

Firewall Layer 2 Access Switch



AI Overview

A Layer 2 access switch forwards frames based on MAC addresses, while the firewall handles Layer 3 routing, security policies, and Internet access, making the firewall the gateway for users.

Layer 2 Switch Overview A Layer 2 (L2) switch operates at the data link layer, forwarding traffic based on MAC addresses within a LAN. It supports VLANs for logical segmentation, trunk ports for carrying multiple VLANs, and basic QoS and security features such as port security and storm control. L2 switches are ideal for access-layer deployment where routing is handled by a firewall or Layer 3 switch at the network edge.

Firewall Role in L2 Deployment In a Layer 2 deployment, the firewall provides Layer 3 services, including routing between VLANs, DHCP, NAT/PAT, and security policies. The firewall can operate in Layer 2 mode or transparent mode, forwarding frames between ports while inspecting traffic and enforcing security rules. It often serves as the default gateway for all VLANs connected to the access switch.

Typical Configuration Steps

- VLAN Assignment on the Switch:** Configure access ports for end devices and assign them to VLANs. For example, port link-type access and port default vlan 2 for user ports.
- Trunk Port to Firewall:** Configure the uplink port to the firewall as a trunk to carry multiple VLANs, e.g., port trunk allow-pass vlan 2 3.
- Firewall VLAN Interfaces:** Configure sub-interfaces or VLANIF interfaces on the firewall to terminate VLAN tags and perform Layer 3 routing between network segments.
- DHCP and NAT:** The firewall can act as a DHCP server and implement PAT/NAT to allow internal users to access the Internet.
- Security Policies:** Define interzone policies on the firewall to control traffic between VLANs and enforce security rules.

Best Practices Use access ports for end devices and trunk ports for uplinks to firewalls or other switches. Ensure VLAN consistency between the switch and firewall to avoid connectivity issues. Deploy inline firewalls in Layer 2 or virtual wire mode for environments using security group tags (SGTs) to inspect traffic with...

Article Content

Configure a Layer 2 Interface

Configure a Layer 2 interface on the firewall so it can act as a switch in your layer 2 network (not at the edge of the network). The Layer 2 hosts are probably geographically close to each other and belong

Example for Configuring a Layer 2 Switch to Work with a Firewall for ...

In Figure 2-41, a company has multiple departments that belong to different network segments, and each department needs to access the Internet. It is required that users access the

Top five: Looking back at OneDrive in 2021 | Microsoft

We wanted to take a quick look back and share our top five most exciting highlights from the past year.& nbsp;& nbsp; & nbsp; Known Folder Move

WORLD WIDE WEB JOURNAL Home

By clicking download, will open to start the export process. The process may take but once it finishes a file will be downloadable from your browser. You may continue to browse the DL while the export

Sophos XGS Series Firewall Comparison

See XGS 1U, 2U, and desktop hardware firewall comparisons. Find everything you need to connect and secure your organization.

Microsoft Options to Migrate SQL Server Databases | Microsoft

Security Considerations Security planning is a critical part of any on-premises to cloud migration. In addition to securing network paths (VPN/ExpressRoute, firewall rules, Private Link

ONU vs Router vs Switch: Key Differences in Fiber Network Devices

Layer 2 Switch: Manages wired devices like printers, PCs, and IP phones Reason: Small businesses prioritize secure internet access and controlled LAN environments.

Layer 2 vs Layer 3 Switch: Key Differences and Use Cases

Layer 2 vs Layer 3 switch explained. Learn MAC vs IP forwarding, inter-VLAN routing, performance differences, and when to choose each switch type.

Cisco Meraki Local Status Page: Overview

Accessing the local status page Most Cisco Meraki devices have a local status page that you can access to make local configuration changes, monitor device status and channel utilization,

Palo Alto Firewall Configuration Options. Tap Mode, Virtual Wire,

In this mode the firewall interfaces are capable of supporting Access or Trunk Links (802.1Q trunking) and do not participate in the Spanning Tree topology. Any BPDUs received on the

Cisco Secure Firewall Management Center Device

For each physical interface, you can set its operation as a firewall interface or as a switch port. See the following information about physical

Layer 2 Interfaces

In a Layer 2 deployment, the firewall provides switching between two or more networks. Devices are connected to a Layer 2 segment; the firewall forwards the frames to the proper port, which is

Example for Configuring a Layer 2 Switch to Work with a Firewall for ...

It is required that users access the Internet through the Layer 2 switch and firewall and that the firewall function as the gateway of users. The configuration roadmap is as follows: Configure interface-based

FIPS 140-2/3 requirements for network switches : r/CMMC

Switches is something I've also been curious about when it comes FIPS 140-2. If the documents are encrypted prior to being sent over the network, then why does the switch need to be 140-2? It makes

Sophos Firewall: Consolidate Your Security

Sophos Next-Gen Firewall. Integration with Sophos MDR and Sophos XDR, Comprehensive SD-WAN Capabilities, Support for SSE/SASE Portfolio, Cloud

Security and VPN Configuration Guide, Cisco IOS XE 17.x

A Layer 2 transparent firewall operates on bridged packets and is enabled on a pair of locally-switched Ethernet ports. Embedded IP packets forwarded through these ports are inspected

how to config Firewall routing with Layer 2 Switch

It may be easier to use the firewall to terminate both vlans by creating a sub-interface for each one (1.1.1.0 and 2.2.2.0) and have a layer-3 link between the firewall and the router.

Example for Configuring a Layer 2 Switch to Work with a Router for ...

Example for Configuring a Layer 2 Switch to Work with a Router for Internet Access
Layer 2 Switch Layer 2 switches perform only Layer 2 forwarding instead of Layer 3 forwarding. That is, Layer 2

OSI Model Explained — All 7 Layers with Real-World Examples

Configuration difference: a Layer 2 switch uses switchport mode access or switchport mode trunk on interfaces; a Layer 3 switch additionally uses no switchport to convert an interface into a routed port

Network Devices

Layer 2 Devices: Data Link Layer These devices work with MAC Addresses (Physical Addresses). They are smarter than hubs. 4. Switch A switch is a high-speed networking device that

DrayTek Vigor ADSL Routers, Firewalls and Networking

DrayTek networking products including routers, switches, access points, firewalls, VPN, central management, and 4G/5G connectivity solutions.

headTitleNoCommunity

First published on TECHNET on May 19, 2014 Storage Classification was introduced in System Center 2012 Virtual Machine Manager (VMM 2012) to provide the...

how to config Firewall routing with Layer 2 Switch

i need your advice and help to configure routing in a proper way, the scenario is, i have one Layer 2 switch 2960G 24TCL connected to Firewall ASA 5520 and firewall connected to Router

Example for Configuring a Layer 2 Switch to Work with a Firewall for ...

Layer 2 switches perform only Layer 2 forwarding instead of Layer 3 forwarding. That is, Layer 2 switches support only Layer 2 features instead of Layer 3 features such as routing. Layer 2

Access, Distribution, and Core Layers Explained

Switches in this layer are called access switches. End devices connect to the LAN through the access switches. In other words, an access

L2 vs L3 Switch: How to Choose for Your Access Layer

This article breaks down the differences between L2 and L3 switches in the access layer, analyzes key decision factors like network scale and complexity, and finally provides a practical

Types of Network Firewall

Types of Firewalls Based on Traffic Filtering Method Network Security is the process of protecting networks, systems, and data from unauthorized access, attacks, and damage.

Contact Us

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

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

Email: info@estlascleaning.co.za

Phone: +27 63 214 8579

Address: 22 Oxford Road, Parktown, Johannesburg, 2193, South Africa

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

