White Paper

Redefine Network Visibility in the Data Center with the Cisco NetFlow Generation Appliance

What You Will Learn

Modern data centers power businesses through a new generation of applications, service delivery solutions, and hosting models. The number of applications is growing, application architecture is increasingly complex, workloads are mobile, and traffic patterns are becoming difficult to predict. Virtualization, cloud computing, high-performance computing, data warehousing, and disaster recovery strategies, among other factors prevalent in the current environment, are prompting a whole new set of requirements for more detailed traffic visibility in data centers. The modern data center is also demanding new techniques and best practices for managing network and application delivery, helping ensure business continuity, and reducing any impact of failure scenarios on revenue streams. The Cisco® NetFlow Generation Appliance (NGA) helps address these challenges.

Management Challenges

The increasing complexity of the data center is presenting numerous challenges to IT administrators:

- Security: Can I detect and thwart network security attacks and protect my business assets?
- Billing: How do I truly quantify the use of network resources for effective monetization?
- Troubleshooting: Are my business-critical applications getting the network resources they need to deliver committed service levels? Are noncritical applications contending for resources and affecting the performance of my business applications?
- Capacity planning: Do I have a good understanding of my network load and can I confidently plan for growth? Can I align my IT investment and effectively support the business goals?
- Resource optimization: Do I understand physical and virtual machine network traffic trends sufficiently to help ensure efficient use of network resources? How do I effectively support workload mobility and take advantage of my hybrid cloud deployment?
- Operations: How can I get 100 percent flow visibility without affecting network device performance? Can I get end-to-end visibility across multiple network segments without requiring network reconfiguration?

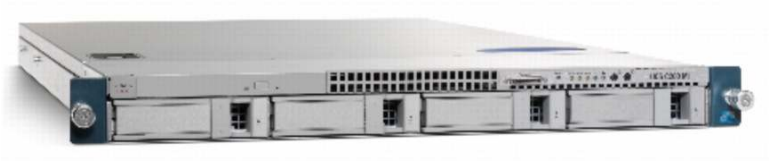
The Solution: Cross-Device Approach to Flow Analysis with Cisco NetFlow Generation Appliance

Cisco NGA introduces a cross-device approach to flow analysis, facilitating hop-by-hop flow visibility across multiple network segments. This visibility is achieved by connecting Cisco NGA to multiple network devices, such as Cisco Nexus® 7000 and 5000 Series Switches and Cisco Catalyst® 6500 Series Switches, using Switched Port Analyzer (SPAN) or a network tap, and exporting flow information for the traffic of interest. The solution enhances operating efficiency, improves network return on investment (ROI), and reinforces network security.

Overview of Cisco NGA

The Cisco NetFlow Generation Appliance (NGA) 3140 (Figure 1) redefines network visibility and establishes a new standard for high-performance, cost-effective solutions for flow visibility. It empowers network operations, engineering, and security teams with actionable insight into network traffic for the purposes of resource optimization, application performance improvement, traffic accounting, and security.

