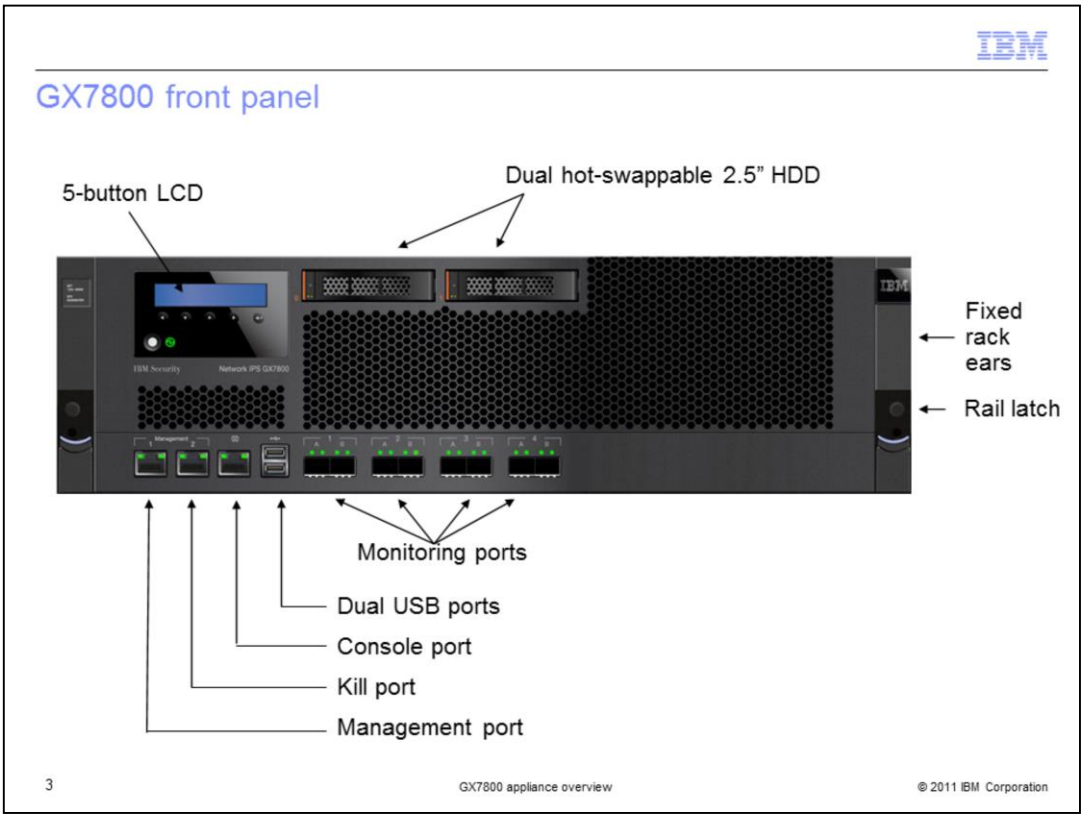
IBM Security Network Intrusion Prevention System: GX7800 appliance overview

When you complete this module, you should be able to:
- Connect GX7800 ports to a network and
- List GX7800 appliance features

