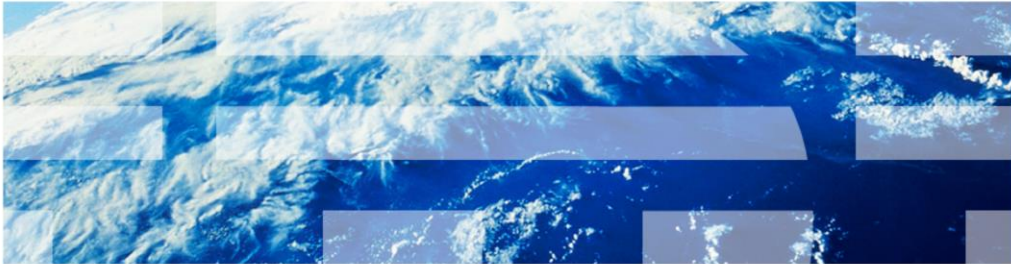


# IBM Security Network Intrusion Prevention System

## GX7800 appliance overview



© 2011 IBM Corporation

IBM Security Network Intrusion Prevention System: GX7800 appliance overview

## Objectives

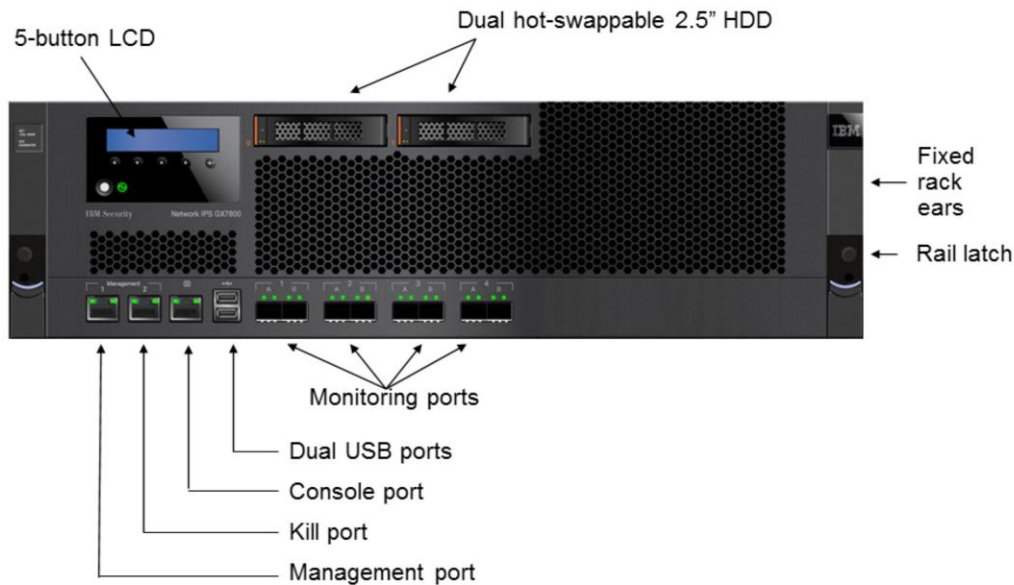
When you complete this module, you should be able to:

- Connect GX7800 ports to a network
- List GX7800 appliance features

When you complete this module, you should be able to:

