3 Standout New Features in Cisco's Firepower 6.3 Release

MULTI-INSTANCE FOR FIREPOWER

One of the headline features that the 6.3 release brings to Firepower, specifically to Firepower 4100/9300 w/ Firepower Threat Defense (FTD), is multi-instance. Previously, admins could deploy a lone instance of FTD on a given security utility. As a result of this update, however, admins can now spin up multiple virtual appliances per security device. Each such appliance has its own FTD container and admins can customize it independently.

This revamped security architecture can support organizations in their pursuit of two constant data center objectives. By using this approach, admins can deliver a data center that is both highly available and also flexible enough to scale alongside organizational demands.

TWO-FACTOR AUTHENTICATION

Another new feature ushered in by version 6.3 is two-factor authentication for FTD. Remote users connecting via a VPN can now take advantage of the extra security of two factor authentication. The initial factor in the authentication process can be any RADIUS or LDAP/AD server. Secondary validation can occur through either an RSA token or from a DUO passcode sent out to a user's internet-connected device.

Leveraging two-factor authentication can ensure users have the flexibility they want to work remotely without opening the organization up to any unnecessary risks.

LOCAL AUTHENTICATION FOR VPN USERS
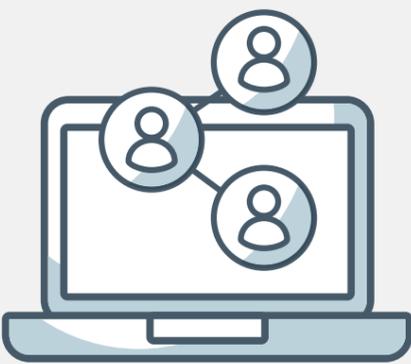
On the subject of authentication, version 6.3 brings additional verification capabilities to the table. So, admins are able to create users by way of Firepower Device Manager. They can use this locally-hosted account database to authenticate access requests coming in through a remote VPN connection. In this type of arrangement, that local cache of accounts can serve as either the primary or fallback verification method.

Of course, proximity is no longer a prerequisite for an attack. Given the ever-increasing threat posed by far-off malicious actors, it's critical for organizations to take whatever steps necessary to tightly manage remote access to sensitive data.

NEXT STEPS: IS CISCO'S FIREPOWER 6.3 RELEASE THE RIGHT FIT FOR YOU?

These are just a few of the changes the 6.3 version of Firepower software can bring to organizational security postures. Want to learn more about what else it has in store? Thinking about upgrading your existing Firepower deployment or bringing the solutions to your company for the first time? Arraya Solutions' Network and Security teams can help. Our experts are available to help you assess your current security environment and address any gaps with solutions and strategies designed to fit your individual needs. Visit arraya.rocks/CyberSecurity to learn more.

Arraya