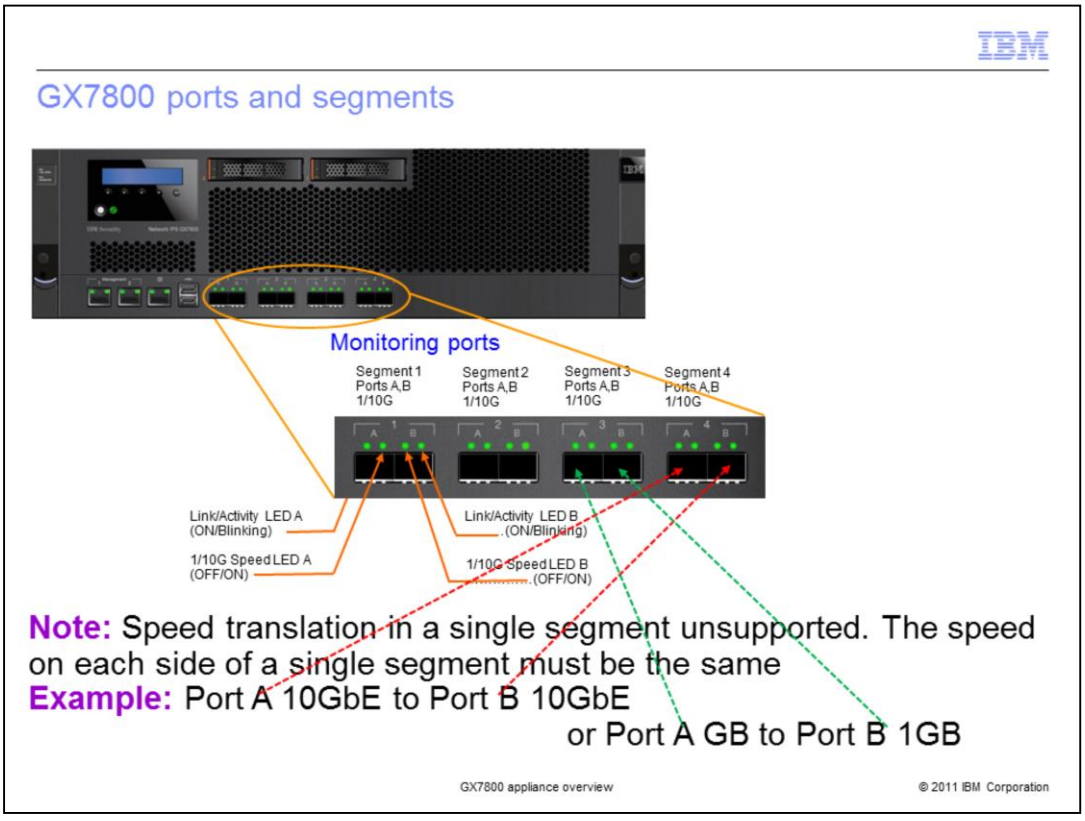


In this diagram, you see the front panel of the GX7800 appliance. You can use the 5-button LCD for initial network configuration, for restarting or shutting down the appliance, and for obtaining IPS version information. You can also use it to view the serial number of the appliance.

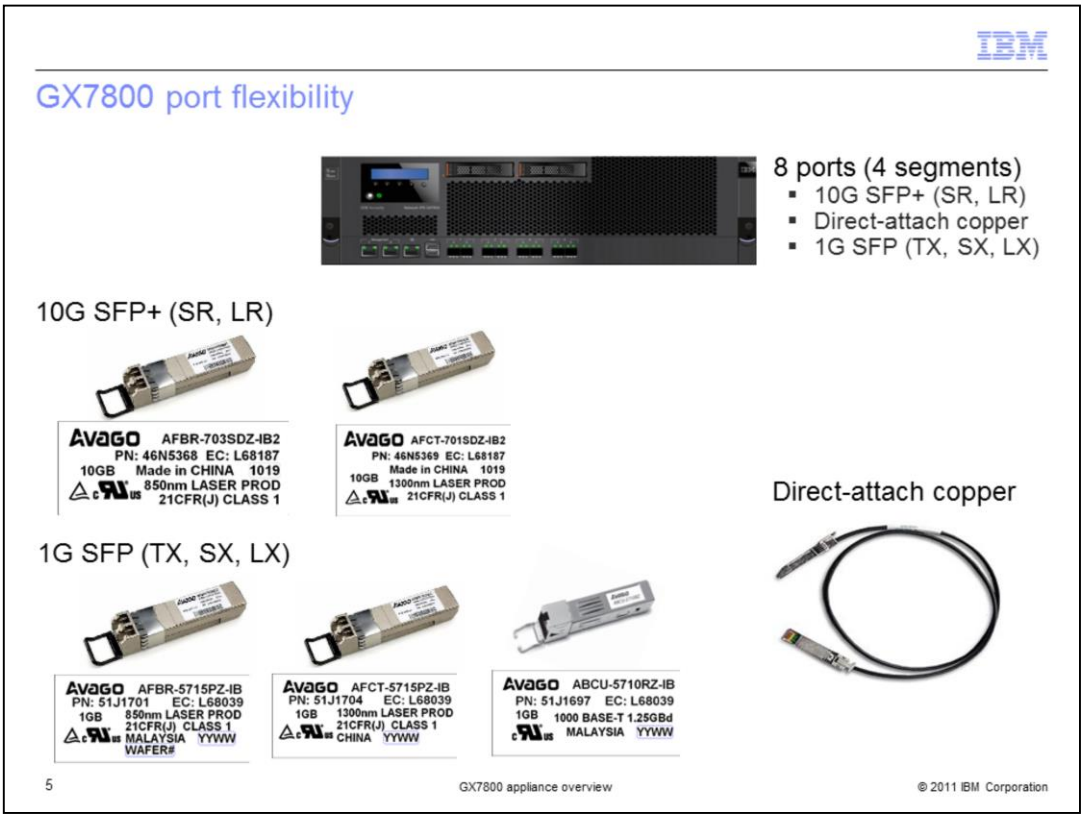
There are two hot swappable drives built into the appliance. The fixed rack ears and rail latch are new to this model. These improvements have reduced the amount of time it takes to install the GX7800 appliance on your network.

