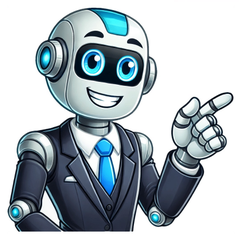
Click to prove you're human



# Guide مستخدم cisco asa 5525 firepower configuration

At-a-GlanceEvolution Beyond Traditional “Defense in Depth” SecurityTraditional “defense in depth” architectures typically force organizations to buy multiple security solutions — such as firewalls, VPN gateways, web filters, and other appliances — from different vendors. This approach increases complexity, as the products don’t always work well together. The lack of unified protection creates multiple blind spots. Attackers exploit these gaps, leaving organizations vulnerable and too often unaware of threats and attacks. Enterprises usually need to hire several dedicated teams to install and manage these disconnected security solutions. These security teams try to compensate for gaps in visibility and threat protection with manual processes that are inefficient, unreliable, and costly. This environment prevents rapid responses to the fast-changing threat landscape.With Cisco ASA with FirePOWER Services, you consolidate multiple security layers in a single platform, eliminating the cost of buying and managing multiple solutions. This integrated approach combines best-in-class security technology with multilayer protection integrated in a single device that’s less costly than piecemeal security solutions. You also get much greater visibility into what’s going on in your network, far beyond what’s available with traditional solutions. With full contextual awareness you will see all the resources you are charged with protecting. Blinds spots that are avenues for exploit are eliminated. Full visibility lets you better detect and prioritize threats based on their risk. Their possible impact is assessed and prioritized by an automated system. Meanwhile, the number of events associated with monitoring and response is reduced. The time between detection and cure quickly shrinks in a streamlined operation. Unprecedented Network VisibilityCisco ASA with FirePOWER Services is centrally managed through the Cisco Firepower Management Center which provides security teams with comprehensive visibility into and control over activity within the network. This capability includes users, devices, communications between virtual machines, vulnerabilities, threats, client-side applications, files, and websites. Holistic, actionable indications of compromise (IoCs) correlate detailed network and endpoint event information and provide further visibility into malware infections.Cisco ASA withFirePOWER Services© 2016 Cisco and/or its affiliates. All rights reserved.Features and BenefitsCisco ASA with FirePOWER Services provides:• Precise application visibility and control (AVC). More than 3000 application-layer and risk-based controls can invoke tailored IPS threat-detection policies to improve security effectiveness.• Industry-leading Cisco ASA with FirePOWER NGIPS. Highly effective threat prevention and a full contextual awareness of users, infrastructure, applications, and content help you detect multivector threats and automate the defense response.• Reputation - and category-based URL filtering. This filtering provides comprehensive alerting and control over suspect web traffic. It enforces policies on hundreds of millions of URLs in more than 80 categories.• Advanced malware protection.Effective breach detection with low TCO offers protection value. Discover, understand, and stop malware and emerging threats missed by other security layers. Some links below may open a new browser window to display the document you selected. About the ASA REST API 13/Jul/2021 Firepower Management Center Configuration Guide, Version 6.6 25/May/2022 Firepower Management Center Configuration Guide, Version 6.4 18/Feb/2022 Firepower Management Center Configuration Guide, Version 6.2.3 18/Feb/2022 Firepower Management Center Configuration Guide, Version 6.2.2 25/May/2019 Firepower Management Center Configuration Guide, Version 6.2.1 25/May/2019 Firepower Management Center Configuration Guide, Version 6.2 25/Apr/2019 Firepower Management Center Configuration Guide, Version 6.1 08/Oct/2019 Firepower Management Center Configuration Guide, Version 6.0.1 14/Feb/2024 Firepower Management Center Configuration Guide, Version 6.0 FireSIGHT System User Guide Version 5.4.1 02/Feb/2017 Cisco Firepower Threat Defense Hardening Guide, Version 6.4 09/May/2019 Cisco AnyConnect Deployment Guide for Cisco Jabber See the section for your firewall mode and ASA model to determine how to connect the ASA FirePOWER module management interface to your network. The ASA FirePOWER module includes separate management interfaces from the ASA. All management traffic to and from the ASA FirePOWER module must enter and exit the Management 1/0 or 1/1 interface. The ASA FirePOWER module also needs Internet access. Because the Management 1/x interface is not an ASA data interface, traffic cannot pass through the ASA over the backplane; therefore you need to physically cable the management interface to an ASA interface. See the following typical cabling setup to allow ASA FirePOWER