Fortigate configuration step by step pdf

Hello tod@s. In this post, we'll see how to execute the initial configuration and commissioning to begin working with the Fortigate firewall of the American company Fortinet, dedicated to the development and commercialization of software, devices and cybersecurity services such as firewalls, antivirus, intrusion prevention and security on user devices, among others. Topology used is simple and will be as follows, Fortigate port for Internet access (WAN1) and another port for internal network (LAN_RAGASYS): The first thing we do is connect to our Fortigate with a cable console and login, with the user administrator and password blank: Once you are registered, with the next command we see the status interfaces: As we see, port1 has allowed access to ICMP (Ping), HTTP, HTTPS, SSH and FGFM protocols, all of this, so that once we assign it an IP address we can manage Fortigate through this address, anyway, once we access the firewall through the web interface we can incorporate all these access to the ports that interest us, we can also do it through CLI, which is to the consumer. Now let's assign appropriate IP addresses for interfaces LAN_RAGASYS and WAN1, for this we do this: After assigning IP addresses we can already access Fortigate through a web portal, in my case, as a good practice, I always create a static type of recording on my DNS server, so we can access the device through its name: Once we've gained access to Fortigate we can see the address assigned to the two interfaces: As good practice the first thing we're going to do is disable all the ports that we won't use and as we need them, we'll let them, for that we edit every port and disable: We're doing the same operation for all other ports, and we're going to stay that way. : Now we're editing port1 and port8: Now let's customize the host name and system time, for which we access the System of zgt; Settings: The next step will be to set up DNS, in the DNS Network: Now let's assign a password to the user administrator, which is determined by default in Fortigate, since the factory does not assign a password: now we will create profiles to manage Fortigate, assigning permissions that interest us to each profile, in my case I will create a profile for system administrators Ragasys: As soon as the profiles are created, we can now create users and assign them to profiles that we are interested in: the next step will be to create a route for default Internet access, for this we will go to the Internet. our computers will not yet have an Internet connection, we need to adjust the policies that we will see in the following points: Now we will customize some policies so that computers of our local network have access to the Internet, although first we will see that the default implicit policy is set up denying all traffic from any source to any destination and with any service , We will add policies and allow traffic that we are interested in: To set up the policies, the first thing we will do is set up addresses, in which case I will cover all addresses belonging to the internal network LAN_RAGASYS: Now we will create a group and add these addresses LANRAGASYS, which will include the entire network: Once addresses and group are created, let's create service groups to apply them to our policies As we want to provide Internet access to all computers on our internal network, we will create a service group called Web Access, in which we will include DNS, HTTP and HTTPS services so that computers can view, most services are already identified in the firewall because they can be FTP, SMB, HTTP, HTTPS, POP3, SMTP, DNS, etc....: As soon as service groups will be established We will introduce policies that interest us, in which case we will introduce a policy so that all computers of our internal network can browse the Internet: With this we will already have access to the Internet from any computer in our internal network. Now let's create another group of services called ICMP Access, in which we'll include the ALL_ICMP service: Once the service team is set up, we'll include a policy, in which case we'll include a policy so that all computers on our internal network can ping any IP address on the Internet and check its status: As we can see from the Windows 10 computer from which I set up Fortigate we can already ping any Internet address. A: Greetings and I hope you find help ☺ Related Every FortiGate in the cluster should have the same HA configuration. Once you've connected the cluster, you can set it up the same way you set up a standalone FortiGate. The next example sets HA mode for active-passive and ha password for HA_pass. Make sure FortiGate interfaces are configured with static IP addresses. If any interface receives its address using DHCP or PPPoE, you should temporarily switch it to a static address and turn on DHCP or PPPoE after you create the cluster. Make sure both FortiGates work under the same version of the FortiOS firmware. Register and apply licenses to both FortiGates before adding them to the cluster. This is fortiCare Support, IPS, AntiVirus, Web Filtering, Mobile Malware, FortiClient, FortiCloud and Additional Virtual Domains (VDOM). All FortiGates in the cluster must have the same licensing level for FortiGuard, FortiCloud, FortiClient and VDOM. FortiToken licenses can be added at any time because they are synchronized with all members of the cluster. You can also install any third-party certificates on the main FortiGate before forming a cluster. Once a cluster is formed, third-party certificates are synchronized with FortiGate backup. Set up FortiGate for HA - GUI Power on FortiGate to set up. Enter the graphical interface. Find the System Information Dashboard widget. Click on the system information