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.



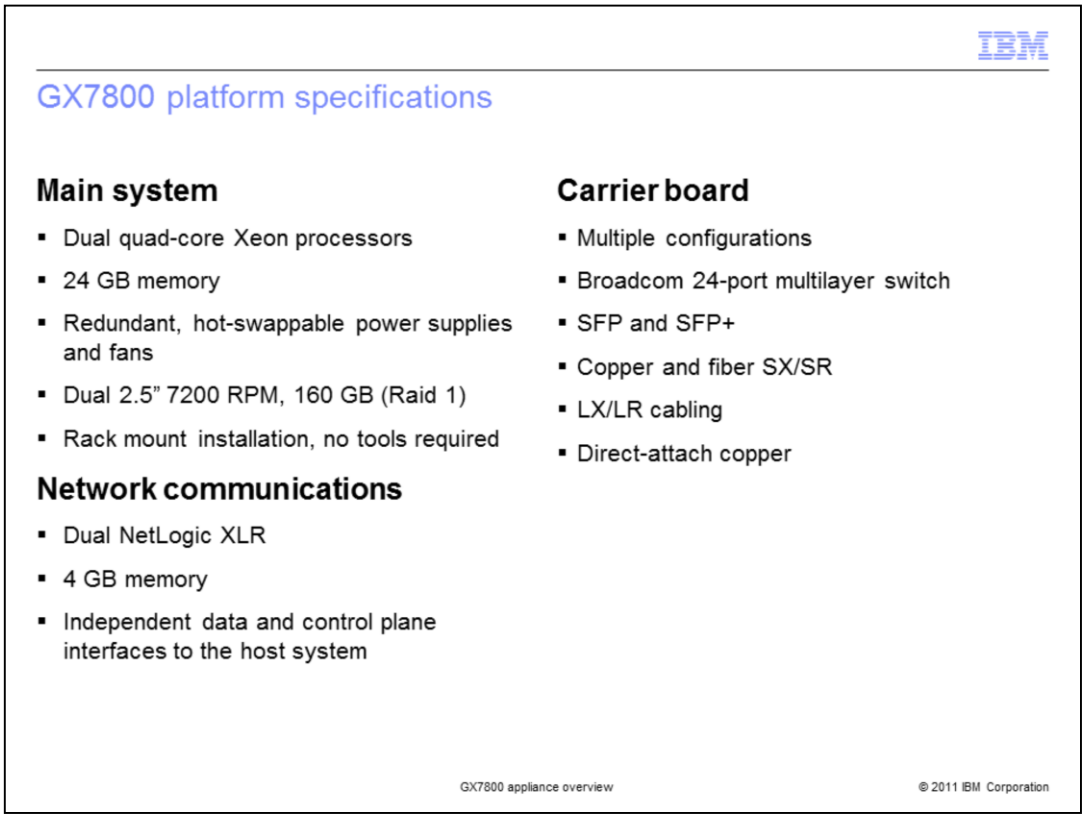
Speed translation within a segment is not supported. As you can see from the example on the slide, the ports within a segment must be set at the same speed. You cannot have a 10 Gb router plugged into port A and a 1 Gb switch plugged into the paired port B.