access to the Internet through the ASA management interface (or you could use a data interface). Other options are possible, depending on how you want to connect your network; for example, you can make the Management 1/0 interface outside facing; or you can route between it and a different ASA interface if you have an inside router. Note: The ASA 5506-X does not support the FirePOWER module in 9.10 and later. The ASA 5506-X series runs the ASA FirePOWER module as a software module, and the ASA FirePOWER module shares the Management 1/1 interface with the ASA. All management traffic to and from the ASA FirePOWER module must enter and exit the Management interface. The ASA FirePOWER module also needs Internet access. Management traffic cannot pass through the ASA over the backplane; therefore you need to physically cable the management interface to an ASA interface to reach the Internet. If you do not configure a name and IP address in the ASA configuration for Management, then the interface belongs exclusively to the module. In this case, the Management interface is not a regular ASA interface, and you can: 1. Configure the ASA FirePOWER IP address to be on the same network as a regular ASA data interface. 2. Specify the data interface as the ASA FirePOWER gateway. 3. Directly connect the Management interface to the data interface. The following figure shows the recommended network deployment for the ASA 5506-X with the ASA FirePOWER module. This deployment includes an inside bridge group that includes all but the outside and wifi interfaces so you can use these interfaces as an alternative to an external switch. For the ASA 5506-X on 9.7 and later, the default configuration enables the above network deployment; the only change you need to make is to set the module IP address to be on the same network as the ASA inside interface and to configure the module gateway IP address. Note: The ASA 5506-X and 5512-X do not support the FirePOWER module in 9.10 and later. These models run the ASA FirePOWER module as a software module, and the ASA FirePOWER module shares the Management 0/0 or Management 1/1 interface (depending on your model) with the ASA. All management traffic to and from the ASA FirePOWER module must enter and exit the Management interface. The ASA FirePOWER module also needs Internet access. Management traffic cannot pass through the ASA over the backplane; therefore you need to physically cable the management interface to an ASA interface to reach the Internet. If you do not configure a name and IP address in the ASA configuration for Management, then the interface belongs exclusively to the module. In this case, the Management interface is not a regular ASA interface, and you can: 1. Configure the ASA FirePOWER IP address to be on the same network as a regular ASA data interface. 2. Specify the data interface as the ASA FirePOWER gateway. 3. Directly connect the Management interface to the data interface (using a Layer2 switch). See the following typical cabling setup to allow ASA FirePOWER access to the Internet through the ASA inside interface: For the ASA 5506-X on 9.6 and earlier, the ASA 5508-X, and the ASA 5516-X, the default configuration enables the above network deployment; the only change you need to make is to set the module IP address to be on the same network as the ASA inside interface and to configure the module gateway IP address. For other models, you must remove the ASA-configured name and IP address for Management 0/0 or 1/1, and then configure the other interfaces as indicated above. Note: For ASA 9.7 and later, you can avoid using an external switch if you have extra interfaces that you can assign to an inside bridge group. Be sure to set all bridge group interfaces to the same security level, allow same security communication, and configure NAT for each bridge group member. See the ASA interfaces configuration guide chapter for more information. Note: If you want to deploy a separate router on the inside network, then you can route between management and inside. In this case, you can manage both the ASA and ASA FirePOWER module on the Management interface with the appropriate configuration changes, including configuring the ASA name and IP address for the Management interface (on the same network as the ASA FirePOWER module address). The ASA FirePOWER module includes separate management interfaces from the ASA. All management traffic to and from the ASA FirePOWER module must enter and exit the Management 1/0 or 1/1 interface. The ASA FirePOWER module also needs Internet access. Because this interface is not an ASA data interface, traffic cannot pass through the ASA over the backplane; therefore you need to physically cable the management interface to an ASA interface. See the following typical cabling setup to allow ASA FirePOWER access to the Internet through the ASA inside interface when using an inside router. If you do not use an inside router, you can manage the ASA over the inside interface (using the BVI IP address) and not use the Management 0/0 interface: Note: You can avoid using