AT A GLANCE

Security Challenges in the Data Center

SOLVED WITH THE HPE ARUBA NETWORKING CX 10000 SERIES SWITCH

INTRODUCTION TO DATA CENTER SWITCHING

In a data center, network switches comprise what is referred to as the data center ***Fabric***. In this fabric most of the traffic stays within the data center, this is typically referred to as ***East-West*** traffic. Within the Fabric are the ***Spine*** switches (also known as "core" switches) and ***Leaf*** switches (also known as "Top of Rack" or "ToR" switches). Data Center ***Servers***, high performance compute devices where organizations execute their applications, are connected to TOR switches. Data center ***Stateful Services*** are provided by separate devices, such as security firewalls and load balancers, are also connected to dedicated ToR switches and appliances, generally referred to as a ***Service POD***.

THE PROBLEM WITH DATA CENTER SECURITY FIREWALLS

In a typical data center, firewalls inspect only a small amount of the traffic, generally only as it enters and leaves the data center fabric. To secure the east-west traffic, an agent(s) is required or the data needs to be re-directed to a firewall from a ToR switch. The firewall then forwards approved traffic to the designated endpoint based upon a pre-set policy (i.e. permissions). This could be back to the switch where it originated or to another switch within the data center fabric.

There are several problems with this scenario:

- Additional packet traffic in the data center fabric can cause bottlenecks and latency
- Standalone firewall hardware and licensing adds significant additional costs
- Firewall devices add (yet another) point of management
- Agents are costly and difficult to manage and keep up to date
- Scaling the data center fabric for growth gets cumbersome and expensive

SECURITY CHALLENGE SOLVED WITH THE HPE ARUBA NETWORKING CX 10000 SERIES SWITCH

HPE Aruba Networking CX 10000 switch series is the industry's first and only switch with embedded firewall capabilities on all ports. Due to this unique and highly differentiated architecture, security policy decisions can be made at the top of rack switch instead of requiring data packets to be forwarded to a separate standalone firewall. The expense and complexity of redirecting packets to separate firewalls has made securing traffic inside of the data center impractical, if not impossible. The HPE Aruba Networking CX 10000 switch series makes securing east-west traffic practical by eliminating the additional cost(s) and complexities of "plumbing" traffic to these external appliances and/or deploying agents on every server.

THE BOTTOM LINE: TAKEAWAYS ABOUT ARUBA CX 10000 SERIES SWITCH

- Lower upfront and total cost of ownership
- Reduced data center traffic = better performance
- Single point of management = easier automation
- Highly scalable = fewer devices, with less costs and greater efficiencies