Software-Defined WAN (SD-WAN)

SD-WAN ဆိုတာဘာလဲ??? Networking, Cloud, Security တွေနဲ့ဘယ်လို ဆက်နွယ်မှုတွေ ရှိလဲ???

လွန်ခဲ့တဲ့ နှစ်အနည်းအငယ်က WAN (Wide Area Network) နဲ့ ပတ်သက်ပြီးတော့ အရေးအကြီးဆုံး ပြောင်းလဲမှု ကိုပြုလုပ်ခဲ့ပါတယ်။ အဲ့ဒါကတော့ Software-Defined WAN Technology (SD-WAN) ကို Deploy လုပ်ခဲ့တာပဲဖြစ်ပါတယ်။ ၄င်း SD-WAN ဟာ Network Professional တွေအတွက် Optimization ကိစ္စတွေနဲ့ WAN Connectivity ရဲ့ Security ကိစ္စရပ်တွေကိုပါ ပြောင်းလဲ တိုးတက်စေခဲ့တာဖြစ်ပါတယ်။ အဲ့ဒီတော့ SD-WAN ဆိုတာ ဘာကြီးလဲ တစ်ချက် ကြည့်ရအောင်။

What is SD-WAN?

SD-WAN ဆိုတာကတော့ Software ကိုအခြေခံပြီးတော့ Datacenter တွေ၊ ရုံးတွေ၊ Enterprise တွေနဲ့ Cloud Resources တွေ အချင်းချင်း ကြားမှာရှိတဲ့ Connectivity ၊ Management နဲ့ Services တွေကို Control လုပ်တာပဲဖြစ်ပါတယ်။ SD-WAN ဟာလည်း SDN (Software-Defined Networking) လိုမျိုး Control Plane နဲ့ Data Plane ကို သီးသန့် သပ်သပ်စီ ခွဲထုတ်ခြင်းအားဖြင့် အလုပ်လုပ်တာပဲဖြစ်ပါတယ်။ SD-WAN Deployment မှာလည်း ကိုယ့် Infra မှာ နဂိုရှိပြီးသားRouter တွေ Switch တွေ နဲ့ Virtualized CPE (vCPE) တွေပဲ ပါဝင်တာပဲဖြစ်ပြီးတော့ ၄င်း Device တွေအနေနဲ့ Policy ၊ Security ၊ Networking နဲ့ အခြားသော Management Functions တွေကို Handle လုပ်နိုင်ရမှာ ဖြစ်ပါတယ်။ SD-WAN ရဲ့ Key Features တွေထဲက တစ်ခုကတော့ များစွာသော Connection Types တွေဖြစ်တဲ့ MPLS ၊ Broadband နဲ့ Wireless တွေကို Manage လုပ်နိုင်တဲ့ စွမ်းရည် ဖြစ်ပြီးတော့ WAN မှာဖြတ်သန်း နေတဲ့ Traffic တွေရဲ့ Segmentation ၊ Partition နဲ့ Security ကိုပါ Manage လုပ်နိုင်စွမ်းရှိတာပဲဖြစ်ပါတယ်။

What are the benefits of SD-WAN?

SD-WAN Technology ဟာဆိုရင် Popular ဖြစ်လာပါတယ်။ ဘာ့ကြောင့်လဲဆိုတော့ အခုလက်ရှိမှာ Companies တွေဟာ သူတို့ရဲ့ အမျိုးမျိုးသော Business Process တွေအတွက် Cloud-Based Applications တွေကို အသုံးများလာလို့ပဲ ဖြစ်ပါတယ်။ Traditional WAN မှာဆိုရင် ဥပမာ Branch Office ကနေ Head Office ဒါမှမဟုတ် Centralize Datacenter ကို ပြန်လာတဲ့ Backhaul Traffic တစ်ခုဟာ လမ်းကြောင်းတစ်လျှောက် နေရာတစ်ခု မှာ Security ချိုးဖောက်ခံရနိုင်ပါတယ်။ Branch Office ကနေ Traffic တွေကို Main Center တစ်ခုကိုပို့ ၊ ပြီးရင် Internet ကိုထွက် ၊ ဒါမျိုးဟာဆိုရင် Delay Time ပြဿနာတွေနဲ့ Network Performance ကိုပါကျဆင်းစေနိုင်ပါတယ်။ ဒါ့အပြင် Backhauling ဟာဆိုရင် Expensive ဖြစ်ပါတယ်။ ဘာလို့လဲဆိုရင် ၄င်းဟာ Branch Office တစ်ခုရဲ့ Traffic တွေဟာ Internet ကိုတိုက်ရိုက်တက်ရတာဖြစ်ပါတယ်။ ဘာလို့ Expensive ဖြစ်လဲဆိုရင် Branch Office တွေနဲ့