an external switch if you have extra interfaces that you can assign to the inside bridge group. Be sure to set all bridge group interfaces to the same security level, allow same security communication, and configure NAT for each bridge group member. See the ASA interfaces configuration guide chapter for more information. Note: The ISA 3000 does not support the FirePOWER module in 9.17 and later. Note: The ASA 5506-X and 5512-X do not support the FirePOWER module in 9.10 and later. These models run the ASA FirePOWER module as a software module, and the ASA FirePOWER module shares the Management 0/0 or Management 1/1 interface (depending on your model) with the ASA. All management traffic to and from the ASA FirePOWER module must enter and exit the Management interface. The ASA FirePOWER module also needs Internet access. The following figure shows the recommended network deployment for the ASA 5500-X or ISA 3000 with the ASA FirePOWER module when you have an inside router: If you do not use an inside router, you can manage the ASA over the inside interface (using the BVI IP address) and not use the Management interface for ASA management: Note: You can avoid using an external switch if you have extra interfaces that you can assign to the inside bridge group. Be sure to set all bridge group interfaces to the same security level, allow same security communication, and configure NAT for each bridge group member. See the ASA interfaces configuration guide chapter for more information. Share — copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt — remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits. You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation . No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. The rapid change in the business landscape--especially in 2020 and 2021--transformed applications and provisioning environments. Your employees and users can now use recent technologies like microservices, containers, and APIs to align themselves with the pace of business changes. Modern data centers becoming more complex is both an indicator of growth and a challenge for a data center’s security. The increase in data volume, number of applications, and interaction with the data center can translate to an increase in data-theft opportunities. The firewall is the critical component to secure the data center. In this blog, we will discuss the features and benefits of the Cisco ASA 5500 series firewall. Looking to configure your Cisco ASA firewall? Check out our configuration guide here. Not sure the ASA 5500 is best for your network? Check out our other comparison blogs: Cisco ASA Fully Integrated, Threat-Focused Firewalls As the network perimeter continues to evolve, organizations must re-think their approach to firewalling to stay ahead of an increasingly complex set of threats. The Cisco Secure Firewall portfolio is optimized for today’s threat landscape, delivering evolved network security backed by industry-leading threat intelligence, with consistent security policies, visibility, and management experience. The Secure Firewall portfolio allows you to protect your network, data, users, and devices from even the most sophisticated threats while delivering consistent security policies, visibility, and improved threat response. You can leverage the power of Cisco to turn your existing network infrastructure into an extension of your firewall solution, leading to robust security for your data center, branch offices, cloud environments, and everywhere in between. The depth, breadth, and integration of the Cisco Secure Firewall portfolio help you to rein in the chaos created by the huge number of disparate point solutions typical of today’s security architecture. Secure Firewall appliances set the foundation for consistent visibility, policy harmonization, and unified management. The result is a comprehensive system that prevents breaches and stops the stealthiest attacks, all while maintaining optimal network performance and uptime. Secure Firewall sets the bar as the industry’s leading fully integrated, threat-focused, next-generation firewall (NGFW). It prevents more breaches and can quickly detect and mitigate stealthy attacks using enhanced visibility and the most advanced security capabilities of any firewall available today. What’s more, Cisco was named a 2020 Forrester Wave Leader for Enterprise Firewalls. Cisco ASA 5500-X With Firepower Services Cisco ASA is an adaptive, threat-focused, next-generation firewall – in a single, 1RU form-factor device. These appliances deliver multiple security services, multigigabit performance, flexible interface options, and redundant power supplies. Need to quote a firewall? Click here Cisco ASA 5500 Series provides effective security. It surpasses legacy NGFW offerings with multi-layered protection to provide an integrated threat defense. The Cisco ASA 5500-X range of models for enterprises, branch offices, and industrial applications meet a variety of price-performance needs. Cisco ASA 5500 Series Features The Cisco ASA 5500 Series has the following main features