Figure 1. Cisco NGA 3140

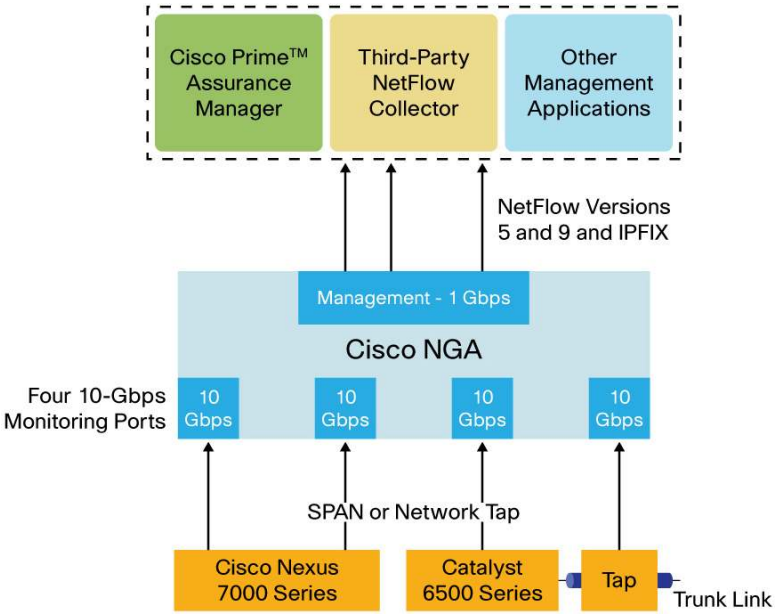


High-Performance Architecture for Flow Visibility

Cisco NGA is a purpose-built, high-performance solution for flow visibility in high-throughput Gigabit Ethernet networks typical in most data centers and campus core deployments. To simplify operation manageability, the appliances can be deployed at critical observation points such as the server access layer, fabric path domains, and Internet exchange points. The power of visibility is dramatically amplified when Cisco NGA is connected to multiple network devices to analyze flows hop by hop - essential for security, capacity planning, and troubleshooting.

Designed for high performance and deployment flexibility, the appliance gathers network data from platforms such as Cisco Nexus 7000 and 5000 Series Switches and Cisco Catalyst 6500 Series Switches using SPAN and network taps. It implements a large active flow cache and can be configured to export NetFlow records (NetFlow Versions 5 and 9 and Internet Protocol Flow Information Export [IPFIX]) to multiple collectors. The NetFlow Data Export (NDE) records are exported using Weighted Round-Robin (WRR) to achieve load balancing or flow replication across collectors. The exports can also be customized to meet specific management application needs using 10 filters per destination (Figure 2).

Figure 2. Cisco NGA Solution Architecture



Main Benefits

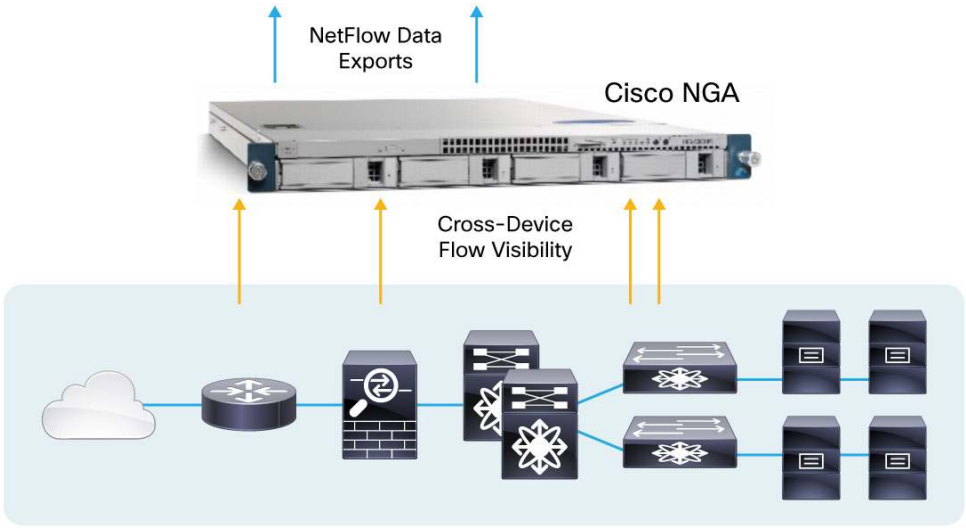
Improved Network ROI

Cisco NGA helps improve the effective use and monetization of both switching and network resources. It offers the option to offload the NetFlow generation function from the network device and dedicate the CPU cycles to increase forwarding performance. In addition, accurate characterization of network use allows true sizing of the network resources to support business needs. The information also becomes the basis of any billing or chargeback mechanism implemented by IT for effective monetization.