Headquarters တွေကြားထဲက Connection တွေဟာ MPLS-Based တွေဖြစ်ပါတယ်။ ၄င်း MPLS-Based Connections တွေဟာဆိုရင် Internet Broadband တွေနဲ့ Wireless WAN (4G,5G) links တွေထက် ပိုပြီး Expensive ဖြစ်ပါတယ်။ SD-WAN ရဲ့ Principle ကတော့ Company တွေအနေနဲ့ Branch Office တွေကို Link တွေချိတ်ဆက်တဲ့အခါမှာ Management ကို အရင်ကထက် ပိုကောင်းဖို့ဖြစ်ပြီးတော့ နောက်တစ်ခုကတော့ "Saving Money" ဖြစ်ပါတယ်။ Network Infrastructure Market ထဲမှာ SD-WAN ဟာ Fastest-Growing Segments တွေထဲကတစ်ခုအနေနဲ့ ဆက်လက်ချီတက်လျက်ရှိပါတယ်။ ပထမဆုံးအနေနဲ့ Traditional WAN Technology တွေဟာ လက်ရှိမှာ Modern Digital Business ရဲ့ လိုအပ်ချက်တွေနဲ့ ကိုက်ညီမှုမရှိတော့တာ တွေ့ရပါတယ်။ အထူးသဖြင့် SaaS Applications တွေနဲ့ Multi- and Hybrid-cloud Usage တွေအတွက် မကိုက်ညီတော့တာတွေ့ရပါတယ်။ ဒုတိယတစ်ခုအနေနဲ့ Enterprise တွေအနေနဲ့က WAN နဲ့ပတ်သက်ပြီး Multiple Connections တွေကိုလွယ်လွယ်ကူကူနဲ့ Manage လုပ်ချင်တာရယ် ၊ Application Performance တွေနဲ့ End User Experience တွေကို Improve ဖြစ်ချင်တာ ရယ် ၊ တို့နဲ့ပတ်သက်ပြီး စိတ်ဝင်စားလျက်ရှိနေကြပါတယ်။ Communication Service Providers တွေက ဦးဆောင်ပြီးတော့ SD-WAN ကို Deployment လုပ်ခြင်းဟာ Enterprise တွေကို Hybrid WAN Connection တွေအတွက် Dynamic Management ပြုလုပ်နိုင်ခြင်း၊ QoS အတွက် High Level Guarantee ပေးနိုင်ခြင်း ၊ စတဲ့ Abilities တွေကိုပေးစွမ်းနိုင်မှာပဲ ဖြစ်ပါတယ်။

How does SD-WAN help to improve network security?

