Business Goals

- Reduce troubleshooting costs with more network visibility

- Monitor network level SLAs accurately with the right tools in the right places

- Optimize the usage of tools and reduce CapEx by avoiding unnecessary tools

cPacket's Benefits

- Complete visibility at all speeds and feeds

- Provide value to specialized tools with network level (NPM) information

- 'Single pane of glass' access to all cPacket sensors

- Integrate with other external devices using RESTful APIs for automation

According to a study by IHS, downtime is costing North American organizations $700 billion per year. This downtime ranges from $1 million a year for a typical mid-size company to $60 million a year for a large enterprise.

An estimated $700 billion is spent on troubleshooting and resolving issues in the datacenter (DC). However, a well-designed data center architecture can minimize troubleshooting time, improve network visibility, and reduce an organization's total cost of ownership (TCO). For instance, accurate remote management of devices can reduce troubleshooting costs by up to 70%. Therefore, it's imperative to configure these devices for easy in-band and out-of-band management. This will eliminate the need for a technician to travel onsite in order to troubleshooting the issue. By having remote management and visibility, NetOps can proactively take action to resolve impending issues such as modifying policies, security rules, modifying routes, and/or changing appropriate filters.

This use case will explain how to build an efficient packet broker architecture in a DC to provide pervasive network visibility for your specialized tools. The benefits of this architecture will result in optimized tool utilization, improved efficiency of network operations, reduced MTTR, and increased network uptime. By building such an architecture, organizations will benefit from a reduction in TCO, greater ROI, and a stronger competitive advantage.

Visibility is key to efficient maintenance and troubleshooting. Having a complete visible monitoring architecture that allows NetOps to quickly access any part of the DC architecture, right from the servers dangling off the leaf nodes to the core, will allow for quicker troubleshooting.
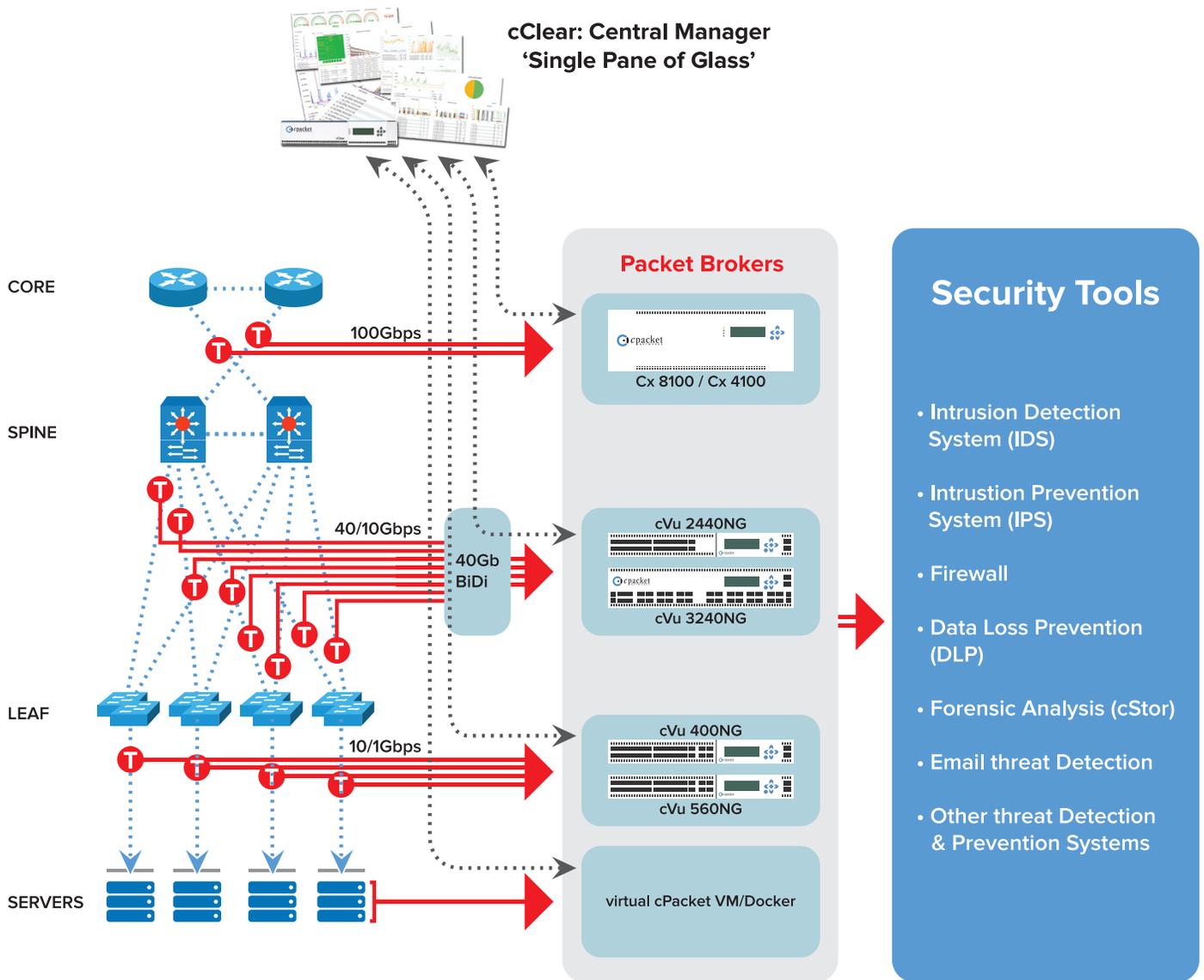
cClear: Central Manager 'Single Pane of Glass'