Enhanced Operation Efficiency

Cisco NGA allows you to combine flow visibility across different observation points in the network, drastically reducing the time it takes to solve a performance problem. This capability is especially powerful in Layer 2 networks for identifying network bottlenecks and behavior that affects performance. For example, Cisco NGA can be used for combined visibility across multiple access switches and server access VLANs and for comparing flows before and after implementing network services such as firewalls and Network Address Translation (NAT). The visibility not only helps in troubleshooting but also in validating network service policies: for instance, in isolating incidents when a firewall may be dropping flows, affecting application performance.

Figure 3. Cross-Device Flow Visibility



Operation design efficiency is also enhanced by the use of the same source of flow visibility for up to six collectors representing different management applications. The exports are replicated or load balanced using WRR across multiple collectors, and you can apply filters per destination to meet the needs of specific applications. For example, the security application may need visibility into every flow, whereas network troubleshooting may require visibility into specific application traffic flows.

Reinforced Network Security

Network threat analysis is one of the most compelling use cases for Cisco NGA. Cisco NGA can provide visibility into every flow, providing multihop flow information so that you can detect and analyze suspicious network behavior.

Deploying Cisco NGA to Address Management Challenges

Cisco NGA offers the deployment flexibility to enable a broad range of use cases to ease manageability in the data center. Common use cases include:

- Profiling of server access network traffic
- Characterization of traffic across Cisco FabricPath domains
- Visibility into hosted application traffic, such as Oracle, FTP, Microsoft Exchange, Citrix Remote Desktop, and Common Internet File Service (CIFS) traffic
- Application performance troubleshooting
- Capacity planning
- Quality-of-service (QoS) monitoring and validation
- Cyber threat detection through traffic behavior visibility
- Traffic utilization of IP storage, such as Small Computer System Interface over IP (iSCSI, Network File System (NFS), Fibre Channel over Ethernet (FCoE), and Serial Attached SCSI (SAS)
- Interactions across virtual machines in a virtual server environment
- Characterization of peering traffic across Internet exchange points (IXPs)
- Monitoring of Border Gateway Protocol (BGP) traffic

Some of the use cases are discussed in greater detail in the following sample deployment topologies.

Deployment Scenario 1: Visibility Across Cisco FabricPath Domain

Cisco FabricPath is an innovation in Cisco NX-OS Software that brings the stability and scalability of routing to Layer2. The switched domain does not have to be segmented any more, providing data center–wide workload mobility. With the scalability of the Layer 2 domain, it is critical to gain end-to-end hop-by-hop visibility into traffic flows across the domain. This visibility allows comprehensive insight into virtual machine network traffic, server access VLANs, and workload mobility to ease manageability of Cisco FabricPath domains (Figures 4 and 5).