SD-WAN ရဲ့ အားသာချက်ကတော့ Network Security ကောင်းခြင်းပဲ ဖြစ်ပါတယ်။ "SD-WAN က Customer တွေကို ဆိုင်ရာ Region အလိုက် Secure Zone လေးတွေခွဲထားပေးပါတယ်။ ဒါ့အပြင် မိမိတို့ရဲ့ Traffic တွေကို လုံလုံခြုံခြုံနဲ့ ကိုယ်ရဲ့ Local Internal Security Policies တွေကို အခြေခံပြီးတော့ ကိုယ်ပို့ချင်တဲ့ နေရာဆီကို ပို့နိုင်ပါတယ်။ SD-WAN ဟာ AWS နဲ့ Office 365 တို့လိုမျိုး Applications တွေအတွက် လိုအပ်တဲ့ Security Issues တွေအတွက်ပါ Design ပြုလုပ်ပြီးတော့ Collaboration လုပ်နေပါတယ်။ ဒါဟာ SD-WAN ကို Migration လုပ်ဖို့အတွက် အကြီးမားဆုံး Motivation ပါပဲ။" လို့ SP World Wide Technology ရဲ့ Network Solution Practice Director တစ်ဦးဖြစ်သူ Neil Anderson ကဆိုပါတယ်။ SD-WAN ဟာ Enterprise တွေအတွက် Critical Traffic တွေနဲ့ Vulnerabilities တွေကို Partition နဲ့ Protection ပြုလုပ်ပေးနိုင်စွမ်းရှိမှာလည်းဖြစ်ပါတယ်။ ဒီ Cases တွေဟာ Retail ၊ Healthcare နဲ့ Financial Services တွေအတွက် အရေးကြီးပါတယ်။ ဒါ့အပြင် SD-WAN Solutions တွေမှာ Firewall Capabilities တွေ ပါဝင်လာမှာ ဖြစ်ပြီးတော့ Companies တွေအနေနဲ့ Branch Office တွေမှာ Security Compromise လုပ်စရာမလိုပဲ SD-WAN Quick Deploy ပြုလုပ်နိုင်မှာဖြစ်ပါတယ်။ ဥပမာအားဖြင့် Network Administrator အနေနဲ့ Network မှာ Identity (or) Roles တွေအရ Network Segment အလိုက် Zone တွေခွဲပြီးတော့ Intrusion တွေ ရှာဖွေခြင်းနဲ့ကာကွယ်ခြင်း (DDoS)၊ Deep Packet Inspection ၊ App Based Filtering ၊ Active

Network Connection Monitoring ၊ Data Encryption ၊ Log Security Events ၊ Tightly Integrating Cloud-Security Functions (Secure Web Gateway ၊ Cloud Access Security Brokers (CASB) ၊ Zero-Trusted Network Access) တို့ကိုလုပ်ဆောင်နိုင်မှာဖြစ်ပါတယ်။

Will SD-WAN kill MPLS?

