Cisco XR 12000 Series Routers for Advanced Business Services

Q. What is Cisco® announcing today?

A. Cisco is announcing the new hardware and software capabilities of the Cisco XR 12000 Series platform that enhance the ability of service providers to offer advanced, predictable business services, including Cisco IOS® XR Session Border Controller (SBC), business video, managed network-based security, and VPNs.

Q. What has changed in terms of business services capability on the Cisco XR 12000 Series platform?

A. In the past the Cisco XR 12000 platform supported the following business services:

- Multiprotocol Label Switching (MPLS) VPN
- Managed security using appliances

To address changing customer needs for more sophisticated business services, the Cisco XR 12000 platform supports:

- MPLS VPN
- IPsec VPN
- Layer 2 Tunneling Protocol Version 3 (L2TPv3) Layer 3 VPN
- Managed security using integrated hardware
- SBC
- Telepresence enabled by the SBC
- Business video
- Application-aware VPNs
- Managed voice over IP (VoIP)

Q. What new Cisco XR 12000 hardware and software are being offered to enable these new business services capabilities?

A. The following hardware and software elements are being offered on the Cisco XR 12000 platform to enable or enhance these capabilities:

- IPsec VPN Shared Port Adapter
- Multi-Service Blade
- Integrated SBC on Multi-Service Blade
- Virtual Firewall on Multi-Service Blade

Cisco XR 12000 Series Platform

Q. What is the Cisco XR 12000 Series?

A. The Cisco XR 12000 Series Routers accelerate the service provider evolution toward IP Next-Generation Networks (NGNs), combining the unparalleled innovation of Cisco IOS XR Software with investment protection for the market-leading Cisco 12000 Series. Offering secure virtualization, continuous system operation, and multiservice scale, the Cisco XR

12000 Series provides intelligent routing solutions that scale from 2.5 Gbps per slot to n x 10 Gbps per slot capacity, enabling next-generation IP/MPLS networks.

Q. How does the Cisco XR 12000 Series support secure virtualization?

A. The Cisco XR 12000 Series is powered by Cisco IOS XR Software, allowing service providers to isolate public and private services through the virtualization of a single router into separate physical and logical partitions. Cisco IOS XR Software supports secure virtualization through the innovative Cisco Service Separation Architecture, which provides the ability to logically and physically separate the control planes of different services on a single router. Services and customers are isolated from each other for maximum security and increased operational and management efficiency.

Q. How does the Cisco XR 12000 Series support continuous system operation?

A. Cisco IOS XR Software has been optimized to operate in platforms, such as the Cisco CRS-1 Carrier Routing System and Cisco XR 12000 Series, that can scale and distribute processing as well as perform distributed forwarding. Cisco IOS XR Software is built on a distributed, microkernel-based operating system infrastructure that allows processes and subsystems to be distributed to any of potentially thousands of processing resources, and includes critical optimizations to allow for the support of millions of routes, hundreds of thousands of interfaces, and thousands of peers. Cisco IOS XR Software includes support for Nonstop Forwarding (NSF), Stateful Switchover (SSO), In Service Software Upgrades (ISSUs), control-plane data checkpointing, service separation, and embedded management elements that allow the Cisco CRS-1 and Cisco XR 12000 Series to provide continuous system operation required in converged IP NGNs.

Q. How does the Cisco XR 12000 Series offer multiservice scale?

A. With distributed processing intelligence, robust quality of service (QoS), and multicast mechanisms, the Cisco XR 12000 Series allows providers to scale both services and customers with predictable performance.

- Cisco IOS XR Software distributes processing intelligence to each ISE line card (that is, OS infrastructure and applications, Layer 3 forwarding, line card-specific control functions, and packet manipulation) and to additional route processors installed in the system (that is, Border Gateway Protocol [BGP], Integrated System-to-Integrated System [IS-IS], etc.). Distributed processing intelligence removes software limitations to system scale and allows network operators to take full advantage of the aggregate capacity of installed hardware in the system.
- Dedicated queuing application-specific integrated circuits (ASICs) on each ISE line card provides unparalleled per-customer QoS that protects against jitter and delay of video, and time-sensitive data and voice applications without affecting scale or performance.
- Multicast replication is handled by the fabric to avoid service-disrupting congestion associated with routing systems that replicate frames at the line card level.