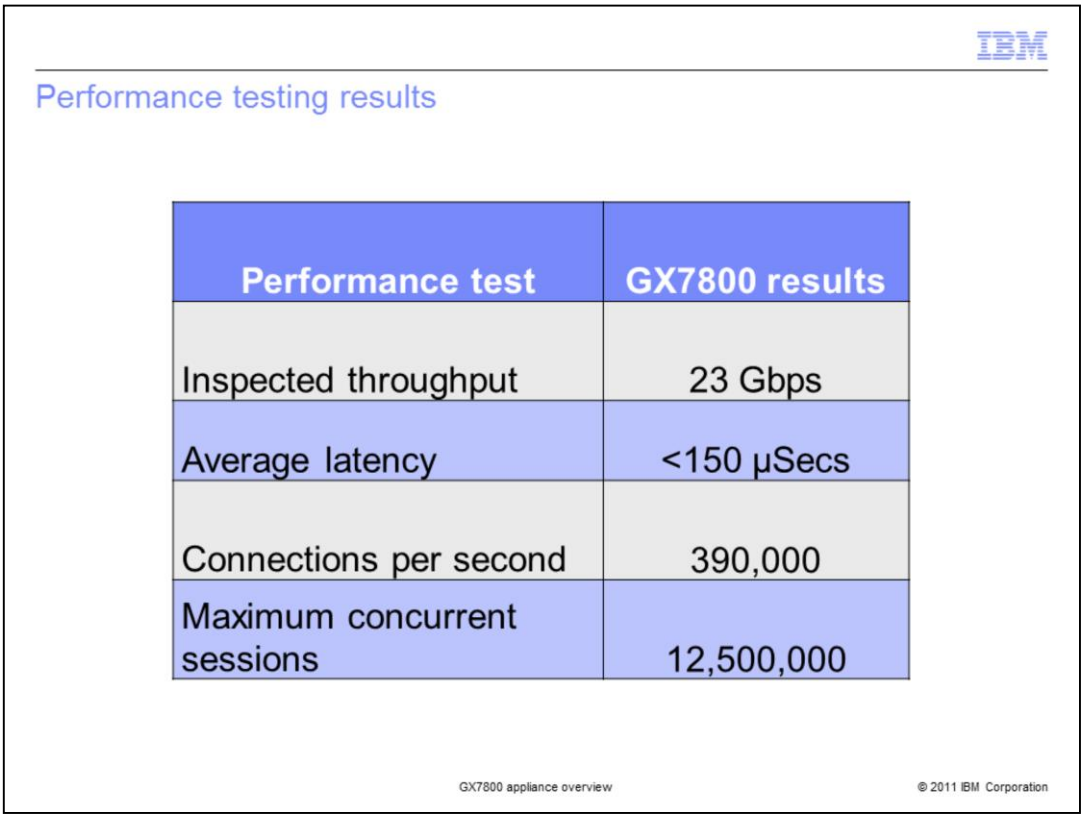
The GX7800 has port flexibility. The small form-factor pluggable (SFP) transceivers that work with the appliance are listed on the slide. The short range (SR) and long range (LR) transceivers support 10 Gb segments.