SD-WAN နဲ့ပတ်သက်ပြီး Hot ဖြစ်နေတဲ့ ဝေဖန်မှုတစ်ခုကတော့ SD-WAN ဟာ MPLS နေရာကို ပြောင်းလဲအစားထိုးယူမလားဆိုတာပဲ ဖြစ်ပါတယ်။ MPLS ကိုအများဆုံးအသုံးပြုရတဲ့ Cases တွေကတော့ Branch Offices ၊ Campus Networks ၊ Metro Ethernet Services ၊ Enterprise တွေနဲ့ QoS For Real-time Applications တွေပဲ ဖြစ်ပါတယ်။ Networking Vendors တွေကတော့ MPLS ဟာ အချိန်အကြာကြီး ဆက်လက်တည်ရှိနေဦးမှာဖြစ်ပြီးတော့ SD-WAN ဟာ MPLS ရဲ့ လိုအပ်ချင်တွေ အားလုံးကို အစားထိုးဖြည့်ဆည်းနိုင်မှာ မဟုတ်ဘူးလို့ ယုံကြည်နေကြပါတယ်။ Gartner ကတော့ Organization အများစုအနေနဲ့ Expensive ဖြစ်တဲ့ MPLS Connections တွေကို Internet-based VPNs တွေနဲ့ အစားထိုးခြင်းအားဖြင့် ၄င်းတို့ရဲ့ WAN Expansion နဲ့ Updates တွေကိုရရှိလာနိုင်မယ်လို့ ပြောပါတယ်။ SD-WAN ဟာအခုနောက်ပိုင်းမှာမယုံနိုင်လောက်အောင် ရိုးရှင်းလာပါတယ်။ အဲ့လို ရိုးရှင်းလာရတာဟာလဲ အကြောင်းပြချက်တွေရှိနေပါတယ်။ ရိုးရှင်းလွယ်ကူတဲ့ Operational Environment တွေနဲ့ အမျိုးမျိုးသော Carrier Operators တွေဆီကနေ Multiple Circuit တွေကို အသုံးပြုနိုင်စွမ်း ရှိတာတွေကြောင့် Enterprise တွေအနေနဲ့ Logical Layer ကနေ Transport Layer အထိ ဆွဲချုံ့နိုင်မှာဖြစ်ပြီးတော့ Service Provider တွေဆီကနေ အမှီအခိုလဲ နည်းလာမှာဖြစ်ပါတယ်။အဲ့လိုမျိုး Layer တွေခွဲထုတ်လိုက်ခြင်းဟာ Multiple Service Provider တွေကို ဘယ် Organization ဟာ ၄င်းတို့ရဲ့ WAN Connections တွေကို ဘယ် Service Provider ကနေ Offering လုပ်ပေးနေတယ် ဆိုတာကို သိသာစေမှာဖြစ်ပါတယ်။ Traditional Service Provider တွေအနေနဲ့လဲ Orchestrate Services (SD-WAN, Security, WAN Optimization) တွေကို ပေါင်းစပ်ထားတဲ့ NFV-based Offerings (Network Function Virtualization) တွေကို Support ပေးနိုင်မှာပဲ ဖြစ်ပါတယ်။ Virtualized Network Functions တွေကတော့ Routing ၊ Mobility နဲ့ Security ပဲ ဖြစ်ပါတယ်။ Customer တွေအနေနဲ့ MPLS ကိုပဲဆက်ပြီးအသုံးပြုလိမ့်မယ်လို့ ထင်ရတဲ့ အကြောင်းပြချက်ရှိပါတယ်။ ဒါကတော့ " Customer တွေအနေနဲ့ Outages ဖြစ်တဲ့အခါမှာ System Backup ဘယ်လိုလုပ်ကြမလဲဆိုတာ စိုးရိမ်စရာပါ " လို့ Anderson ကပြောပါတယ်။ "အခုအချိန်မှာက MPLS နဲ့အတူ အခြားသော Technologies တွေကလည်း အဆင့်အတန်းတစ်ခုအနေနဲ့ရှိနေပါသေးတယ် " လို့ဆက်လက်ပြီးပြောကြားပါတယ်။ ကျွမ်းကျင်သူတွေကတော့ Enterprise တွေအနေနဲ့ SD-WAN ကို MPLS မှာကျန်ရှိနေသေးတဲ့ Legacy Applications တွေနဲ့ Internet Traffic တွေကို SD-WAN အပေါ် Offload ချဖို့အတွက် Hybrid Approach အနေနဲ့ ချဉ်းကပ်လာနိုင်ပါတယ်လို့ သုံးသပ်နေကြပါတယ်။

How SD-WAN involves cloud environments?

