



Cortina Systems® CS1331 Octal-48/12/3 Framer/GE MAC Network For Security Applications

With the significant increase in number and severity of viruses, worms, and other types of malware, users and network administrators must be more vigilant than ever about intrusion detection, spam, and network monitoring. Network monitoring equipment is required to constantly monitor a computer network to identify malicious content.

Network monitoring is a task of increasing importance. On the corporate side, the greater numbers of telecommuting and traveling employees generate increased mobile device usage requiring better protection against the loss of sensitive corporate and user data. Data that is coming into the organization is an equal concern. Network monitoring applications allow businesses to understand the traffic flow of information into the company's network – traffic that may include malware, non-work related reading items (news, sports), recreational video or audio streaming, or pornography. Controlling employee access to these outside sources through employee education and network monitoring is an important component of corporate network security.

Governments also make use of network monitoring equipment to protect government computer systems from hackers and foreign governments attempting to steal sensitive information. Law enforcement agencies use network monitoring in fighting organized crime. Some governments also use network monitoring to snoop on unwanted activities of their citizens.

There are significant technological challenges in network security due to the exponential growth in network bandwidth. Static network security technologies such as MIPS chips or standardized CPUs do not keep up with modern network speeds so specialized high-bandwidth processing equipment is required. To reduce deployment costs, the processing equipment should provide a seamless connection to high-throughput fiber networks and interoperate with common data communication protocols such as Ethernet and SONET/SDH.

The network monitoring algorithm performs functions such as deep packet inspection – a form of filtering that examines the data (can be any form of content including text, video, or even VoIP) for pre-defined criteria such as viruses or malware, spam, or some content of interest.

The challenge to vendors is to provide an interface that supports both corporate and government requirements including the underlying electronics that support a variety of algorithms and high bandwidth network performance demands.

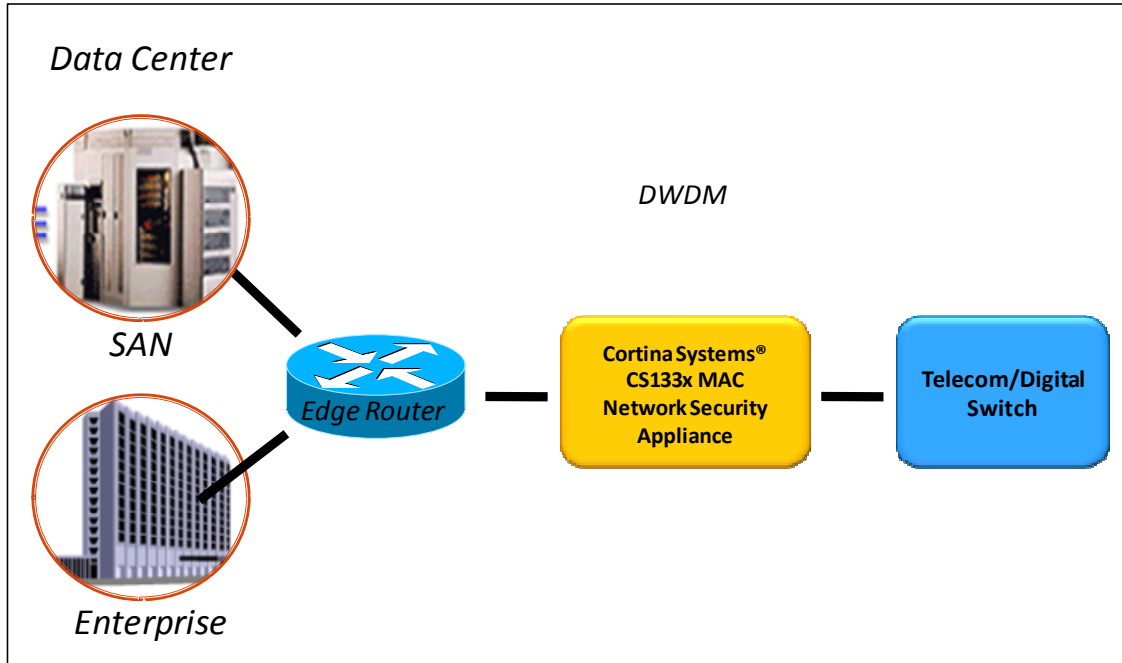
Existing Applications

Existing applications perform a variety of functions including: Denial of Service (DoS) prevention, traffic flow monitoring, network forensics, snooping, compliance and governance, and firewalls.

A DoS attack is typically an attempt to prevent an Internet site or service from functioning. These types of attacks are commonly targeted at banks and other financial institutions. As such, the majority of corporations and institutions utilizing security appliances are paying for DoS prevention that is not required. Similarly, network forensic tools and government compliance features often go unused. Network forensic tools are traffic recording and analysis engines acting like security cameras requiring hardware and software to capture and manage significant quantities of data. With the raw data, investigators can perform analyses of historical events. Government compliance features help firms meet governmental data security regulations.

A stand-alone device is required to perform such extensive security features. As shown in Figure 1, this device typically exists between a router and a digital switch.