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

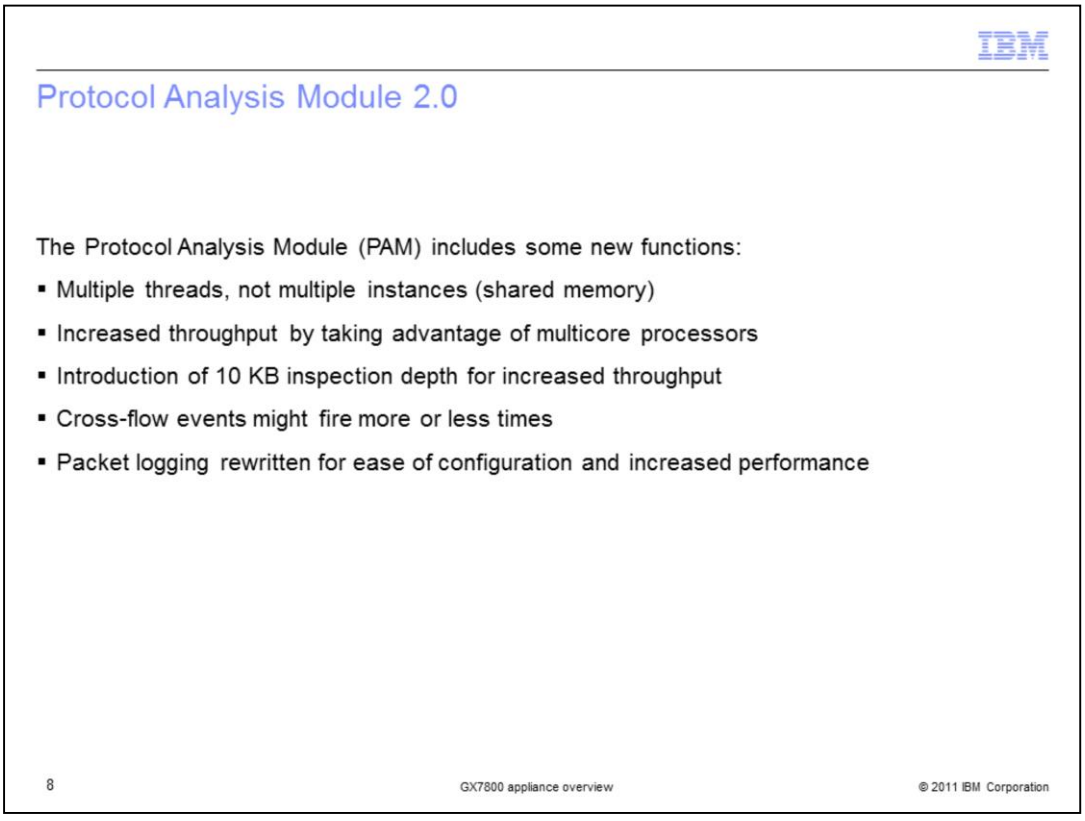
The direct-attach copper cable is new. It is a short, 10 Gb copper cable that has SFP+ connectors on each end. You use it when you convert fiber to copper. For example, you might use it connect the appliance and another device that is mounted in the same cabinet.



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



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.