Security ကောင်းခြင်းနဲ့ Traditional WAN Costs တွေကို လျှော့ချခြင်းဟာ SD-WAN ကို Adopt လုပ်ဖို့ အကြောင်းပြချက် တစ်ခုဖြစ်ပါတယ်။ နောက်တစ်ခုကတော့ Cloud Services တွေကို လုံလုံခြုံခြုံနဲ့ လျင်လျင်မြန်မြန် Setup လုပ်ဖို့ပဲ ဖြစ်ပါတယ်။ SD-WAN Technologies တွေကို အသုံးများစေတဲ့ အကြောင်းအရင်းအများကြီးထဲကမှအဓိကကျတဲ့ အချက်တစ်ခုကတော့ Edge ကနေလှမ်း Access လုပ်လို့ရတဲ့ Containers တွေနဲ့ Cloud-based Applications တွေအသုံးပြုမှု မြင့်တက်လာလို့ပဲ ဖြစ်ပါတယ်။ Customer တွေအနေနဲ့ ၄င်းတို့ရဲ့ Data Center တွေကို Cloud Resources တွေနဲ့ Tie လုပ်ဖို့အတွက် SD-WAN Technologies တွေကို တော်တော်များများ အသုံးပြုလာကြပါတယ်။ "SD-WAN ဟာ လွန်ခဲ့တဲ့ ၂ နှစ်လောက်ကမှ စတင်ထွက်ပေါ်လာခဲ့ပြီးတော့ Resources တွေကိုအသုံးပြုဖို့အတွက် လျင်လျင်မြန်မြန် နဲ့ ဈေးသက်သက်သာသာ ဖြစ်စေခဲ့ပါတယ် " လို့ Anderson က ဆိုပါတယ်။ SD-WAN နဲ့ပတ်သက်ပြီး အရေးကြီးတဲ့ အချက်တစ်ခုကို ဖန်တီးနေတာကတော့ Premises တွေနဲ့ Public Cloud အကြားမှာ Data Resources တွေလျင်လျင်မြန်မြန် စီးဆင်းဖို့ပဲ ဖြစ်ပါတယ်။ Enterprise တွေအနေနဲ့ ၄င်းတို့ ရဲ့ Private Data Center တွေ ပိုပြီးDevelop ဖြစ်လာဖို့နဲ့ ၄င်းတို့ရဲ့ Public Cloud Servicesတွေအသုံးပြုမှု ပိုမို ကျယ်ပြန့်လာဖို့အတွက် ရှေးရှု ဆောင်ရွက်လျက် ရှိနေပါတယ်။

Where does SD-Branch fit into SD-WAN?

SD-WAN ရဲ့အခြားသော Software-based Technology တစ်ခုကတော့ SD-Branch လို့ခေါ်ပါတယ်။၄င်းဟာ Hardware Platform တစ်ခုဖြစ်ပြီးတော့ SD-WAN ၊ Routing ၊ Integrated Security နဲ့ LAN/Wifi Functions တွေကို Support ပေးပြီးတော့ Centralize Manage လုပ်နိုင်ပါတယ်။ အများဆုံး အငြင်းပွားဖွယ်ရာ ကိစ္စတစ်ခုကတော့ SD-Branch ရဲ့ Operational Agility (လျင်မြန်မှု) ပဲ ဖြစ်ပါတယ်။ SD-Branch နဲ့ဆိုရင် IT Organization တွေအနေနဲ့ နေရာအသစ်တွေမှာ Branch-in-a-box Solutions တွေကိုလျင်လျင်မြန်မြန် Deploy လုပ်နိုင်မှာပဲ ဖြစ်ပါတယ်။ Centralize Management Console ဖြစ်တဲ့အတွက်ကြောင့် Branch အားလုံးရဲ့ Network နဲ့ Security Functions တွေကို တစ်နေရာထဲကနေ ထိန်းချုပ် ချိန်ညှိနိုင်မှာပဲ ဖြစ်ပါတယ်။ Branch တွေကို Remote နဲ့ဝင်ပြီး Control လုပ်ဖို့အတွက် IT Personnel လိုအပ်ချက် ကိုလည်းလျှော့ချနိုင်တဲ့အတွက် Cost နဲ့ Time ကို သိသိသာသာ သက်သာစေမှာဖြစ်ပါတယ်။ တစ်စုတစ်စည်းထဲရှိတဲ့ Hardware တွေပေါ်မှာ Software Deploy လုပ်ခြင်းဖြင့် Hardware Cost ကိုလည်းသက်သာစေမှာဖြစ်ပါတယ်။ SD-Branch Deployment မှာဆိုရင် Network Functions တွေကို Virtualized Environment အတွင်းမှာ Run နိုင်မှာဖြစ်ပါတယ်။ "SD-Branch Deployment ဟာဆိုရင် Virtual Appliances တွေကိုတောင် Discrete Functions တွေဖြစ်အောင် ခွဲခြမ်းနိုင်မှာဖြစ်ပြီးတော့ ၄င်း Functions တွေကို Centralize Control လုပ်နိုင်မှာဖြစ်ပါတယ် " လို့ Cisco က ဆိုပါတယ်။ Cisco ဟာ SD-Branch နဲ့ SDN Separate Monolithic Appliances တွေကို