- Connect GX7800 ports to a network and
- List GX7800 appliance features

## GX7800 front panel



3

GX7800 appliance overview

© 2011 IBM Corporation

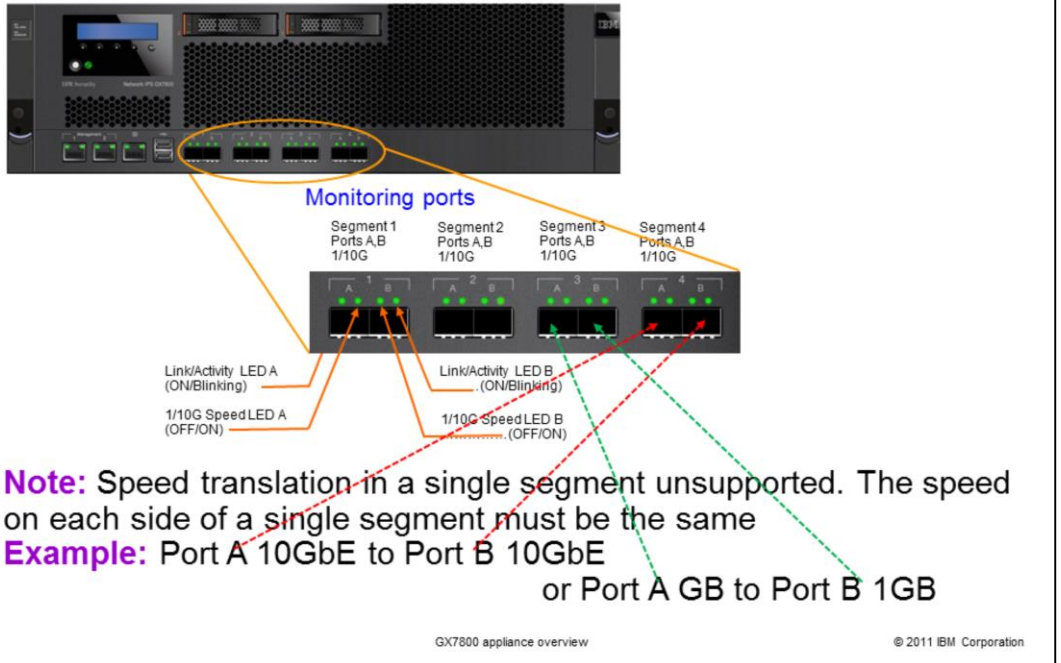
In this diagram, you see the front panel of the GX7800 appliance. You can use the 5-button LCD for initial network configuration, for restarting or shutting down the appliance, and for obtaining IPS version information. You can also use it to view the serial number of the appliance.

There are two hot swappable drives built into the appliance. The fixed rack ears and rail latch are new to this model. These improvements have reduced the amount of time it takes to install the GX7800 appliance on your network.

Several ports are available. The management port is used for communicating with the appliance local management interface (LMI) and the SiteProtector Console. The kill port is used exclusively to send TCP reset responses. The console port is for terminal-based setup and recovery. The dual USB ports are for retrieving data and installing firmware.

There are eight monitoring ports divided into four segments. Each segment can support 10 Gb Ethernet or 1 Gb Ethernet connections.

## GX7800 ports and segments



Speed translation within a segment is not supported. As you can see from the example on the slide, the ports within a segment must be set at the same speed. You cannot have a 10 Gb router plugged into port A and a 1 Gb switch plugged into the paired port B.

## GX7800 port flexibility



- 8 ports (4 segments)
- 10G SFP+ (SR, LR)
  - Direct-attach copper
  - 1G SFP (TX, SX, LX)

### 10G SFP+ (SR, LR)



**AVAGO** AFBR-703SDZ-IB2  
 PN: 46N5368 EC: L68187  
 10GB Made in CHINA 1019  
 850nm LASER PROD  
 21CFR(J) CLASS 1



**AVAGO** AFCT-701SDZ-IB2  
 PN: 46N5369 EC: L68187  
 10GB Made in CHINA 1019  
 1300nm LASER PROD  
 21CFR(J) CLASS 1

### 1G SFP (TX, SX, LX)



**AVAGO** AFBR-5715PZ-IB  
 PN: 51J1701 EC: L68039  
 1GB 850nm LASER PROD  
 21CFR(J) CLASS 1  
 MALAYSIA YYWW  
 WAFER#



**AVAGO** AFCT-5715PZ-IB  
 PN: 51J1704 EC: L68039  
 1GB 1300nm LASER PROD  
 21CFR(J) CLASS 1  
 CHINA YYWW



**AVAGO** ABCU-5710RZ-IB  
 PN: 51J1697 EC: L68039  
 1GB 1000 BASE-T 1.25GBd  
 MALAYSIA YYWW

### Direct-attach copper



The GX7800 has port flexibility. The small form-factor pluggable (SFP) transceivers that work with the appliance are listed on the slide. The short range (SR) and long range (LR) transceivers support 10 Gb segments.

Three modules support 1 Gb segments. These modules are copper (TX), multi-mode fiber (SX), and single-mode fiber (LX).

The direct-attach copper cable is new. It is a short, 10 Gb copper cable that has SFP+ connectors on each end. You use it when you convert fiber to copper. For example, you might use it connect the appliance and another device that is mounted in the same cabinet.

## GX7800 platform specifications

### Main system

- Dual quad-core Xeon processors
- 24 GB memory
- Redundant, hot-swappable power supplies and fans
- Dual 2.5" 7200 RPM, 160 GB (Raid 1)
- Rack mount installation, no tools required

### Network communications

- Dual NetLogic XLR
- 4 GB memory
- Independent data and control plane interfaces to the host system

### Carrier board

- Multiple configurations
- Broadcom 24-port multilayer switch
- SFP and SFP+
- Copper and fiber SX/SR
- LX/LR cabling
- Direct-attach copper

The GX7800 platform specifications are listed on the slide. Take a few moments to examine them.

