Application Intelligence and Integrated Security Using Cisco Catalyst 6500 Supervisor Engine 32 PISA

Overview

The Cisco® Catalyst® 6500 Series Supervisor Engine 32 Programmable Intelligent Services Accelerator (PISA) is the next generation supervisor engine for the Cisco Catalyst 6500 Series of modular switches, delivering industry-leading deep packet inspection, application awareness, security, availability, and manageability services for the networks of small and medium-sized businesses, enterprises, and service providers. This whitepaper outlines the benefits of implementing Application Intelligence and Integrated Security using Supervisor Engine 32 PISA and highlights the steps required to implement this solution.

Over the past five years, the proliferation of peer-to-peer (P2P) and instant messaging traffic has had a profound effect on networks and is continuously increasing bandwidth requirements. The resulting effect on operations is significant. This traffic not only compromises the experience of the majority of the users, but affects the quality of new services as well, especially services that are sensitive to the effects of latency, congestion, and jitter—voice and video. This traffic, along with other noncritical applications, can overwhelm the network and jeopardize delivery of critical application traffic. Clearly, an innovative solution for controlling traffic is required—one that is capable of deep packet inspection to identify such applications and take appropriate action to help ensure application fluency.

Additionally, malicious attacks against networking environments are increasing in frequency and sophistication. To counter these attacks, functionality is needed that is flexible in terms of both classification and mitigation capabilities. Many of the tools available today were not designed with deep packet inspection as a requirement; instead, they were designed to provide matching for predefined fields in well-known protocol headers. If an attack uses a field outside the limited range of inspection of these features, one is left without a defense against the attack.

By integrating Supervisor Engine 32 PISA into the network infrastructure, enterprises and service providers can unobtrusively control P2P and instant messaging traffic and protect their network against increasingly sophisticated malicious attacks.

Secure Application Intelligence and Integrated Security: PISA Advantage

Application Intelligence and Integrated Security is delivered using the Cisco Catalyst 6500 Supervisor Engine 32 PISA platform, which provides deep packet inspection and services acceleration at multigigabit speeds. This platform enables enterprises and service providers to identify and control application traffic, apply quality-of-service (QoS) parameters to differing application traffic streams, and provide protection against malicious attacks. The platform is based on an adaptable, programmable architecture that allows the solution to grow with the dynamic needs of the enterprise or service provider. As new techniques for network intrusion or application compromise are created, the programmable nature of the Cisco Catalyst 6500 Supervisor Engine 32 platform helps ensure that the network administrator has the ability to quickly react to the changing environment. The enterprise's or service provider's investment is always protected.

Solution Components

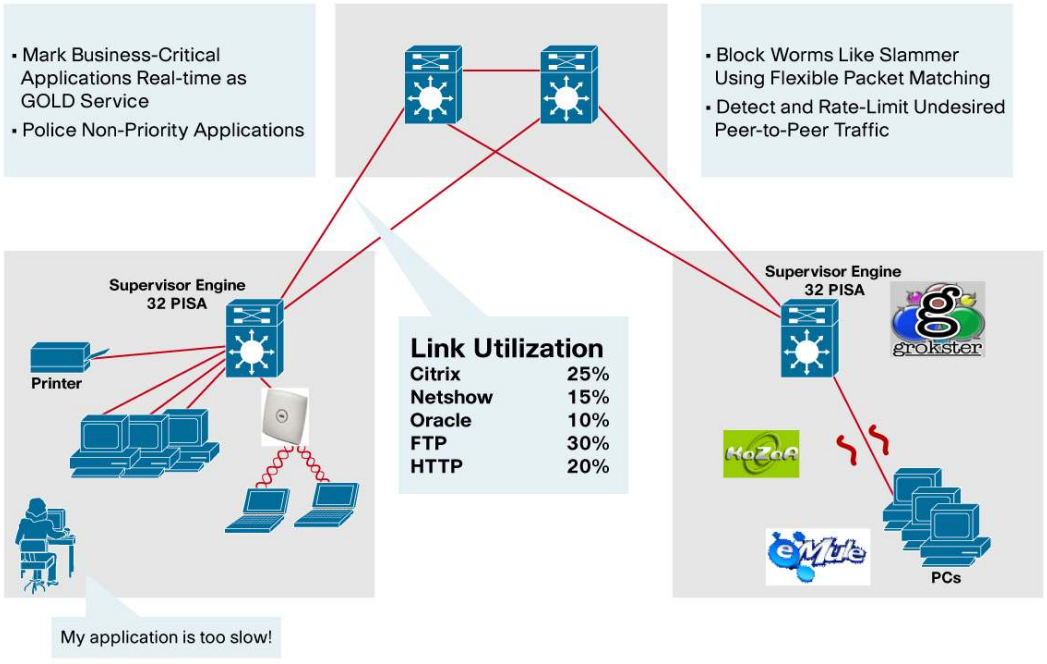
Application Intelligence and Integrated Security solution on the Cisco Catalyst 6500 Supervisor Engine 32 PISA could include some or all of the following components:

- The Cisco Catalyst 6500 Supervisor Engine 32 PISA, available in eight Gigabit Ethernet uplink or two 10 Gigabit Ethernet uplink options along with the associated set of Cisco Catalyst 6500 Ethernet and WAN interfaces
- Cisco IOS® Software Release 12.2(18)ZY–based Internet operating system for Cisco Catalyst 6500 Supervisor Engine 32 PISA supporting Network-Based Application Recognition (NBAR) and Flexible Packet Matching (FPM) services
- Firewall Services Module (FWSM), Intrusion Detection Services Module (IDMS2), IPsec shared port adapter SPA for comprehensive security
- QoS Policy Manager (QPM) for provisioning and monitoring NBAR
- Flexible configuration option in the Cisco Security Manager (CSM) to push configuration files containing FPM policies to Supervisor Engine 32 PISA based switches
- Integration services, performed by either the Cisco Advanced Services team or a systems integration partner

Solution Deployment Scenarios

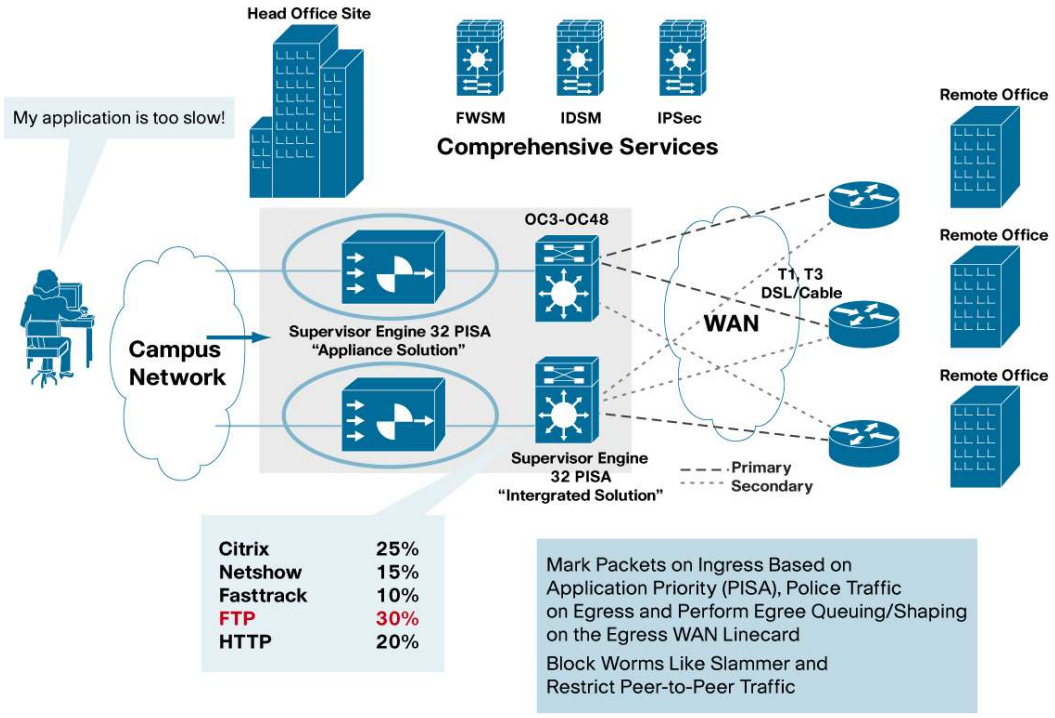
The solution can be deployed at the campus access, allowing customers to move security and classification to the edge of the network (Figure 1).