Q. How many customers worldwide have deployed the Cisco XR 12000 Series in their network?

A. With distributed processing intelligence, robust QoS, and multicast mechanisms, the Cisco XR 12000 Series allows providers to scale both services and customers with predictable performance. Eight Cisco XR 12000 customers run live traffic using Cisco IOS XR Software (five networks on Release 3.3 and three networks on Release 3.4). Additionally, six customers are scheduled for deployment of Release 3.4.1 prior to May 2007.

IPsec VPN Shared Port Adapter

Q. What is the Cisco Network-Based Security Services solution?

A. The Cisco Network-Based Security Services solution helps service providers deliver cost-effective, scalable, integrated security services for businesses of all sizes. Service providers can expand their service portfolio and offer a more comprehensive bundle of secure VPNs and security services for enterprise and small- and midsized-business (SMB) customers.

The Cisco XR 12000 IPsec VPN Shared Port Adapter (SPA) provides secure, on-net and off-net remote access and remote site-to-site services on the Cisco XR 12000 Series Router with Cisco IOS XR Software Release 3.4 or higher. With the release of Cisco IOS XR Software Release 3.5, Cisco Network-Based Security Services will be extended to include virtual firewall support on the Cisco XR 12000 Multi-Service Blade (MSB).

Q. Who is the target market for the solution?

A. This solution is most suited to service providers with the following attributes:

- Currently offering MPLS VPN services and looking to extend their geographic coverage without new network build-out in order to capture the mobile worker, telecommuter, and remote, site-to-site VPN market
- Currently offering MPLS VPN services or dedicated Internet access and looking to add remote-access VPN

This solution is also suitable for service providers that have one or more of the following:

- An IP core or plans to deploy an IP core and offer VPN services over the IP core
- Existing Layer 2 Frame Relay or ATM service and seeking to extend geographic coverage
- Broadband aggregation services or plans to offer broadband aggregation services plus VPN services
- Hosting services with desire to offer secure access as a premium service

Q. What is IPsec?

A. IPsec is an industrywide standard for assuring the privacy, integrity, and authenticity of information crossing public IP networks.

Q. What is the Cisco XR 12000 IPsec VPN SPA?

A. A SPA is a modular port adapter that is interchangeable across Cisco routing platforms by way of the SPA interface processor (SIP). The Cisco XR 12000 IPsec SPA (Figure 1) can be used with the Cisco 12000 Series SPA Interface Processor-400 (Cisco 12000 SIP 401), Cisco 12000 SIP 501, or Cisco 12000 SIP 601 to provide hardware-assisted encryption, key generation, and other services suitable for IPsec VPNs.

More information about the full range of SPAs and SIPs available for the Cisco XR 12000 Series Router is available at: http://www.cisco.com/en/US/prod/collateral/routers/ps167/product_data_sheet0900aecd80465682.html

Figure 1. Cisco XR 12000 IPsec VPN SPA

Q. What are service virtual interfaces (SVIs)?

A. SVIs are routable configuration entities used for diverting packets from physical interfaces into IPsec SPAs; they are available in two types:

- service-ipsec (to terminate IPsec tunnels)
- service-gre (to terminate generic routing encapsulation [GRE] tunnels protected by IPsec)

Association of security parameters to SVI traffic is accomplished by attaching the cryptographic IPsec profile to the SVI.

Q. Does the Cisco XR 12000 IPsec SPA have a physical interface?

A. No. The Cisco XR 12000 IPsec SPA does not have physical interfaces. It is connected to the router backplane through the SPA interface processor card and interoperates with any type of physical interfaces supported on the Cisco XR 12000 Series Router.

Q. What Cisco IOS XR Software release is required to use IPsec VPN SPA services on the Cisco XR 12000 Series?

A. The Cisco XR 12000 IPsec VPN SPA requires Cisco IOS XR Software Release 3.4 or later.

Q. Is IPsec supported on the Cisco XR 12000 Series using Cisco IOS Software?

A. No. IPsec requires Cisco IOS XR Software on the Cisco XR 12000 Series Router.

Q. What are some typical deployments for the Cisco XR 12000 Series with IPsec VPN SPA?

A. Many service providers deploy IPsec VPN technology for geographical extension of their existing VPN network and to offer IPsec for remote users when accessing a corporate VPN. This technology is also used by enterprises to replace their traditional WANs with site-to-site and remote-access VPNs. The Cisco XR 12000 IPsec VPN SPA offers next-generation encryption technology and a form factor designed to enable a more flexible and scalable network infrastructure.