Figure 1 Network Security Appliance in Use



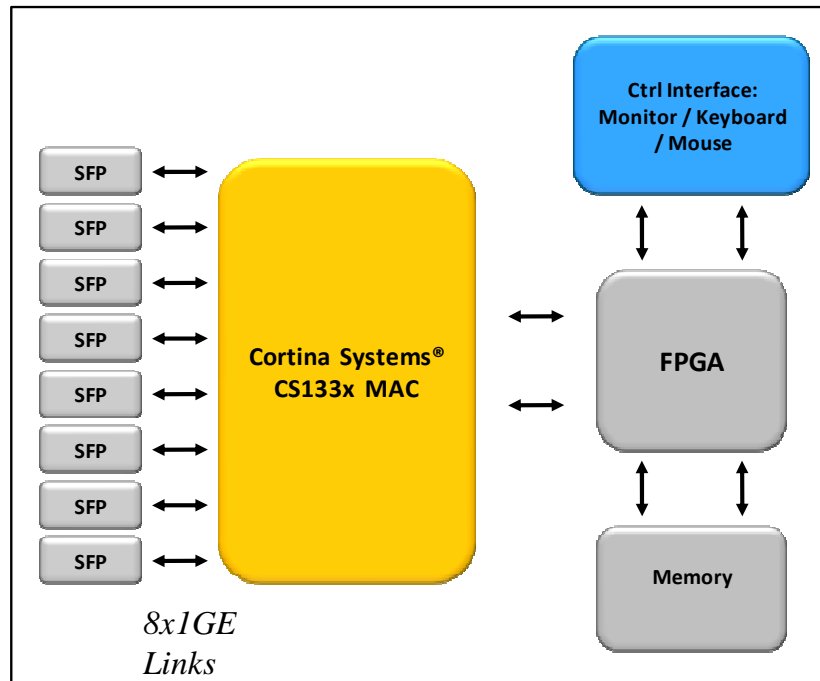
Reducing Costs by Limiting the Feature Set

A typical security appliance performs a variety of functions including network monitoring, DoS protection, traffic flow monitoring, and firewalling. Such functional and performance demands require the appliance to reside in the WAN and not the router (DoS prevention appliances for example cannot operate in the router). The result is a device that, like typical software applications, supports many more features than is required by the average customer. By limiting the feature-set to network monitoring only, the security appliance can be a much simpler linecard co-existing with other router cards.

An application with a limited feature-set would consist of a human interface to a network monitoring device, network monitoring software, and supporting hardware and electronics. The interface and network monitoring algorithm will likely be proprietary or application specific, coming in the form of field programmable hardware with supporting firmware and application software. The supporting electronics are required in order to access and format data for handoff to the monitoring processor. Such supporting electronics would connect to common industry standard protocols such as Ethernet and SONET/SDH. The desired device would be low cost, capable of supporting multiple protocols, and have a low power requirement to not impact router design.

The Cortina Systems® CS133x Octal-48/12/3 Framer/GE MAC shown in Figure 2 is a cost-effective hardware solution for network security. The CS1331 MAC is a multi-rate, multi-service device which provides a seamless connection to SFP optics and supports connections to industry standard protocols including Ethernet and SONET/SDH. The device provides up to 8 channels of Gigabit Ethernet in one low cost device, and can be upgraded to provide OEM vendors with the capability to monitor SDH/SONET traffic directly. With both capabilities, the device can support vendors that build multi-BOM options in an effort to support a variety of interfaces. The device comes in a low power package and as such, is suitable for this router based application.

Figure 2 Network Monitoring Card



Conclusion

The Cortina Systems® CS133x Framer/MAC offers a highly cost-effective and flexible network security solution for most corporate and commercial applications.

References

- Trends in Network Security; November 2007; http://www.pcworld.com/businesscenter/article/139648/trends_in_network_security.html
- Chinese Snooping on Skype Raises Question about Chat Network's Security; Friday October 3, 2008; Associated Press – <http://www.foxnews.com/story/0,2933,432043,00.html>
- <http://us.trendmicro.com/us/solutions/enterprise/security-solutions/threat-management/security-challenges/index.html>
- Open Web Application Security Project – www.owasp.org



About Cortina Systems

Through continuous innovations in advanced port processing and intelligent port connectivity, Cortina Systems, Inc is a leading supplier of intelligent communication solutions for the Core, Metro, Access, and Enterprise network market segments. Cortina delivers a wide suite of products that address customers' performance, density, and flexibility needs with state-of-the-art, high-speed, analog-digital integration technology. Cortina solutions enable faster time-to-market, longer time-in-market, and increased revenue opportunities. Working closely with customers to understand their system requirements and anticipate their needs, Cortina is creating the foundation for new generations of services. For more information, please visit

www.cortina-systems.com.

Cortina Systems, Inc. Confidential

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH CORTINA SYSTEMS® PRODUCTS.

NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT.

EXCEPT AS PROVIDED IN CORTINA'S TERMS AND CONDITIONS OF SALE OF SUCH PRODUCTS, CORTINA ASSUMES NO LIABILITY WHATSOEVER, AND CORTINA DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY RELATING TO THE SALE AND/OR USE OF CORTINA PRODUCTS, INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Cortina products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

CORTINA SYSTEMS®, CORTINA™, and the Cortina Earth Logo are trademarks or registered trademarks of Cortina Systems, Inc. or its subsidiaries in the US and other countries. Any other product and company names are the trademarks of their respective owners.

Copyright © 2009 Cortina Systems, Inc. All rights reserved