## Performance testing results

Performance test	GX7800 results
Inspected throughput	23 Gbps
Average latency	<150 $\mu$ Secs
Connections per second	390,000
Maximum concurrent sessions	12,500,000

GX7800 appliance overview

© 2011 IBM Corporation

During performance testing, the inspected throughput on the GX7800 was 23 Gb. The average latency was less than 150 microseconds. There were 390,000 connections per second, and the appliance reached a maximum of 12.5 million concurrent sessions.

## Protocol Analysis Module 2.0

The Protocol Analysis Module (PAM) includes some new functions:

- Multiple threads, not multiple instances (shared memory)
- Increased throughput by taking advantage of multicore processors
- Introduction of 10 KB inspection depth for increased throughput
- Cross-flow events might fire more or less times
- Packet logging rewritten for ease of configuration and increased performance

In version 2.0, the Protocol Analysis Module (PAM) functionality remains primarily unchanged. The difference is that PAM 2.0 is multithreaded and can inspect six packet streams instead of only one stream. With a multiprocessor system, the threads can run simultaneously; each processor running a particular thread. This function reduces the appliance processing load and increases performance.

In PAM 2.0, you have the option of increasing throughput by only inspecting the first 10,000 bytes of a session. Research has shown that if an attack does not happen in the first 10 KB of a session, that the session has a small chance of being involved in a malicious event.

As a result of multithreaded inspection, multiple identical events detected from cross-flow analysis might be reported as having a different quantity as compared to those same events being detected by a device using single-thread architecture.

In PAM 2.0, packet logging configuration is easier and performance increased



## GX7800 features (1 of 2)

Feature	Description	Firmware
IPv6	Support for management port, protection alerts, and analysis views	4.1 – 4.3
Ready to use	Zero configuration, USB installation, PXE Server, DHCP, NTP, SiteProtector configuration during installation, Radius support	4.1 – 4.3
Blocking from analysis views	Click an event and quarantine the attacker in both the local management interface (LMI) and SiteProtector Console	4.1 – 4.3 SiteProtector 8.1
Health Information	Information about the appliance health is sent to SiteProtector	4.1 – 4.3 SiteProtector 8.0, 8.1
Geographical high availability (HA)	Lower density high availability solution. This architecture securely transfers rules between appliances	4.1 – 4.3
Feature level policies	Framework for supporting higher level policies in place	4.1 – 4.3

GX7800 appliance overview

© 2011 IBM Corporation

The GX7800 supports IPv6, and it takes less time to get the GX7800 appliance installed and running on your network. When using firmware 4.1 and higher or SiteProtector 8.1, you can block events from the local management interface and the SiteProtector Console Analysis view.

Firmware 4.1 and higher supports geographic high availability. In this type of configuration, two GX7800 appliances are physically separated.

## GX7800 features (2 of 2)

Feature	Description	Firmware
AppScan® integration	Integration support through SiteProtector	4.1 – 4.3 SiteProtector 8.0, 8.1
Quarantine DDOS response	Will block traffic from an intruder that is related to a specific attack, which is useful for flood and spoof attacks	4.1 – 4.3
PAM 2.0	Multithreaded Protocol Analysis Module (PAM) supports inspection at higher throughput	4.2
Transactional policies	Batches of policies treated as a single transaction	4.2
Log evidence	Both pcap and sniffer support. Log Connection, Log Interface/All interfaces, Offending/Dropped packet	4.1 – 4.3 Rewritten for 4.2
SNMP V3	Adds security and remote configuration to SNMP responses and traps	4.3

GX7800 appliance overview

© 2011 IBM Corporation

AppScan integration is available through the SiteProtector Console. There is also a distributed denial of service (DDOS) quarantine response.

Note that PAM 2.0 is only available in firmware version 4.2. Transactional policies are also only available in firmware version 4.2.

SiteProtector sends policies to the appliance in batches. If one of the policies fail, you can roll back the entire batch as opposed to having only half the policies applied. This process is somewhat transparent.

Note that the log evidence was rewritten for firmware version 4.2.

SNMP V3 is only available in firmware version 4.3. You can configure SNMP V3 in firmware version 4.2 but it is not functional.

## Summary

Now that you have completed this module, you should be able to:

- Connect GX7800 ports to a network
- List GX7800 appliance features

Now that you have completed this module, you should be able to:

- Connect GX7800 ports to a network and
- List GX7800 appliance features



## Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, and AppScan are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2011. All rights reserved.

© 2011 IBM Corporation