Figure 4. Cisco NGA Deployment in a Data Center Using SPAN

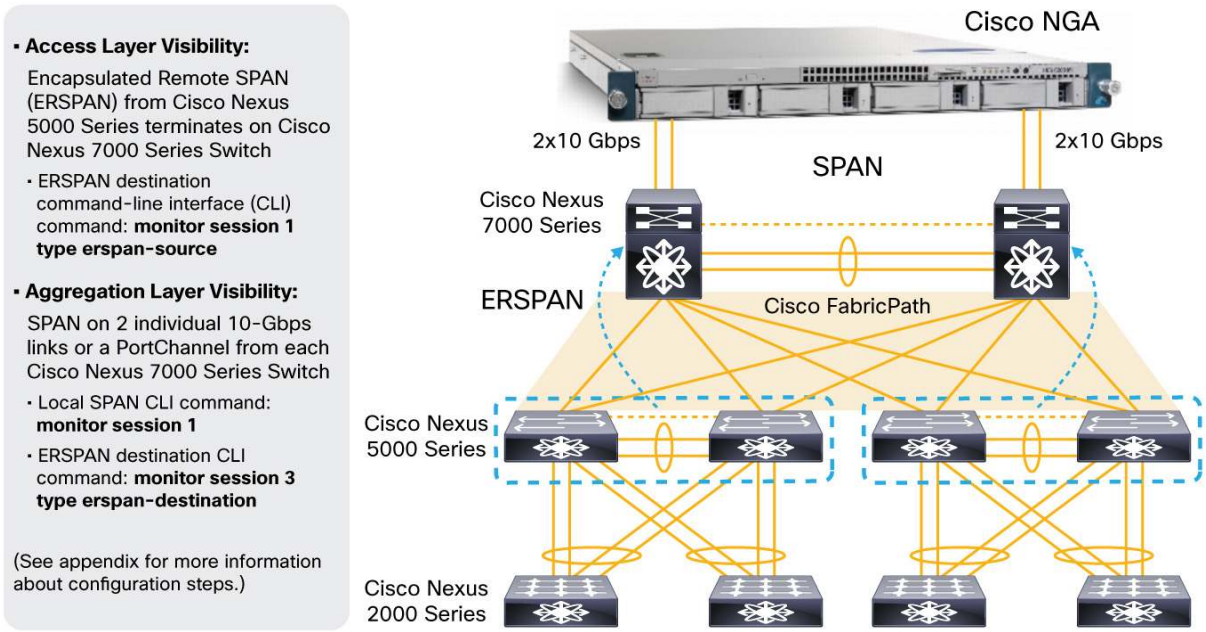
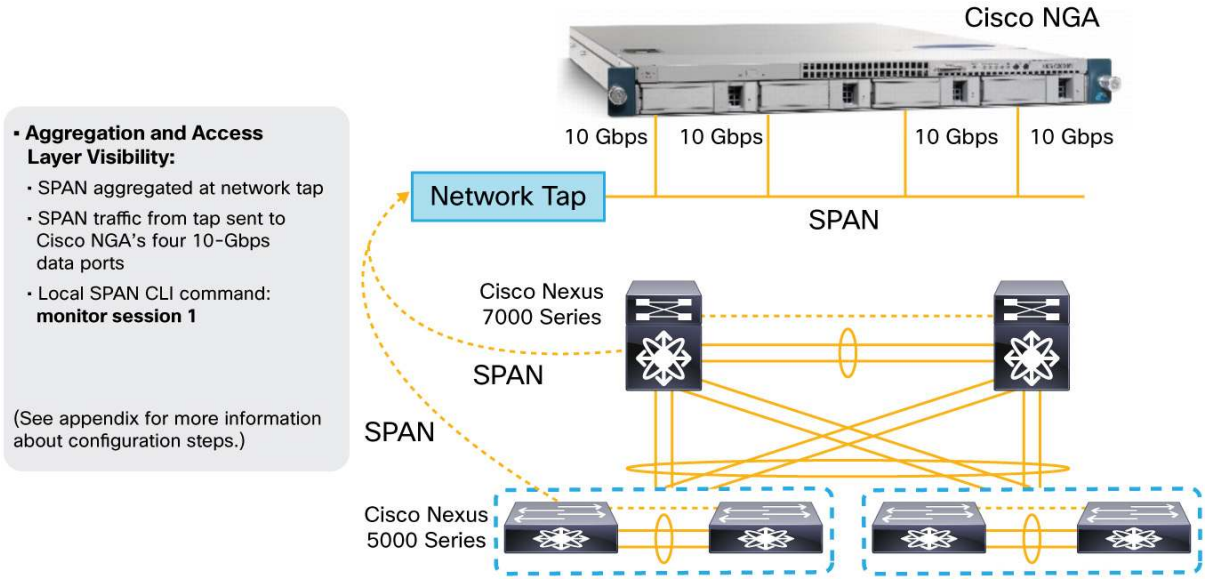