ရိုးရှင်းတဲ့ Functions တွေပါတဲ့ System တစ်ခုဖြစ်အောင် ပေါင်းစပ်လိုက်ပြီးတော့ ပြောင်းလဲနေတဲ့ လိုအပ်ချက်တွေနဲ့အညီ လိုက်လျောညီထွေ ဖြစ်အောင် လွယ်ကူစွာ Configure ချနိုင်အောင် ဆောင်ရွက်လျက် ရှိနေပါတယ်။ Business တွေအနေနဲ့ ကတော့ SD-Branch ကို Costs တွေ လျှော့ချဖို့ ၊ Reliability ကောင်းဖို့ ၊ Management လုပ်ရတာလွယ်ကူဖို့ နဲ့ လျင်မြန် မြန်ဆန်မှုတို့အတွက် အသုံးပြုကြပါတယ်။

How does SASE relate to SD-WAN?

Secure Access Service Edge (SASE) ဆိုတာက ၂၀၁၉ ခုနှစ်မှာ Gartner က သတ်မှတ်ခဲ့တဲ့ Term တစ်ခုဖြစ်ပါတယ်။ ၄င်းကတော့ WAN နဲ့ Security Control အတွက် Cloud-based Service အနေနဲ့ ထွက်ပေါ်လာခဲ့တဲ့Technology တစ်ခုဖြစ်ပါတယ်။ SASE ကို End User Devices ၊ Internet of Things (IoT) Sensors တွေနဲ့ Edge Locations နေရာတွေမှာအသုံးပြုနိုင်ပါတယ်။ SASE မှာ များစွာသော Technologies တွေကိုပေါင်းစပ်ထားတာဖြစ်ပါတယ်။ အဲ့ဒီ Technologies တွေကတော့ SD-WAN ၊ Next Generation Firewall (NGFW) နဲ့ Firewall as a Service (FWaaS) တို့ဖြစ်ကြပါတယ်။ ၄င်း Technologies တွေက WAN နဲ့ပတ်သက်တဲ့ Network Security Services တွေဖြစ်တဲ့ CASB ၊ FWaaS ၊ Zero Trusted into the single နဲ့ Cloud-Delivered Service Model တွေအားလုံးကိုလွှမ်းမိုးထားနိုင်ပါတယ်။ Gartner အနေနဲ့ အဓိပ္ပာယ် သတ်မှတ်ထားတာကတော့ Network နဲ့ Network Security ဆိုတာကတော့ Software-defined နဲ့ Cloud Delivered ဖြစ်ဖို့လိုအပ်ပြီးတော့ Vendor တွေရဲ့ ရွေးချယ်မှုနဲ့ ၄င်းတို့ရဲ့ Infrastructure တွေမှာပြောင်းလဲမှုတွေ ပြုလုပ်ဖို့လိုအပ်တယ်လို့ ဆိုပါတယ်။ SD-WAN Deployment လုပ်ဖို့ပြင်ဆင်နေကြတဲ့ Enterprise တွေရယ် MPLS ကနေ Internet Traffic တွေကို Offload ချဖို့ ကြိုးစားနေကြတဲ့ Enterprise တွေအနေနဲ့ကတော့ SASE ကိုအသုံးပြုမှု တစ်ဖြည်းဖြည်း မြင့်မားလာပါတယ်။ ဒါပေမဲ့လဲ အတော်များများကတော့ Gartner ရဲ့ သတ်မှတ်ချက်ကို သိပ်သဘောမကျကြပါဘူး။ ဥပမာအားဖြင့် IDC Analyst တစ်ယောက်ဖြစ်တဲ့ Brandon Butler ကတော့ "SD-WAN က SD-Branch အဖြစ်ကို ပြောင်းလဲနေပါတယ်။ ပြီးတော့ SASE ဆိုတာကတော့ Technology အသစ်တစ်ခုဆိုတာထက် Gartner ရဲ့ Marketing Term တစ်ခုထက်မပိုပါဘူး " လို့ဆိုပါတယ်။

What does SD-WAN have to do with SDN?