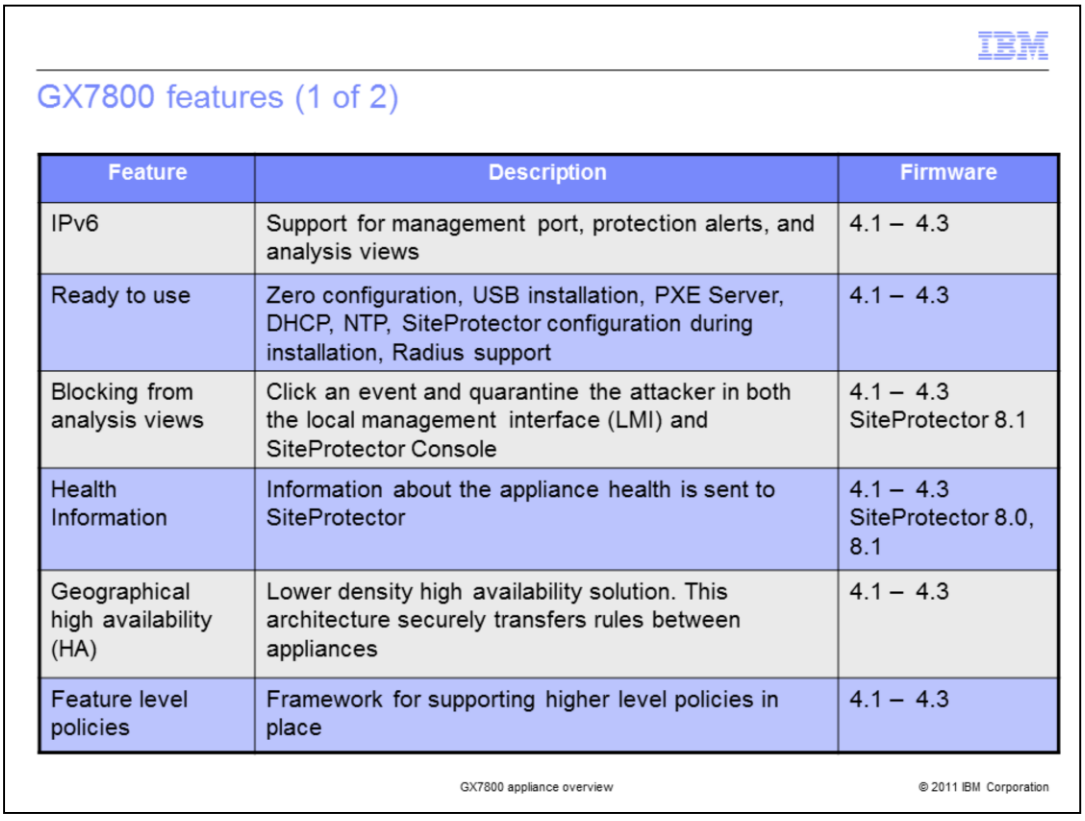


In version 2.0, the Protocol Analysis Module (PAM) functionality remains primarily unchanged. The difference is that PAM 2.0 is multithreaded and can inspect six packet streams instead of only one stream. With a multiprocessor system, the threads can run simultaneously; each processor running a particular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

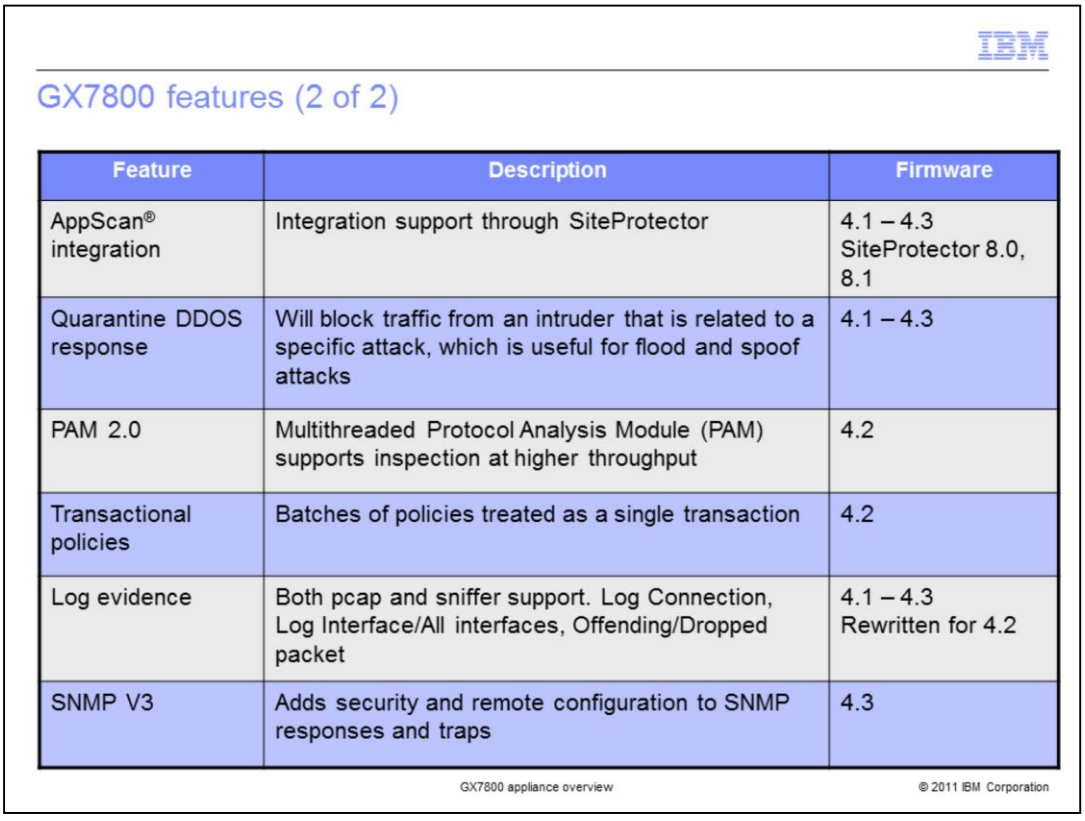
As a result of multithreaded inspection, multiple identical events detected from cross-flow analysis might be reported as having a different quantity as compared to those same events being detected by a device using single-thread architecture.