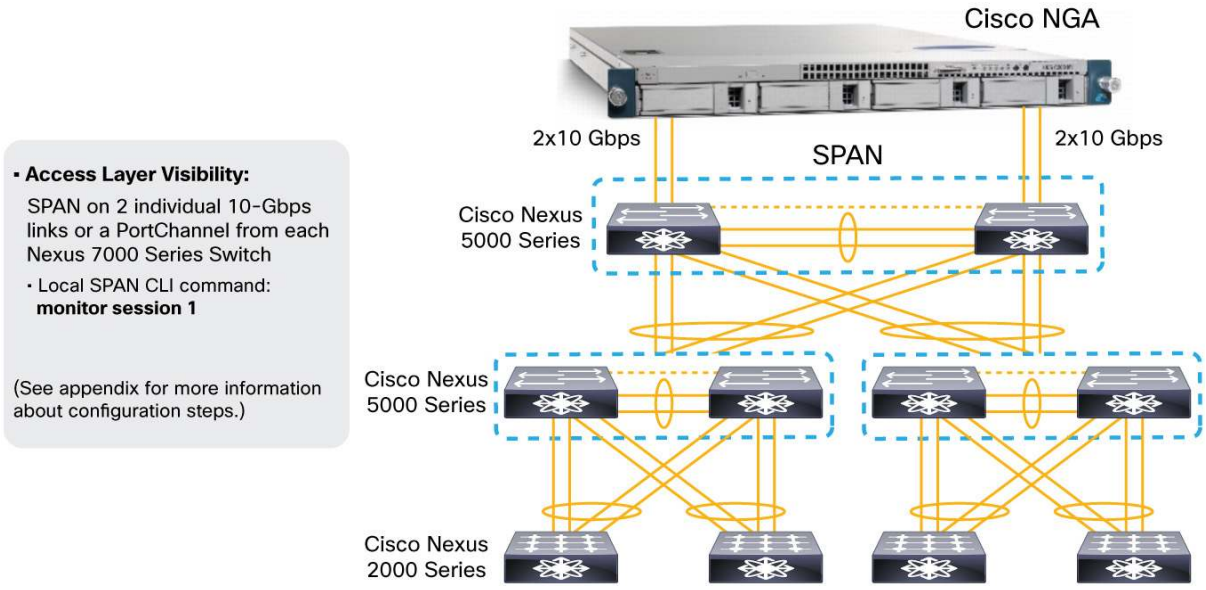
Figure 5. Cisco NGA Deployment in Data Center Using Network Tap



Deployment Scenario 2: Profiling Server Access Network Traffic

With the increasing density of the computing infrastructure (virtual or physical) in modern data centers, workload mobility, and proliferation of VLANs, one of the challenges is characterizing server access network traffic: understanding of what applications are running on the network, who is using them, and how much bandwidth they are consuming; which virtual machines or hosts are placing the most traffic on the network; etc. Cisco NGA can be deployed in the server access layer in conjunction with multiple Cisco Nexus 5000 Series Switches to provide the visibility needed to help ensure optimal use of network resources. Cisco NGA can help profile the traffic behavior by specific applications, virtual machines, hosts, and VLANs (Figure 6).