Q. Is it possible to attach a QoS policy to the outbound, clear (pre-encrypted) IPsec traffic?

A. Yes. A QoS policy can be applied to the clear outbound traffic by attaching a “pre-encrypt” policy map to the SVI. This policy map is similar to the output policy map applied to the egress traffic of physical interfaces and subinterfaces, where it is typically used to shape the traffic toward the customer premises equipment (CPE) and provide low-latency queues for high-priority traffic and guaranteed traffic queues for business-critical traffic.

Q. Is it possible to attach a QoS policy to the inbound, decrypted (clear) SVI traffic?

A. Yes. A QoS policy can be applied to the inbound, decrypted SVI traffic by attaching a post-decrypt policy map to the SVI. This policy map is similar to the ingress policy map attached to the ingress traffic of physical and subinterfaces. A post-decrypt policy map typically is used to

monitor customer service-level agreements (SLAs) by policing and coloring the traffic before it enters the VPN.

Q. Is it possible to apply a QoS policy to the encrypted traffic?

A. Yes. A QoS policy can be applied to SVI-encrypted traffic by attaching a pre-decrypted policy map to the SVI. Such a QoS policy is used mainly for SPA protection and bandwidth isolation between SVIs sharing the same IPsec SPA resource.

Q. Is it possible to apply a QoS policy per IPsec tunnel?

A. No. All tunnels within an SVI are subject to the QoS policy attached to the SVI.

Features

Q. What are the key features of the Cisco XR 12000 IPsec VPN SPA?

A. The Cisco XR 12000 IPsec VPN SPA supports the following:

- IPsec tunnel mode and GRE + IPsec transport mode
- Encryption performance of 2 Gbps per SPA; up to 20 IPsec SPAs can be installed in a Cisco XR 12416 system (10 slots x 2 IPsec SPAs in a slot, plus 2 route processors, plus 4 line cards with line interfaces) to provide 40 Gbps of total throughput
- Large number of simultaneous IPsec, site-to-site, or remote access VPN tunnels (up to 16,000 IPsec tunnels)
- Fast tunnel setup (average of 100 tunnels per second)
- Support for both site-to-site and Cisco Easy VPN remote-access IPsec tunnels
- Virtual Route forwarding (VRF) awareness
- Network Address Translation (NAT) transparency
- Look-ahead fragmentation to reduce loads on peer devices without having to reassemble fragmented IPsec packets before decrypting them
- Support for Diffie-Hellman 1, 2, and 5
- Authentication: RSA digital signature, RSA public key encryption, and preshared keys
- Certificate authority
- Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES) ciphers
- Message Digest Algorithm 5 (MD5) and Secure Hash Algorithm 1 (SHA1) hashing
- Dead peer detection (DPD)
- Authentication, authorization, and accounting (AAA) integration (as well as per-VRF AAA)
- IP address allocation through RADIUS – Framed IP or local IP address pool
- Intrachassis stateful failover per SVI
- Internet Key Exchange (IKE) call admission control (CAC)
- Look-ahead fragmentation plus path maximum transmission unit (PMTU) discovery
- Multicast over both IPsec and GRE SVIs
- QoS (inbound and outbound) per SVI
- IPsec static load balancing
- Extensible Markup Language (XML) and MIB support

Q. Does the Cisco XR 12000 IPsec VPN SPA support Dynamic Multipoint VPN (DMVPN)?

A. No, DMVPN is not supported under Cisco IOS XR Software Release 3.4, but a future release may support this function.

Q. Does the Cisco XR 12000 IPsec VPN SPA support Dynamic Group VPN (DGVPN)?

A. No, DGVPN is not supported under Cisco IOS XR Software Release 3.4, but a future release may support this function.

Q. Does the Cisco XR 12000 IPsec VPN SPA support both site-to-site and remote-access IPsec?

A. Yes.

Q. With what Cisco platforms does the Cisco XR 12000 IPsec VPN SPA interoperate for IPsec site-to-site VPNs?

A. The Cisco XR 1200 IPsec VPN SPA interoperates with all other Cisco IOS Software router platforms – as well as Cisco VPN 3000 Series Concentrators and Cisco PIX® security appliances – using IPsec site-to-site VPNs and should also interoperate with other vendor platforms that implement RFC-compliant IPsec services.