Programmability ဆိုတဲ့ Idea တစ်ခုကတော့ SD-WAN နဲ့ ၄င်းရဲ့ အကိုကြီး ဖြစ်တဲ့ SDN (Software Defined Networking) တွက် အခြေခံတစ်ခုဖြစ်ပါတယ်။ SDN ဆိုတာက Data Plane နဲ့ Control Plane ကိုသပ်သပ်စီခွဲထုတ်ပြီးတော့ Network Traffic တွေကို Forward လုပ်တဲ့ Technology ပဲဖြစ်ပါတယ်။ "Datacenter SDN Architecture တွေမှာ Software-Defined Overlays တွေ ဒါမှမဟုတ် Controllers တွေကို အသုံးပြုပြီး Underlying Network Hardware တွေကနေ ခွဲထုတ်ထားတဲ့အတွက် Network တစ်ခုလုံးကို Intent- ဒါမှမဟုတ် Policy-based Management တွေပြုလုပ်နိုင်မှာဖြစ်ပါတယ်။ Results တွေအနေနဲ့ကတော့ Datacenter တွေမှာ Application

Workloads လိုအပ်ချက်တွေကို Automated Provisioning ၊ Programmatic Network Management နဲ့ Pervasive Application-Oriented Visibility တို့ကိုအသုံးပြုပြီးတော့ ဖြည့်ဆည်းနိုင်မှာဖြစ်ပါတယ်။ ထို့အပြင်အခြားလိုအပ်တဲ့နေရာတွေမှာပါ Direct Integration ကို Cloud Orchestration Platforms တွေကိုအသုံးပြုပြီး ဖြည့်ဆည်းသွားမှာဖြစ်ပါတယ် " လို့ IDC ကဆိုပါတယ်။ SDN ဆိုတာက Network တွေကို Statically Defined လုပ်ရတဲ့ Complexity တွေကိုလျှော့ချပေးပြီးတော့ Network Functions တွေကို လွယ်လွယ်ကူကူ Automated လုပ်နိုင်ဖို့ ရည်ရွယ်ထားတာဖြစ်ပါတယ်။ Network Resources တွေကို ရိုးရိုးရှင်းရှင်း Customize လုပ်နိုင်ဖို့လည်း ရည်ရွယ်ပြီး တော့ Data Center တွေ Campus Network တွေနဲ့ WAN တွေလိုမျိုးကြိုက်တဲ့နေရာကတော့ Manage လုပ်နိုင်ဖို့ ရည်ရွယ်ပါတယ်။

What are some pitfalls of SD-WAN?

SD-WAN ရဲ့ အားသာချက်တွေကို ခဏမေ့ထားပြီးတော့ SD-WAN နဲ့ပတ်သက်ပြီး Companies တွေအနေနဲ့ ကြိုတင်စဉ်းစားထားသင့်တဲ့ မထင်မှတ်ပဲဖြစ်လာနိုင်တဲ့ အန္တရယ်တွေကိုချပြလိုပါတယ်။ Pitfalls ၅ ခုရှိပါတယ်။

⚠ Limited Cost Savings

⚠ Operating SD-WAN without integrating security tools

⚠ Performance and implementation struggles

⚠ Lack of visibility and analytics , especially for security

⚠ Failure to futureproof by not considering private 5G for SD-WANs

သို့ပေမဲ့လဲ Industry တွေအနေနဲ့ SD-WAN Deployment တွေများလာတဲ့အခါမှာ အထက်ပါ Issues တွေကိုကြုံတွေ့လာနိုင်ပြီး Vendor တွေအနေနဲ့လဲ ၄င်း Issues တွေကို သတိပြုမိလာနိုင်ပြီးတော့ ပြင်ဆင်လာကြတဲ့အခါမှာ Customer တွေအနေနဲ့ SD-WAN Deployment တွေကို ပိုမိုကောင်းမွန်အောင် ကျွမ်းကျင်စွာနဲ့ Handle လုပ်လာနိုင်မှာဖြစ်ပါတယ်ခင်ဗျာ....။

ကိုလွင် (Network)

#ref: News | Network World