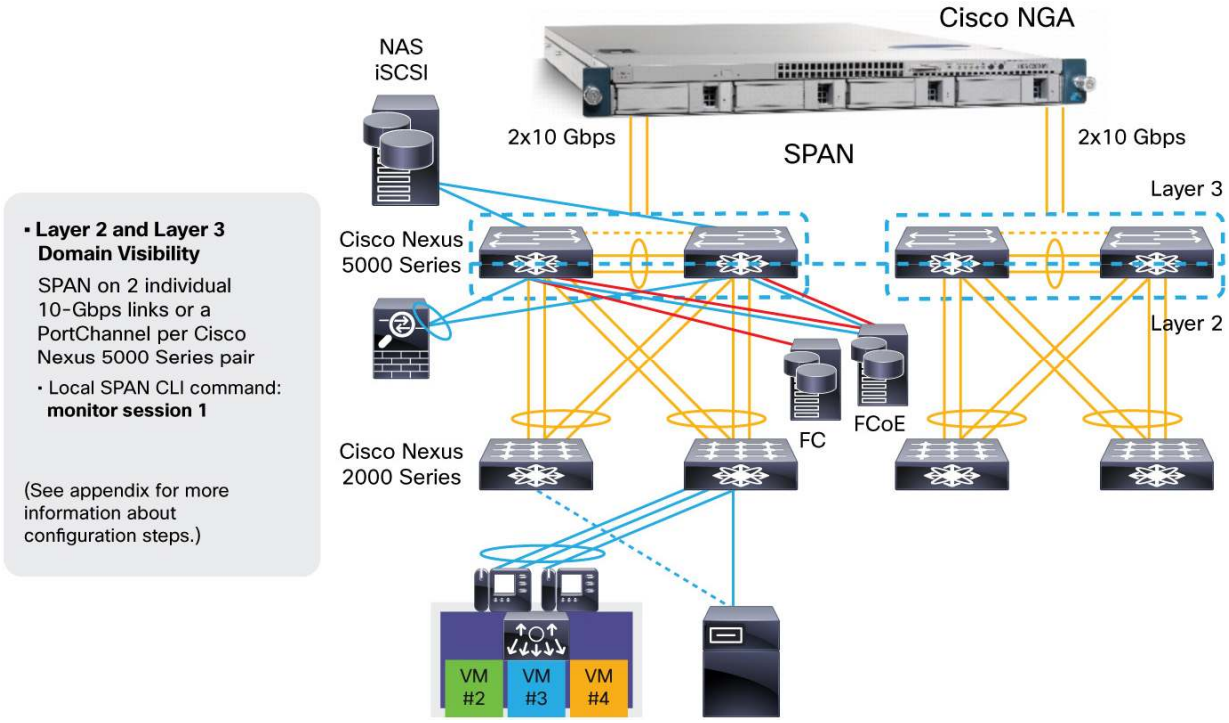
Figure 6. Cisco NGA Deployment to Profile Server Access Network Traffic



Deployment Scenario 3: Visibility Across Virtual Machine, Switching, and Storage Resources in a Small or Medium-Sized Business Data Center

In a small or medium-sized business (SMB) data center, you can use the cross-device flow visibility from Cisco NGA to gain visibility across the entire Layer 2 and Layer 3 domains. Network and security administrators can trace the flow hop by hop from the server to the access switch to the storage, or follow the flow across network services. The visibility supports multiple use cases such as traffic utilization and capacity planning for IP storage, characterization of the effect of workload mobility on network traffic, and troubleshooting of performance problems in the server access layer (Figure 7).

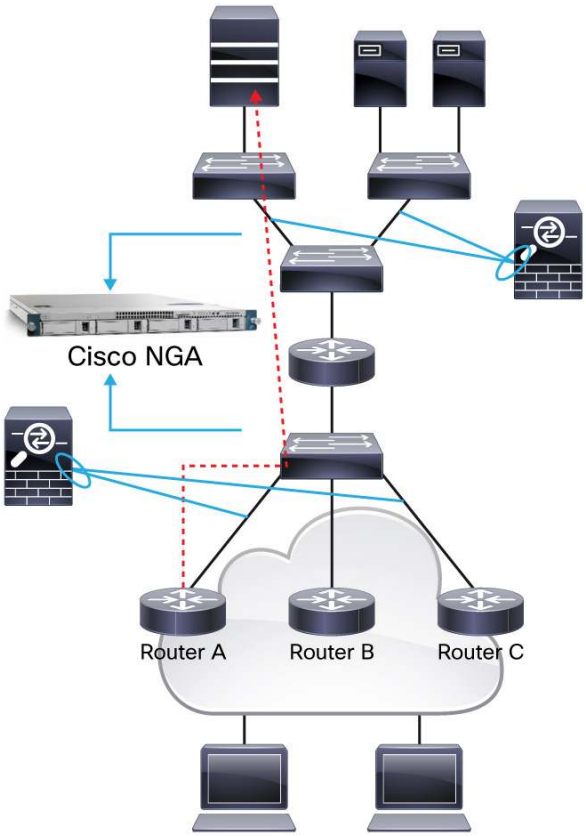
Figure 7. Cisco NGA Deployment in SMB Data Center