dashboard widget and select customization settings in the system's settings. Enter the new host name for this FortiGate.Changing the host name makes it easier to identify individual cluster units when the cluster is running. Go to System and change the following settings: Active-Passive Group Name mode Example_cluster Password HA_passThe password should be the same for all FortiGates in the cluster. You can take the default configuration for the rest of the HA variants and change them later as soon as the cluster works. Choose OK. FortiGate is in talks to create a HA cluster. When you select OK, you may temporarily lose contact with FortiGate as the HA and FGCP cluster is negotiated changes the MAC address of the FortiGate interfaces. To be able to reconnect sooner, you can update your computer's ARP table by deleting the ARP table entry for FortiGate (or simply deleting all ARP table entries). You may be able to remove your computer's ARP table from a command tip using a command similar to arp-d. Turn off FortiGate. Repeat this procedure for all FortiGates in the cluster. Once all units have been set up, continue to connect the FortiGate HA cluster below. Set up FortiGate for HA - CLI Power on FortiGate to set up. Enter CLI. Enter the next command to change the name of the FortiGate host. Config system of global host Example1_host at the end of the host name change facilitates identification of individual cluster units when the cluster is working. Enter the following command to enable HA: the configuration of the system ha set mode is an active-passive set of group names Example_cluster a set of passwords HA_pass end you can take the default configuration for the rest of the HA variants and change them later as soon as the cluster works. FortiGate is in talks to create a HA cluster. You may temporarily lose contact with FortiGate as the HA cluster is negotiated and because FGCP changes the mac address of FortiGate interfaces. To be able to reconnect earlier, you can update the table your control computer by removing the ARP ARP table for FortiGate (or simply deleting all arp table entries). You may be able to remove your control computer's arp table from the command hint using a command similar to arp-d. Turn off FortiGate. Repeat this procedure for all FortiGates in the cluster. Once all the blocks have been set up, continue to connect the FortiGate HA cluster. Connect the FortiGate HA cluster Use the following procedure to connect the cluster. Connect cluster blocks to each other and network. You have to connect all the relevant interfaces in the cluster to the same switch, and then connect those interfaces to their networks using the same switch. While you can use hubs, Fortinet recommends using switches for all cluster connections for best performance. Connecting the HA cluster to the network temporarily interrupts communication on the network due to new physical connections to route traffic through the cluster. In addition, the launch of the cluster interrupts network traffic until individual cluster units function and the cluster completes negotiations. Cluster conversations are automatic and usually take only a few seconds. During the launch of the system and negotiations, all network traffic will be edicto out. This section describes how to connect the cluster shown below, which consists of two FortiGate-100D devices that will be connected between the Internet and the head office's internal network. FortiGate's wan1 interfaces connect the cluster to the Internet, and internal interfaces connect to the cluster to the internal network. The ha1 and ha2 interfaces are used for redundant ha heartbeat links. Example Cluster Connections To Connect the FortiGate HA Cluster Connect the WAN1 interfaces of each cluster block to the Internet-connected switch. Connect the port1 interfaces of each cluster block to a switch connected to an internal network. Combine the HA1 cluster blocks interfaces together. You can use an Ethernet crossover cable or a regular Ethernet cable. (You can also connect interfaces with Ethernet cables and switches.) Put the HA2 cluster blocks interfaces together. You can use an Ethernet crossover cable or a regular Ethernet cable. (You can also connect interfaces with Ethernet cables and switches.) Power on both FortiGates. As cluster blocks run, they negotiate the selection of the main unit and the subordinate unit. These conversations take place without user intervention and usually just take a few seconds. At least one heartbeat interface must be connected together to work the cluster. Do not use the switch port to move the HA heartbeat. This configuration is not supported. You can use one switch to connect all four heartbeat interfaces. However, it is recommended, because if the switch fails, both heartbeat interfaces will be disabled. Now you can set up the cluster as if it were single FortiGate. Checking the status of the cluster from the HA Status widget hack of the HA dashboard shows the mode and names of the cluster groups, the state of the cluster blocks and their host names, the time of the cluster's downtime, and the last time the cluster state changed. A state change may indicate that a cluster is formed first, or one of the cluster blocks changes its role in the cluster. The HA Status Dashboard widget also shows the synchronization of cluster units. The mouse above each FortiGate in the cluster to make sure they both have the same checksum. Checksum. fortigate configuration step by step pdf. fortigate 60e configuration step by step. fortigate 30e configuration step by step. fortigate ssl vpn configuration step by step. fortinet firewall configuration step by step. fortigate 100e configuration step by step. fortigate 60e configuration step by step pdf. fortigate vm configuration step by step