Packet Brokers

Security Tools

CORE

100Gbps

Cx 8100 / Cx 4100

SPINE

40/10Gbps

40Gb BiDi

cVu 2440NG

cVu 3240NG

LEAF

10/1Gbps

cVu 400NG

cVu 560NG

SERVERS

virtual cPacket VM/Docker

- Intrusion Detection System (IDS)
- Intrustion Prevention System (IPS)
- Firewall
- Data Loss Prevention (DLP)
- Forensic Analysis (cStor)
- Email threat Detection
- Other threat Detection & Prevention Systems

Figure 1: Data center topology with an efficient packet broker architecture

Figure 1 above shows a typical core-spine-leaf topology in a DC, tapped and connected to cPacket's monitoring devices. The devices suggested are based on speeds, feeds and performance suitable for each layer. As seen in Figure 1 above, it is evident that cVu devices can be used throughout the network to provide the necessary visibility. cVus come in multiple form factors and can scale from 1Gbps to 100Gbps.

Typically, the core of a data center is a 40Gbps network. However, to keep pace with today's network challenges, many customers are quickly migrating to a 100Gbps network. As a result, cPacket has launched two new additions to the Cx series that provide high level network performance and scalability : Cx 8100 (8 x 100Gbps) and Cx 4100 (4 x 100Gbps).

Spine layer switches are characteristically 40Gbps. cPacket's cVu 3240NG and cVu 2440NG are suited to monitor at these speeds.

As one moves down the topology, speeds become lower. Switches at the leaf layer are mostly 10Gbps. They are predominantly constrained to those speeds to match that of the server's network interface. So for these speeds and port densities, customers will likely choose to deploy cVu 400NG or cVu 560NG devices.

Virtualization is a pervasively used technology in servers because it provides easy management and flexibility to dynamically instantiate and migrate applications. In order to monitor the performance inside the servers, virtual cPacket devices are deployed as VMs and Docker containers. These virtual devices will seamlessly integrate with the rest of the hardware-based devices in the cVu family.

Once the data center switches are efficiently tapped and network traffic is fed to the packet brokers, the remainder of the architecture becomes easy, flexible, and responsive to any troubleshooting and monitoring needs. The packet broker ports can be connected to any specialized monitoring and security tools which may be required to perform an in-depth analysis. When the packet broker architecture uses the cPacket solution, monitoring and managing become highly flexible. cVus devices, which provide packet broker, traffic sensing and security related functionality, are managed by cClear, which is the central management and visualization platform. cStors, which are packet capture and forensic analysis devices, can be connected to cVus for deep packet analyses. Furthermore, any other specialized security and NPM tools can be connected to the cVu for a deeper analysis. The entire solution is managed by cClear which collects and correlates KPIs in real-time with nanosecond accuracy and millisecond resolution that can be visualized on easy to use dashboards.

Benefits

Choosing the right network architecture that can monitor and troubleshoot issues will provide organizations with a stronger competitive advantage and substantial cost reductions. SecOps and NetOps can leverage the increased network transparency and visibility to make informed and accurate decisions. cPacket's solution provides comprehensive network and NPM related metrics to enable downstream tools the ability to provide more intelligent insights. This will simplify decision making, improve the verification of network configurations, and reduce MTTR for more efficient network operations.

Unlock the Advantages with cPacket

cPacket's solutions offer unprecedented performance, deeper levels of insight, and real-time analytics to solve the most complex network challenges faced in today's enterprises. cPacket's advanced distributed intelligence enables network operators to proactively detect problems before they negatively impact end-users using predictive analytics. cPacket provides a unique algorithmic chip that delivers complete packet inspection immediately at the wire for accurate results.

cPacket Networks is committed to achieving quality standards in network performance monitoring and is trusted by network operators worldwide.