Deployment Scenario 4: Validate Firewall Policy

Applying the cross-device approach to flow visibility, Cisco NGA can also be used to gain flow visibility before and after use of network services such as firewalls (Figure 8). In use cases for troubleshooting application performance, a common step is to validate whether the firewall is dropping specific flows and affecting service availability. Similarly, the network policies enforced on the firewall can be verified by observing the traffic behavior using Cisco NGA for visibility.

Figure 8. Cisco NGA Deployment to Validate Firewall Policy



Reporting and Management

The Cisco Prime solution for enterprises is an innovative strategy and portfolio of management products that empower IT departments to more effectively manage their networks and the services they deliver. The Cisco Prime solution is built on a network services management foundation and a set of common attributes. It delivers an intuitive workflow-oriented user experience across Cisco architectures, technologies, and networks. The Cisco Prime solution simplifies network management, improves operation efficiency, reduces errors, and makes the delivery of network services more predictable.

Cisco NGA supports standard NetFlow (NetFlow Versions 5 and 9 and IPFIX) exports. Any NetFlow collector supporting these formats can be used to view NetFlow data exported by Cisco NGA.

Integrated Management Solution with Cisco Prime Assurance Manager

Cisco Prime Assurance Manager is part of the Cisco Prime family of products and provides a centralized service assurance management interface. Cisco Prime Assurance Manager uses the Cisco Prime Network Analysis Module (NAM) and embedded instrumentation available in a Cisco network, such as, NetFlow and NBAR, medianet, Simple Network Management Protocol (SNMP), and performance agents, to provide end-to-end operation visibility from the data center to the branch office (Figure 8). It offers customizable prepackaged dashboards for NetFlow analysis. Cisco NGA can be deployed as a source of flow information for a Cisco Prime Assurance Manager deployment (Figure 9).