Figure 1. Supervisor Engine 32 PISA Deployment Example in LAN Access



Alternatively, the solution can be deployed at the Enterprise WAN aggregation utilizing the comprehensive support of services modules and WAN interfaces on the Cisco Catalyst 6500 platform (Figure 2).

Figure 2. Supervisor Engine 32 PISA Deployment Example in WAN Aggregation

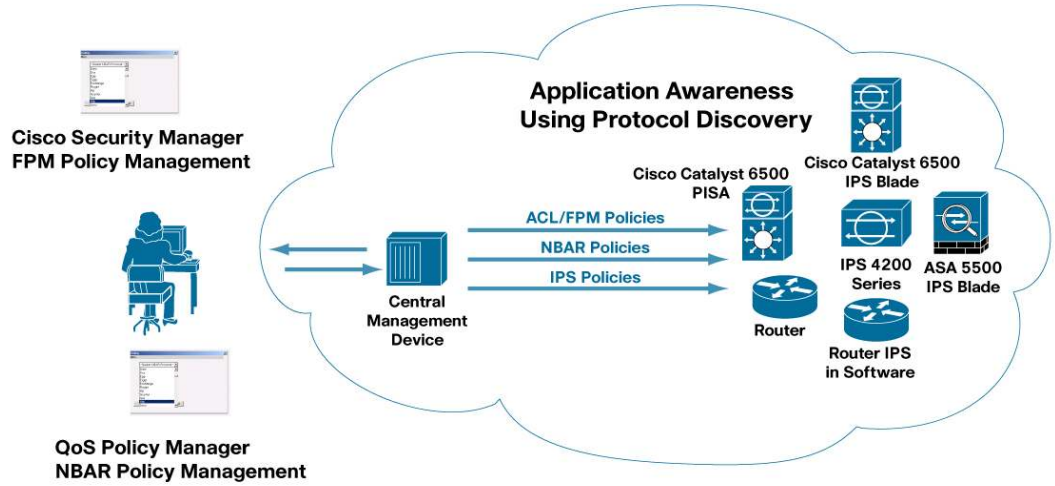


Solution Management

The solution comes with support for graphical user interface (GUI)–based QoS Policy Manager (QPM), which centralizes and automates NBAR policy management. Moreover, QPM dramatically increases the speed and accuracy of defining, validating, configuring, and deploying NBAR policies.

In addition, flexible Configuration option in the Cisco Security Manager (CSM) allows network administrators to push down configuration files containing FPM policies to multiples switches. (See Figure 3.)

Figure 3. Supervisor Engine 32 PISA Management Model



Benefits and Applications

Help Ensure Performance for Mission-Critical Applications

Mission-critical applications, such as Oracle, Citrix, Microsoft Exchange, or the new breed of Web-based applications, must perform well to help ensure your success in today's fast-paced e-business environment. Bottlenecks can occur in many places, including the network. These bottlenecks often occur even though you have budgeted what you thought was more than adequate bandwidth for each application.

What often happens is that employees use new Internet applications, such as streaming audio and video or downloading of new programs. These applications can quickly consume your WAN bandwidth. Unfortunately, these are not typically the mission-critical applications to which you want to give network priority.

By intelligently classifying applications, Cisco Catalyst 6500 Supervisor Engine 32 PISA allows the network to provide differentiated services to each application. You can provide absolute priority and a guaranteed amount of bandwidth to your mission-critical applications, such as Citrix or an application that runs on a particular Webpage. At the same time, you can limit the bandwidth consumed by less critical applications. The end result is that users can access their mission-critical applications with minimal delay without the need to upgrade costly WAN links or cut off access to commonly used, but not mission-critical, applications.

