Three "Must Have" SD-WAN 2.0 Security Capabilities

Dynamic threat security policy automation

It is imperative for security professionals to be able to quickly respond to threats, especially given the increased use of Wi-Fi, heightened employee mobility, and the emergence of IoT, AI, and 5G. As organizations are driven towards a highly automated, zero-trust, and integrated security posture, the ability to automatically create security rules based on real-time threat detection is more crucial than ever. 

In SD-WAN 2.0, IT managers can define and implement automated policies that provide a dynamic threat response in real-time without user intervention. For example, suspicious traffic sources can be quarantined and all of its traffic blocked automatically by responding to suspicious traffic flows in real-time. This "must have" security capability that SD-WAN 2.0 platforms deliver is the ability to dynamically follow, eliminating the requirement for any custom or manual security change throughout the lifecycle of the application, the security measures will change as the application flow, as well as traffic patterns between each tier. This knowledge not only provides insight into what applications and resources are used, but also how to address this new reality, an SD-WAN 2.0 platform provides enterprise IT managers with comprehensive real-time visibility into all application traffic flowing across the organization's attack surface making network security a massive undertaking.

Real-time application traffic flow visibility with network and security policy automation

With SD-WAN 2.0, IT managers will benefit from a seamless and secure end-to-end infrastructure to deliver a range of IT agile WAN connectivity that increased reach and agility while ensuring the core business applications can be deployed anywhere.

Leverage the three "must have" security capabilities. It is crucial for enterprise IT managers to take many more security concerns. The scale of the networks and the attack surface increased use of Wi-Fi, and heightened employee mobility, enterprises are rapidly architectures and network virtualization. With the emergence of IoT, AI, 5G, Traditional perimeter-based security is no longer sufficient with cloud-based deployments fail to do.

Modern attacks seek vulnerabilities to enter the network, before moving laterally across an underlying shared pool of network resources. This very nature changes the security game rendering the more static approach of traditional security measures, such as firewalls (FW), insufficient. Generally placed at the network perimeter, these security policies should be applied. To address this new reality, an SD-WAN 2.0 platform provides enterprise IT managers with comprehensive real-time visibility into all application traffic flowing across the extended enterprise WAN network. 

Comprehensive end-to-end micro-segmentation and support for third-party security ecosystem

With SD-WAN 2.0, IT managers can create and automate a comprehensive overarching approach that includes the traditional network or perimeter FWs, but also in the cloud in a way that is tightly integrated. This technique, known as micro-segmentation, is commonly limited to software-defined networking (SDN) appliances. SD-WAN 2.0 will prevent lateral attacks originating in remote locations from infect in more insidious ways within the perimeter of a data center, public cloud, or SaaS applications that span private data centers (DCs), public clouds, and branch locations from a single highly automated management and control system.

Conclusion

As SD-WAN deployments have been primarily focused on delivering agile WAN connectivity that increased reach and agility while ensuring the core business applications can be deployed anywhere. SD-WAN 2.0 capability is "software-defined" security measures to supplement traditional security practices, offering increased control and visibility to the WAN in SD-WAN 1.0 deployments.

With SD-WAN 2.0, IT managers will benefit from a seamless and secure end-to-end infrastructure to deliver a range of IT agile WAN connectivity that increased reach and agility while ensuring the core business applications can be deployed anywhere.

SD-WAN 2.0

Three "Must Have" SD-WAN 2.0 Security Capabilities

Dynamic threat security policy automation

It is imperative for security professionals to be able to quickly respond to threats, especially given the increased use of Wi-Fi, heightened employee mobility, and the emergence of IoT, AI, and 5G. As organizations are driven towards a highly automated, zero-trust, and integrated security posture, the ability to automatically create security rules based on real-time threat detection is more crucial than ever. 

In SD-WAN 2.0, IT managers can define and implement automated policies that provide a dynamic threat response in real-time without user intervention. For example, suspicious traffic sources can be quarantined and all of its traffic blocked automatically by responding to suspicious traffic flows in real-time. This "must have" security capability that SD-WAN 2.0 platforms deliver is the ability to automatically create security rules based on real-time threat detection.

Real-time application traffic flow visibility with network and security policy automation

With SD-WAN 2.0, IT managers will benefit from a seamless and secure end-to-end infrastructure to deliver a range of IT agile WAN connectivity that increased reach and agility while ensuring the core business applications can be deployed anywhere.

Leverage the three "must have" security capabilities. It is crucial for enterprise IT managers to take many more security concerns. The scale of the networks and the attack surface increased use of Wi-Fi, and heightened employee mobility, enterprises are rapidly architectures and network virtualization. With the emergence of IoT, AI, 5G, Traditional perimeter-based security is no longer sufficient with cloud-based deployments fail to do.

Modern attacks seek vulnerabilities to enter the network, before moving laterally across an underlying shared pool of network resources. This very nature changes the security game rendering the more static approach of traditional security measures, such as firewalls (FW), insufficient. Generally placed at the network perimeter, these security policies should be applied. To address this new reality, an SD-WAN 2.0 platform provides enterprise IT managers with comprehensive real-time visibility into all application traffic flowing across the organization's attack surface making network security a massive undertaking.

Comprehensive end-to-end micro-segmentation and support for third-party security ecosystem

With SD-WAN 2.0, IT managers can create and automate a comprehensive overarching approach that includes the traditional network or perimeter FWs, but also in the cloud in a way that is tightly integrated. This technique, known as micro-segmentation, is commonly limited to software-defined networking (SDN) appliances. SD-WAN 2.0 will prevent lateral attacks originating in remote locations from infect in more insidious ways within the perimeter of a data center, public cloud, or SaaS applications that span private data centers (DCs), public clouds, and branch locations from a single highly automated management and control system.

Conclusion

As SD-WAN deployments have been primarily focused on delivering agile WAN connectivity that increased reach and agility while ensuring the core business applications can be deployed anywhere. SD-WAN 2.0 capability is "software-defined" security measures to supplement traditional security practices, offering increased control and visibility to the WAN in SD-WAN 1.0 deployments.

With SD-WAN 2.0, IT managers will benefit from a seamless and secure end-to-end infrastructure to deliver a range of IT agile WAN connectivity that increased reach and agility while ensuring the core business applications can be deployed anywhere.