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



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.



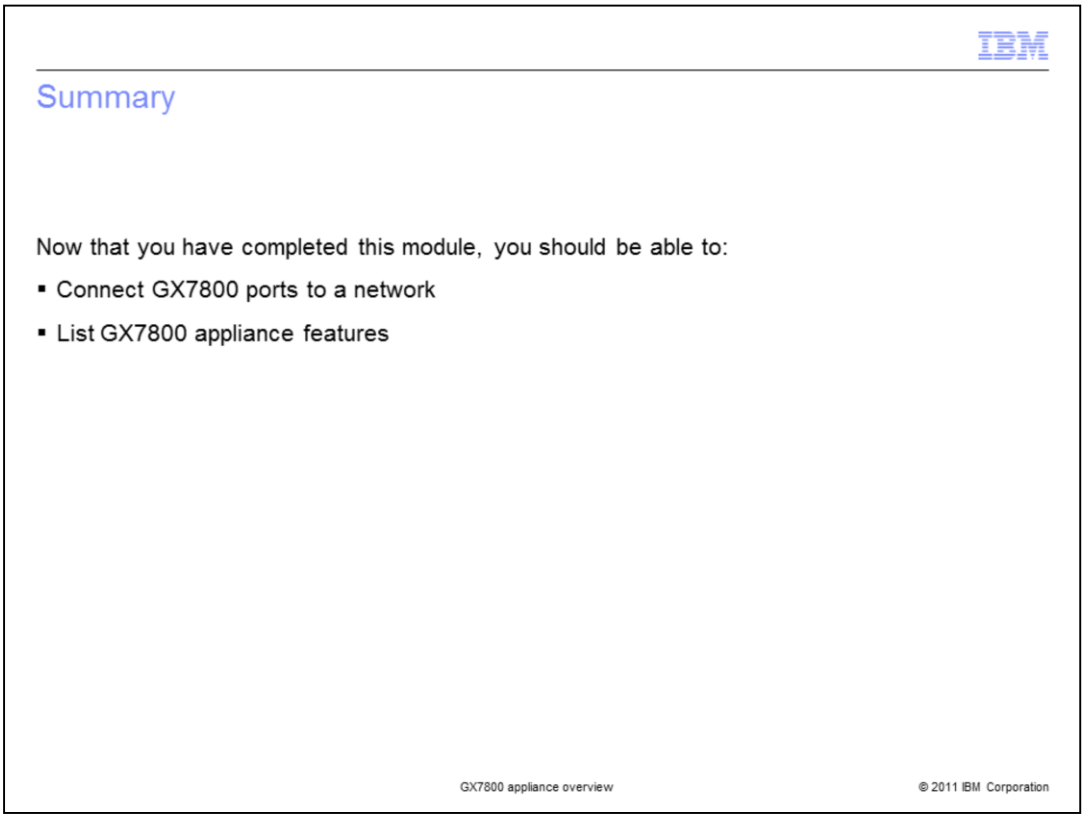
AppScan integration is available through the SiteProtector Console. There is also a distributed denial of service (DDOS) quarantine response.

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.



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