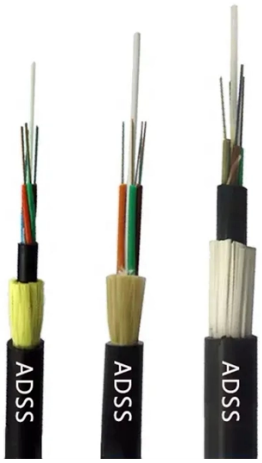
Interconnecting the core switch and WAF



Overview

Configuring Physical Links (Aggregated Links Interconnecting the The aggregated links interconnecting the core switch with egress firewalls and standalone.

Key Takeaways

To interconnect a WAF with a core switch, configure physical or aggregated links on the core switch and ensure proper WAF deployment and rule management for secure traffic flow.

Physical and Aggregated Link Configuration

To connect a WAF to a core switch, you typically use aggregated Ethernet links (Eth-Trunks) to ensure redundancy and higher bandwidth. The process involves: Access the core switch management interface (e.g., iMaster NCE-Campus for Huawei switches). Navigate to Provision > Device > Site Configuration, then select Switch > Interface.

On the interface panel, select the physical interfaces that will connect to the WAF and aggregate them into an Eth-Trunk (e.g., Eth-Trunk 3).

Assign the Eth-

Trunk I

D and apply the configuration. Repeat for additional trunks if multiple links are required for redundancy or load balancing. This setup ensures that traffic between the core network and the WAF is highly available and scalable, reducing the risk of a single point of failure.

© 2026 DOLPHIN FIBER SYSTEMS - All rights reserved

WAF Deployment Considerations

When deploying a WAF in front of your web applications: Use a defense-in-depth strategy, placing the WAF between the core switch and the application servers to filter malicious traffic before it reaches critical systems.

Configure the WA

F with OWASP Core Rule Sets (CRS) and any custom managed rules to protect against common attacks like SQL injection, XSS, and other OWASP Top 10 threats. Consider tuning rules to reduce false positives, which can block legitimate traffic and impact user experience. Automation tools like Azure CLI, PowerShell, or Terraform can help maintain consistent rule sets across updates.

Best Practices

Redundancy: Use multiple aggregated links to prevent downtime. Monitoring: Enable logging and alerts on the WAF to detect and respond to attacks quickly. Testing: Validate traffic flow and rule effectiveness before production deployment.

Updates: Regularly update the WAF rules to address emerging threats while preserving custom exclusions. By combining proper core switch link configuration with well-tuned WAF deployment, you can ensure secure, reliable, and high-performance traffic management for your network.

Article Content

Configuring Physical Links (Aggregated Links Interconnecting the

The aggregated links interconnecting the core switch with egress firewalls and standalone WACs need to be manually configured on the core switch through iMaster NCE-Campus.

Configuring Physical Links (Aggregated Links Between the Core

The aggregated links between the core, aggregation, and access switches have been configured using the network plan import function during site creation, and the aggregated links between the core

Solved: Re: Recommendation for a connection between Core Switch

Hello, I am asking myself what others recommend for the connection between core switch and Firewall. The setup is the following: Two Catalyst 9300 Core switches in stack. The stack

Solved: Connectivity from Core to Firewall

© 2026 DOLPHIN FIBER SYSTEMS - All rights reserved

You want to simply extend L2 all the way from the access switch to the firewall so all ports need to be L2 until they get to the L3 interface on the firewall. One thing to check is your access

Deployment Modes

High availability deployments are available exactly as with physical appliances. See the WAF Administration Guide for details. Some possible deployments are depicted in the following

Core Switch vs. Distribution Switch vs. Access Switch

Comprehensive guide to Core, Distribution, and Access Switches. Roles in the network and important parameters explained.

AWS WAF, AWS Firewall Manager, AWS Shield Advanced, and AWS

Both experiences provide access to the same core AWS WAF functionality, but they differ in how you configure and manage your web application protections. AWS WAF offers two options for using the

F5 BIG-IP SSL Orchestrator Configuration with Advanced WAFaaS

This article shows how to configure SSL Orchestrator with F5 Advanced WAF as a Service (WAFaaS) using the Service Catalog.

Architecture

To ensure that all the traffic goes through the endpoints of Network Firewall, you must update the routing table, as the diagram shows. We recommend that you route all the egress traffic from the application

A beginner''s guide to WAF: When and how should you

A beginner''s guide to WAF: When and how should you use a Web Application Firewall? Some network engineers think that Web Application

Load balancing Metaswitch EAS WAF Gateway: A step-by-step guide

While the WAF provides application-layer security against attacks like SQL injection and XSS, the load balancer acts as an initial shield. It can distribute and absorb Distributed Denial of

Tutorial: Create an application gateway with a Web Application

Applies to: Application Gateway V2 This tutorial shows you how to use the Azure portal to create an Application Gateway with a Web Application Firewall (WAF). The WAF uses

The 7-Layer OSI Model in Cybersecurity | StormWall

© 2026 DOLPHIN FIBER SYSTEMS - All rights reserved

The core strength of the OSI model lies in dividing the data transmission process into independent layers. Each layer can use its own tools, protocols, and security measures without affecting the others.

What Is a Web Application Firewall (WAF)? A Complete Guide to How

A Web Application Firewall, commonly abbreviated as WAF, is a critical cybersecurity technology designed to protect web applications from a wide range of attacks that target their

Configuring the Core Switch

In this scenario, IP addresses of the interfaces connecting the core switch to the BRASs and firewalls and OSPF need to be configured on the core switch, so as to implement connectivity between the

Connecting Core switch to firewall

Hi guys, I have a 3750X four-switch stack acting as the core of a fairly simple LAN. All I need to achieve (and this seems inordinately hard, but it is entirely likely that I''m just being dense) is

switching

This is general design question which all network designers may have. i will explain it very simply. if you want to apply security filtering profiles for inter VLAN routing, its good to have a trunk

Solved: Firewall to 2 core switches

Look at this picture and tell me, is it possible to add another core switch and have them wired to firewall so, that it could improve availability (fault tolerance) to the design? I know how it

© 2026 DOLPHIN FIBER SYSTEMS - All rights reserved

Contact Us

Continue your research online:

Website: https://dolphinspreschool.co.za
Technical inquiry: https://dolphinspreschool.co.za/project-desk.html
African project coordination: Waterfall City, Midrand, Gauteng, South Africa

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

© 2026 DOLPHIN FIBER SYSTEMS - All rights reserved