worth noting: Robust firewalling, including support for BGP, high availability, VPN, NAT, and more. Firewall throughput protects users as their current and future data consumption demands increase. Additional security services allow quick and easy setup without additional hardware. Dedicated Secure Next-Generation Intrusion Protection System (NGIPS) hardware accelerates the response against security threats (ASA 5525-X and 5555-X). Multicore enterprise-class CPUs deliver robust and efficient performance. Cisco Firepower Service Features and Benefits The Cisco Firepower Service has the following features and benefits: Industry-leading Cisco ASA with Firepower: Cisco’s Firepower (NGIPS) integration provides intelligence based on the open-source IPS solution – Snort. It offers highly effective threat prevention and full contextual awareness of users, applications, and infrastructure. The Firepower recommendation option gives the best IPS rule suggestions based on the user traffic and application. Reputation- and category-based URL filtering: This filtering delivers complete alerting and control over suspicious web traffic. It implements policies on hundreds of millions of URLs in more than 80 categories. It takes updates from industry-leading threat intelligence TALOS Security. Distinct application visibility and control: More than 3000 application-layer and risk-based controls can gather tailored IPS threat-detection policies to enhance security effectiveness. Advanced malware protection: Advanced malware protection discovers, understands, and stops malware and emerging threats missed by other security layers. Cisco ASA 5500 Series Details Summary Cisco ASA software can install in Cisco ASA-55XX hardware and new Firepower hardware. The below table shows the Cisco ASA-55XX series hardware comparison. Model Firewall Throughput NGIPS Throughput NGFW Throughput Interfaces ASA-5506 750 Mbps 125 Mbps 125 Mbps 8 x RJ45 ASA-5508 1 Gbps 250 Mbps 250 Mbps 8 x RJ45 ASA-5516 1.8 Gbps 450 Mbps 450 Mbps 8 x RJ45 ASA-5525 2 Gbps 650 Mbps 650 Mbps 8 x RJ45, optional 6 x GE ASA-5545 3 Gbps 1 Gbps 1 Gbps 8 x RJ45, optional 6 x GE ASA-5555 4 Gbps 1.2 Gbps 1.2 Gbps 8 x RJ45, optional 6 x GE Are lead times slowing you down and preventing you from getting the hardware or services you require for your data center? Send us a request or connect with our Team in real-time using our chat feature. Know what you want? Explore our hardware options. Cisco Adaptive Security Virtual Appliance The Cisco Adaptive Security Virtual Appliance is the virtualized option of the Cisco ASA solution and offers security in traditional physical data centers and private and public clouds. It supports site-to-site VPN, remote-access VPN, and clientless VPN functionalities. This scalable VPN capability provides access for employees, partners, and suppliers—and protects your workloads against increasingly complex threats with world-class security controls. Cisco ASA Management Options Cisco ASA can be managed via multiple options. The Command Line Interface (CLI) is the most used method to configure the ASA firewall. But for configuring some new features and monitoring, you need to use other GUI-based management options. The below table describes ASA management options based on the features. Features Cisco Security Manager Adaptive Security Device Manager Cisco Defence Orchestrator Location and Type of Manager On-premise and multi-device On-box local device Cloud, multi-device, and multi-platform Firewall Deployment Modes Active/Standby, Active/Active, Cluster, and VPN Load Balancing Active/Standby, Active/Active, Cluster, and VPN Load Balancing Active/Standby Remote Access VPN Management GUI-based configuration for IPSEC, SSL, and Clientless VPN GUI-based configuration for IPSEC, SSL, and Clientless VPN CLI- and GUI-based configuration for Anyconnect Remote Access VPN (HostScan or DAP configurable through CLI only) Firewall Management Automation Rule optimization, shared configuration, and usage reports Hit counts and configuration wizards Object conflicts, rule optimization, configuration templates, and CLI macros Logging and Event Storage Event Viewer and report manager, Syslog, and Netflow to external logging servers, SAL cloud integration using SEC Event Viewer manager, Syslog, and Netflow to external logging servers SAL cloud integration using SEC Event Viewer and Enhanced VPN monitoring and reporting, and SAL Cloud integration with Cross Launch Solve Your Security Hardware Pains With PivIT's EXTEND Whether you are trying to protect a small or large data center of varying complexity, a breach in your network can cause a catastrophe. At PivIT, our certified engineers are ready to perform a site survey and provide you with the best firewall for your network, using a mixture of new and legacy units. Let our professionals take care of your network security needs with our EXTEND service. For details on configuring a Cisco ASA Firewall using the active/standby feature, view Part 1 and Part 2 of our series where we provide a full overview of the firewall and how to deploy it.