs to the blacklist.

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved

Configuration Highlights

Creating a Blacklist: Use commands like blacklist blacklist-id acl acl-number for IPv4 or blacklist blacklist-id acl ipv6 acl-number for IPv6. Hard Drop: Some models support blacklist blacklist-id acl acl-number hard-drop to discard packets directly in the forwarding chip.

Interface and VLA

N Blocking: Blacklists can be applied to specific interfaces or VLAN ranges, with interface numbers and VLAN IDs specified in the configuration. Maximum Blacklists: A device can support up to 8 blacklists in an attack defense policy. Service Interfaces Only: Blacklists take effect on service interfaces, not management interfaces.

Best Practices

Enable the Blacklist Function: Ensure the blacklist feature is enabled using commands like firewall blacklist enable for dynamic entries. Monitor Impact: Evaluate the effect of blocking IP addresses, especially if NAT or proxy services are involved, to avoid unintended service disruptions.

Use AC

Ls Wisely: Advanced ACLs provide more granular control, including matching source and destination IPs, protocols, and ports. Combine with Whitelists: To allow trusted traffic while blocking malicious sources, configure whitelists alongside blacklists.

Regulatory Considerations

Huawei equipment is included in certain national security blacklists in some regions, which may affect deployment in sensitive environments. Administrators should ensure compliance with local regulations when configuring network security policies. By properly configuring blacklists, Huawei core switches can effectively prevent unauthorized access, mitigate attacks, and safeguard network resources.

Article Content

Configuring a Blacklist

Run the blacklistblacklist-idaclacl-number1 command to create an IPv4 blacklist. The ACL referenced by the IPv4 blacklist can be a basic ACL, an advanced ACL, or a Layer 2 ACL. For details about ACL

blacklist

To defend against malicious packet attacks, the device uses ACLs to add users with the specific characteristic into a blacklist and discards the packets from the users in the blacklist. A maximum of

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved

01-19 BLACKLIST CONFIGURATION

Blacklist matching is simple and can be used to quickly filter packets with specified IP addresses. If an IP address is considered untrusted, you can add the IP address to the blacklist.

01-17 STA BLACKLIST AND WHITELIST CONFIGURATION

Guests or visiting employees sometimes bring their laptops to this AP''s coverage area. If only STAs of guests or visiting employees are not allowed to connect to the wireless network, the enterprise can

Configuring the Blacklist/Whitelist to Block or Allow ...

You can configure the blacklist to block access requests from IP addresses or configure the whitelist to allow them. This section describes how to add a blacklist or whitelist item.

List of Equipment and Services Covered By Section 2 of The Secure ...

Below is the list of covered equipment subject to importation and/or marketing prohibitions. Equipment added to the Covered List 2024 or earlier.

Managing the Blacklist and the Whitelist_Cloud Firewall-Huawei Cloud

After adding a blacklist or whitelist, you can edit or delete it. This section describes how to perform the following operations: Log in to the CFW console. Click in the upper left corner of the

Huawei: Banned and Permitted In Which Countries? List and FAQ

Where is Huawei Technologies banned & permitted for 5G networking business & smartphones? Here''s a list of countries, companies, 5G wireless network projects & their Huawei

Criticism of Huawei

Huawei has faced allegations, primarily from the United States and its allies, that its wireless networking equipment could contain backdoors enabling surveillance by the Chinese government.

U.S. Restrictions on Huawei Technologies: National Security, Foreign ...

There has been support in Congress for policies and restrictions aimed at securing U.S. networks and supply chains, and limiting Huawei''s presence in global networks. In 2017, Congress passed

Campus Switches | Huawei Enterprise

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved

Huawei campus switches offer high-performance, secure, and reliable switching for enterprises, governments, finance and manufacturing networks. Learn more.

Checking Whether a Blacklist Is Configured

Checking Whether a Blacklist Is Configured After a cpu-defend blacklist is configured, the switch discards the packets sent from the blacklisted users.

blacklist

This document lists all the commands for configuring and maintaining the CX310, CX311, CX312,and CX110 (switch modules for short) of the . By reading this document, you can learn about the syntax,

Data Center Switches

Data Center Switches CloudEngine Data Center Switches — Ethernet switches widely used in diverse applications and in different network sizes, in both data centers and high-end campus networks —

Huawei CloudEngine S6750-H Series 10GE Switches Datasheet

Introduction Huawei CloudEngine S6750-H series 10GE switches are next-generation enterprise-class core and aggregation switches that offer high performance, high reliability, cloud management, and

blacklist

This document provides the configuration commands of each feature supported by the CX11x&CX31x&CX91x series switches module, including the syntax, view, default level, description,

Criticism of Huawei

In September 2014, Huawei faced a lawsuit from T-Mobile US, which alleged that Huawei stole technology from its Bellevue, Washington, headquarters. T-Mobile claimed that Huawei''s employees

Configuring a Blacklist

To defend against malicious packet attacks, the device uses ACLs to add users with the specific characteristic into a blacklist and discards the packets from the users in the blacklist. A maximum of

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved

Contact Us

Continue your research online:

Website: https://cgweb.co.za
Technical inquiry: https://cgweb.co.za/project-enquiry.html

This document is for preliminary research. Verify specifications against current standards, product documentation and project requirements.

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved