SECURITY HARDENING GUIDELINES

VMware SD-WAN by VeloCloud

Introduction

Network infrastructure devices play a critical role in providing access to business-critical resources and information systems. Given their importance, they need to be protected and configured accordingly. VMware SD-WAN Edges by VeloCloud are no exception. This document will provide technical guidance to network administrators to improve the security of the VMware SD-WAN Edges and configure instructions to achieve a minimal attack surface.

Compromised network devices can have devastating consequences to the enterprise since they can be used to gain access to data, reconfigured to route traffic to other destinations, used to launch attacks to other networks, and to gain access to other internal resources. Therefore, hardening of the VMware SD-WAN Edges is essential for enhancing the overall security posture of the enterprise.

Network device hardening separates a network device in three functional elements called “planes.” These are the following:

- The Management Plane is responsible for the management of network devices and is used to access, configure, manage and monitor a network device.
- The Control Plane consists of the protocols and processes that communicate between network devices in order to transport data from its source to the intended destination. This includes routing protocols such as the BGP and OSPF.
- The Data Plane is responsible for the actual transport of data from source to destination. This is where packets are flowing within the network device.

In the VMware SD-WAN solution, the planes are being hosted and consumed by the individual components:

- The VMware SD-WAN Orchestrator serves both management and control plane functions to the SD-WAN domain.
- The VMware SD-WAN Gateways primarily function as a distributed data plane but in addition serve as a proxy for the control plane hosted by the VMware SD-WAN Orchestrator.
- The VMware SD-WAN Edges consume all planes from the VMware SD-EAN Orchestrator and Gateways (or Controllers)

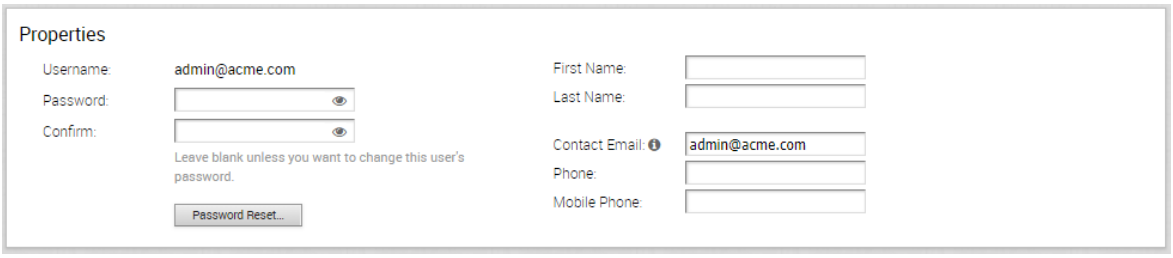
The document will outline how to harden each of the planes.

Orchestrator Management Plane

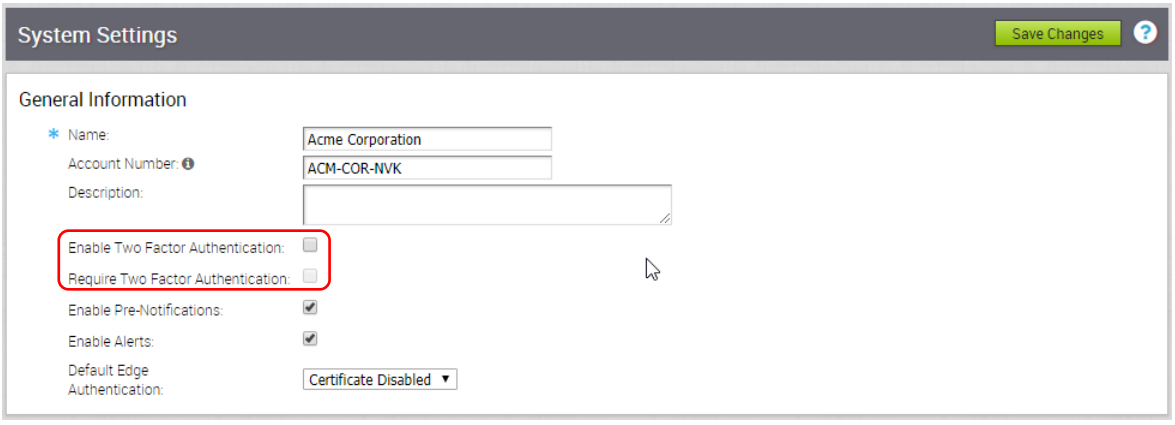
While the VMware SD-WAN Orchestrator is not in the data path, it remains an important vector that requires securing and as such VMware, recommends making the following changes in the VMware SD-WAN Orchestrator to bolster the overall security stance of the solution.

- Restrict the personnel that can access the VMware SD-WAN Orchestrator portal to an absolute minimal set.
- Use the principle of least privilege where users and administrators of the portal are only afforded the privilege level that is required to complete assigned work items.
- Restrict the number of SuperUser to 3. These operators will be able to create additional Standard Admin accounts
- If it is unclear what privilege level should be assigned to a new user, assign them the minimal 'Enterprise Read Only' role.
- Establish a cadence to review all active accounts and the associated privilege level and adjust these bases on changes in the organization.
- Disable accounts that are no longer in use. This can be done by editing an individual user account:

- Force a password reset of any account that is suspected to be compromised. This can be initiated at the individual user account:

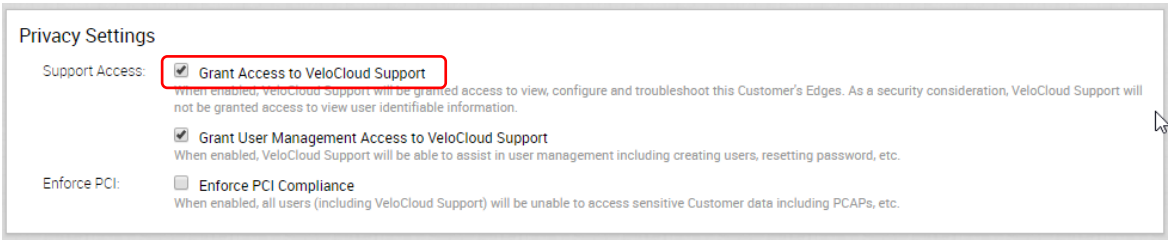


- Do not create accounts that are shared between two or more users. Establish individual accounts per user to ensure traceability of actions taken in the VMware SD-WAN Orchestrator portal.
- Establish and enforce a password policy that regulates password length and complexity. It is recommended to have at least a 12-character password with a mandatory lowercase, uppercase, number and special character as part of the password. Longer passwords are generally more secure.
- For stronger authentication of portal users, enable two factor authentication via the System Settings page:

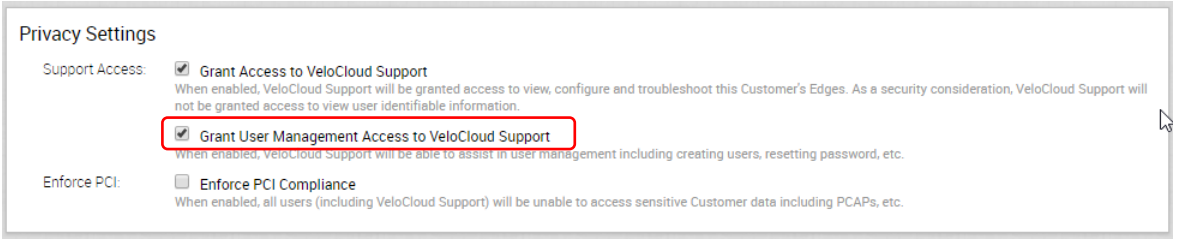


In order for Two Factor Authentication to operate, each user must have a mobile phone number registered in its account. This will be used to send a token to the phone that can be used when challenged during login.

- Disable support access delegations to the operator, which will obfuscate user identifiable information (such as source IP address, hostname and MAC address) when support operator assists a customer during diagnostic activities. This can be modified in the System Settings:



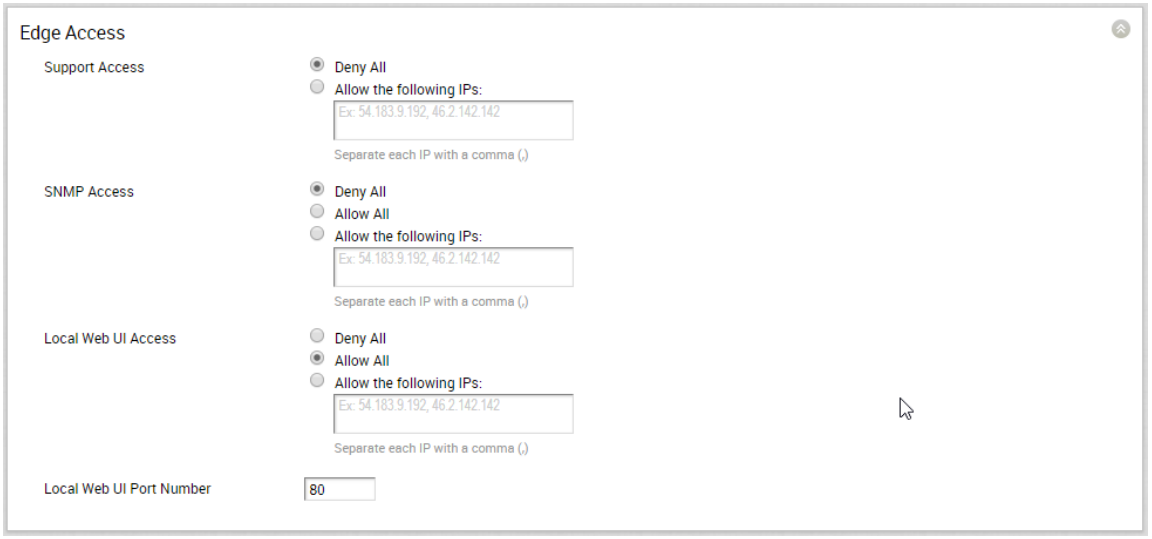
- Disable User Management delegations to the operator, which allows operators to assist with creation of new users in the enterprise account as well as with password resets. This can also be modified in the System Settings:



Edge Enablement Plane

- Establish a cadence to review the port forwarding and NAT rules to ensure they are still relevant. Remove any unused entries to close unnecessary open ports exposed to public vectors.

- Review the VMware SD-WAN Edge Access policies in the profiles attached to any VMware SD-WAN Edges. This is in the Firewall tab of the Profile Configuration dialog:

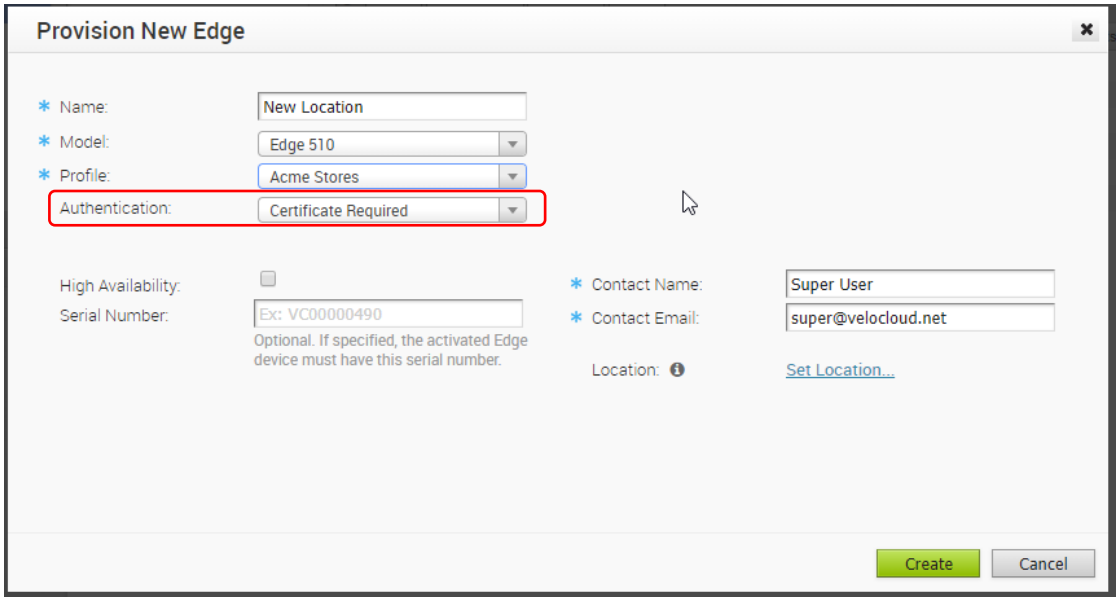


- Disable (Deny All) Support Access to disable the SSH daemon in the VMware SD-WAN Edge that can provide access to the local diagnostic CLI.
    - If access needs to be afforded to a user, ensure that it is temporary and that it is restricted to a single host.
- Disable (Deny All) Local Web UI Access, preventing access of the minimal web interface that gives insight into port configurations, system status and diagnostics tools. Note that this interface is always available before the device is activated but its behavior can be influences after activation has been completed.
    - If access needs to be afforded to a user, ensure that it is temporary and that it is restricted to a single host.
    - Set the Local Web UI Port Number to a non-standard port (i.e. different from 80, 443, 8080)
- Disable (Deny All) SNMP Access if it is not used. If it is used, restrict access to the SNMP collector IP addresses only. In addition, set the following items in the profile with regards to the SNMP Settings:

- Enable SNMP v3 only
- Set long, non-predictable community strings
- Set long, non-predictable v3 Names as well as passwords
- Enable the Privacy option and use AES encryption to secure the data exchange

Control Plane

- Remove all inactive routing configurations. These can be potentially used to form a rogue adjacency when left in place
- When using BGP, community tag all received routes to promote transparency of route origination.
- For both BGP and OSPF set up a filter to drop all unknown routes
- For both BGP and OSPF, filter out a received default route
- Enable certificate for VMware SD-WAN Edge device authentication during the VMware SD-WAN Edge provisioning. This will allow the Orchestrator to verify the identity of the VMware SD-WAN Edge and allows a network administrator to revoke a compromised Edge from the SD-WAN network. Set the Authentication mode to 'Certificate Required' during Provision New Edge dialog:



Data Plane

- Disable any unused features

- Enable Segmentation in the profile even when it is perceived not needed. When enabled, it is easy to add additional segments and extend these to branches. Converting from a network-based profile to a segment-based profile requires more planning. At the same time, it provides an easy mechanism to isolate interfaces of suspected compromised segments while investigations progress.

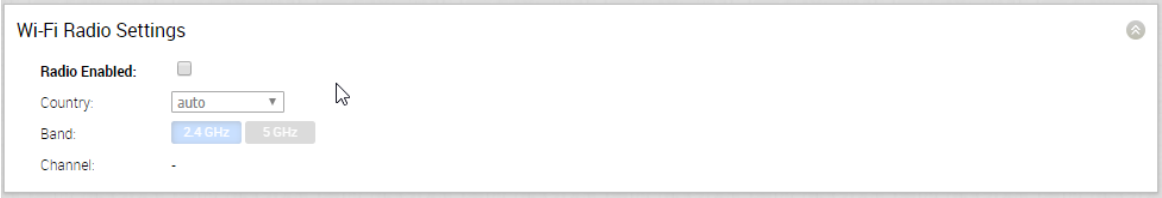
- Associate guest traffic on a dedicated segment, isolating it from other corporate traffic. For this segment:

    - Disable the Cloud VPN capabilities

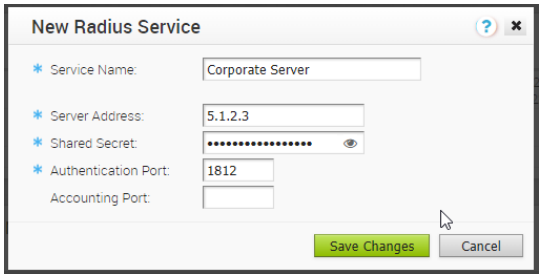
    - Optionally set up overlapping address space to further promote isolation as well as address space conservation.

- Disable all unused physical ports in the profile. Re-enable ports in the VMware SD-WAN Edge configuration so that there is a default closed position in place that prevents rogue devices to be connected to open ports and gain access to network resources.

- If wireless functions are not required, disable the wireless radio in the profile device settings

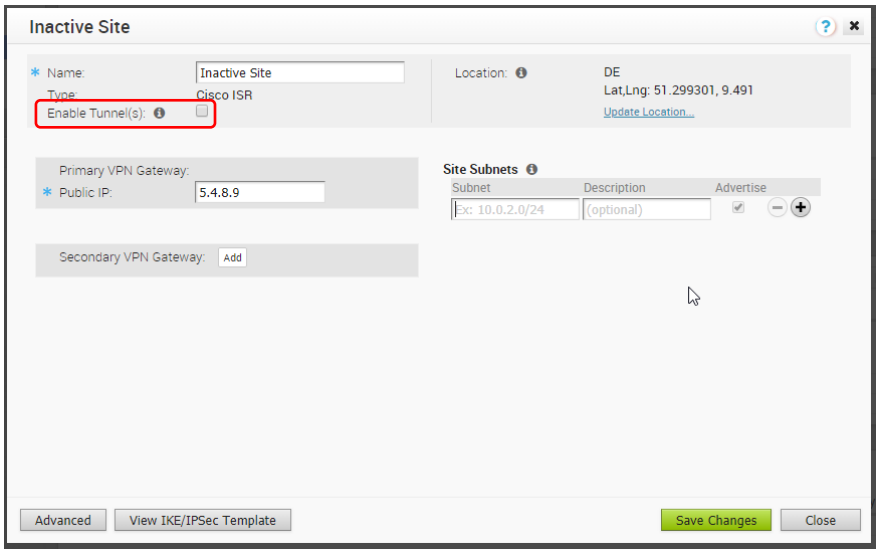


- If wireless services are offered from the VMware SD-WAN Edge directly, ensure that WPA-ENT authentication is set and that RADIUS services are configured to provide AAA services for accessing the wireless network. RADIUS services should be defined in the Configure | Network Services tab. Look for the Authentication Services dialog to provide the details on how to contact the server:



  Note that it is recommended to have the RADIUS server be reachable over the corporate VPN network. VMware SD-WAN Edges will attempt to reach this server through a normal route lookup. It should be pointed out that RADIUS is not a secure protocol and should never be operated over open Internet links without additional protections in place.

- Disable all inactive non-VMware SD-WAN site tunnels and remove them from any profiles where they are used. At a minimum, the tunnel should be disabled:



- When configuring a non- VMware SD-WAN site tunnel, continue to use the generated Pre-Shared Key (PSK) or replace it with a long PSK of at least 32 characters, mixing lowercase and uppercase alphanumerical values.

- If an external third party firewall is used at the WAN side of the VMware SD-WAN Edge and the VMware SD-WAN Edge is configured as a hub site, ensure that the firewall allows inbound port UDP/2426. This ensures expedient establishment of Branch to hub overlay tunnels. The firewall should allow all outbound flows without any restriction.

Edge Physical Security

- Install the VMware SD-WAN Edge device in an inherently secure location with proper cooling.

- Install the system in a locked room equipped with access controls

- Restrict personal that can access the room and can physically manipulate the VMware SD-WAN Edge device

- Install Kensington security cable and attach the cable to a permanent fixture