Figure 9. Integrated Management with Cisco Prime Assurance Manager

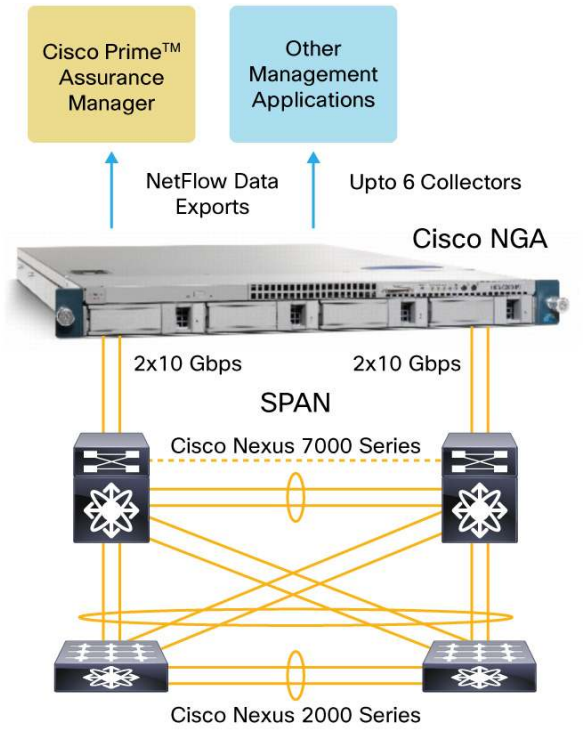
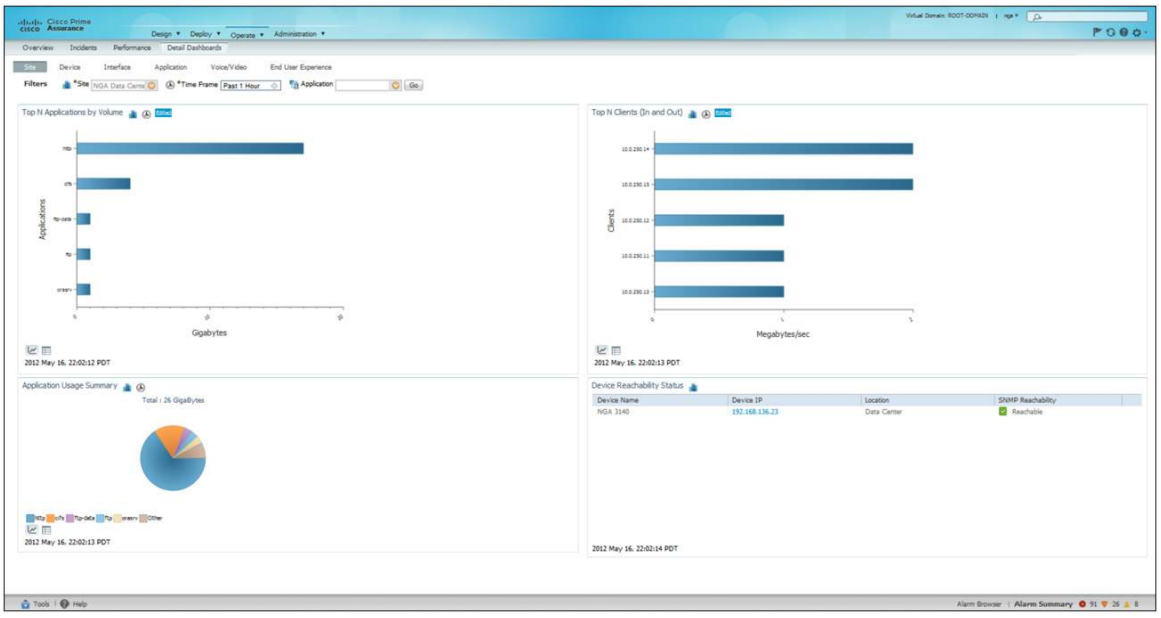


Figure 10. Cisco Prime Assurance Manager Site Monitoring Dashboard



Conclusion

Cisco NGA redefines network visibility and establishes a new standard for a high-performance, cost-effective solution for flow visibility. The product introduces a cross-device approach to flow visibility, facilitating hop-by-hop analysis of flows across multiple network segments. Cisco NGA delivers 100 percent accuracy with no impact on network device forwarding performance. As a result, it enables a broad set of use cases: for security, forensics, billing, troubleshooting, capacity planning, and more.

Cisco NGA empowers network and security administrators with actionable insight for resource optimization, traffic accounting, troubleshooting, and security reinforcement. Cisco NGA supports standard NetFlow formats for export flow information, helping ensure interoperability with existing NetFlow reporting solutions. Used in combination with Cisco Prime Assurance Manager, it offers an integrated traffic monitoring solution for the data center.

For More Information

Please visit http://www.cisco.com/go/nga.

Appendix

Steps to Configure Aggregation and Access Layer Visibility

Step 1. Configure ERSPAN on Cisco Nexus 5000 Series Switch and destination pointed to Cisco Nexus 7000 Series Switch.

- Command reference

Step 2. Configure ERSPAN termination on Cisco Nexus 7000 Series Switch.

- Command reference

Step 3. Configure SPAN on Cisco Nexus 7000 Series Switch and point it to Cisco NGA.

- Command reference

Step 4. (Cisco Nexus 7000 Series only): Configure RSPAN from the source switch to the destination.

- Command reference

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-708294-00 06/12