Provide Rapid Protection against Malicious Attacks

Malicious attacks against networks are increasing in frequency and sophistication. To counter these attacks, tools are needed that are as flexible as possible and that can provide packet inspection capabilities at different levels. Many of the tools available today do not allow deep packet inspection. These tools are constrained to specific fields in well-known protocol headers. If an attack uses a field outside the limited range of inspection provided by these tools, it is difficult to classify and defend against the attack.

Cisco Catalyst 6500 Supervisor Engine 32 PISA provides network and security administrators with powerful tools to filter traffic as it enters the network and to immediately drop questionable items and/or keep a log for auditing purposes. Cisco Catalyst 6500 Supervisor Engine 32 PISA allows network and security administrators to specify custom patterns on which to match, deep within the packet header or payload. The functionality introduces the concept of protocol header definition files (PHDFs), which give names to offset locations within a packet, thereby enhancing usability and flexibility. Ready-made definitions for standard protocols are included using PHDF, making it easy to deploy immediately at run time. High-level custom scripting for PHDFs is supported by standard Extensible Markup Language (XML) editors.

Improve Web Response

The Web is now a critical business resource in many enterprises, for both internal and external communications. Employees, partners, and customers must have access to the Webpages they need without such problems as slow downloads or Web-based application failure.

Cisco Catalyst 6500 Supervisor Engine 32 PISA allows you to identify the Webpages and type of Web content that you deem critical. For example:

- Customers accessing the sales ordering page would be given priority. This prevents the customer from getting frustrated at the point of sale.
- Sales tools can be given absolute priority and guaranteed bandwidth, helping ensure that your sales force is never forced to wait for a price quote because another employee is browsing the latest version of the firm's new television commercial on streaming video.

- Web-based applications often load slowly. With Cisco Catalyst 6500 Supervisor Engine 32 PISA, applications can be identified by MIME type and be given priority in the network.
- Some classes of content, such as JPEG pictures, consume large amounts of bandwidth, but might not be considered critical Web-based information. In such cases, you can control the amount of bandwidth consumed by such types of content.

Improve Multiservice Performance

Multiservice networks allow you to combine your data, voice, and video requirements into one unified network. Unfortunately, each of these services requires different network characteristics. Supervisor Engine 32 PISA is able to intelligently identify the type of each packet and provide the proper network characteristics.

For example, if you deploy a training system that utilizes streaming video, such as the Cisco IP/TV® solution, you will want to try to ensure that employees see a clean picture, not one that is choppy and hard to understand. With Cisco Catalyst 6500 Supervisor Engine 32 PISA, the network can easily recognize the streaming video traffic and assign it to a higher priority class of traffic that receives a minimum guaranteed bandwidth. Other traffic, such as e-mail, can be assigned to a lower priority class, because e-mail must be delivered, but it does not have the latency and bandwidth constraints of the streaming video. The end results are that trainees receive their video training on demand with high quality while the network concurrently serves other applications.

Reduce WAN Expenses

The cost of WAN bandwidth has decreased significantly over the last decade, especially in deregulated markets. However, in many parts of the world, and especially between countries, telecommunications links can still be prohibitively expensive. This leads to a dilemma for the network manager: you need to provide access to new client-server and Internet-enabled applications, while also controlling WAN service costs. Cisco Catalyst 6500 Supervisor Engine 32 PISA provides a solution to this problem by enabling you to intelligently utilize WAN bandwidth so that you can provide acceptable service levels with the minimum possible bandwidth.

Cisco Catalyst 6500 Supervisor Engine 32 PISA will identify your mission-critical applications so that you can assign them higher priority or guaranteed bandwidth on the link. This helps ensure that the noncritical applications do not overwhelm these slower international links and bring your mission-critical traffic to a halt.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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 C22-384941-00 04/07