Q. What VPN clients work with the Cisco XR 12000 IPsec VPN SPA?

A. DevTest has successfully tested the Cisco XR 12000 IPsec VPN SPA with the Cisco Easy VPN client. The Cisco XR 12000 IPsec VPN SPA should interoperate with any IPsec RFC-compliant VPN client. However, many third-party clients lack the value-add policy push innovations available with the Cisco Easy VPN client. Because Cisco provides the Easy VPN client free of charge for unlimited distribution, the company strongly urges its use whenever possible.

Support for SafeNet remote client is included in Cisco IOS XR Software Release 3.5.

Q. Does the Cisco XR 12000 IPsec VPN SPA support high availability?

A. Yes. Intrachassis, stateful failover (active-active and active-standby) is supported.

Q. Does the Cisco XR 12000 IPsec VPN SPA support Cisco Encryption Technology?

A. No. Only IPsec encryption is supported.

Q. Does the Cisco XR 12000 IPsec VPN SPA support RSA encryption?

A. Yes.

Q. Does the Cisco XR 12000 IPsec VPN SPA support AES encryption algorithm?

A. Yes.

Q. Does the Cisco XR 12000 IPsec VPN SPA support compression?

A. No. The Cisco XR 12000 IPsec VPN SPA does not support the IP Payload Compression Protocol (IPComp or IPPCP).

Q. Are GRE keepalives supported on service-GRE protected interfaces?

A. No. GRE keepalives are not supported under Cisco IOS XR Software Release 3.4, but a future release may support this function.

Q. Is dynamic PMTU supported on service-IPsec interfaces?

A. Yes.

Q. Is dynamic PMTU supported on service-GRE interfaces (IPsec + GRE)?

A. No, the Cisco XR 12000 IPsec VPN SPA does not support PMTU with GRE interfaces.

Performance and Scalability

Q. What is the maximum encryption throughput of the Cisco XR 12000 IPsec VPN SPA?

A. The IPsec VPN SPA supports up to 2.5 Gbps throughput.

Q. What is the maximum encryption packets-per-second performance of the Cisco XR 12000 IPsec VPN SPA?

A. The Cisco XR 12000 IPsec VPN SPA supports up to 600 kpps.

Q. Is there a performance penalty when using 3DES versus DES?

A. No. There is no performance difference when using DES or 3DES.

Q. Is there a performance penalty when using AES versus DES or 3DES?

A. Yes. There is minimal performance penalty when using AES.

Q. What is the maximum number of IPsec tunnels supported per Cisco XR 12000 IPsec VPN SPA and per Cisco XR 12000 platform equipped with multiple IPsec VPN SPAs?

A. The maximum number of IPsec tunnels per platform, regardless of the number of IPsec SPAs installed, is 16,000, where each tunnel is represented by 1 IKE and 2 IPsec Security Associations (inbound and outbound Security Associations).

Future Cisco IOS XR Software releases will significantly increase the number of IPsec tunnels supported on the router, but the number of IPsec tunnels per SPA will remain 16,000.

Q. What is the tunnel per second (TPS) establishment rate?

A. The average tunnel establishment is 100 tunnels per second for all 16,000 tunnels.

Q. What is the maximum encryption throughput supported on the Cisco XR 12000 Series Router?

A. A full rack of Cisco XR 12416 (10 x IPsec SIPs + 2 route processors + 4 line cards) provides 40-Gbps IPsec traffic.

Q. What is the maximum number of SVIs supported on the Cisco XR 12000 Series Router?

A. The Cisco XR 12000 Series Routers support 750 SVIs per line card and 2200 SVIs per box, but future releases will scale to higher numbers of SVIs per router and per line card.

SIP hardware resources limit the maximum number of SVIs per line card to no more than 2048.

Q. What is the maximum MTU (packet size) supported by the Cisco XR 12000 IPsec VPN SPA?

A. The Cisco XR 12000 IPsec VPN SPA supports a maximum MTU of 9200 bytes.

Q. What is the maximum number of access control lists (ACLs) on the Cisco XR 12000 Series Router when using the IPsec VPN SPA?

A. The Cisco XR 12000 IPsec VPN SPA supports up to 10,000 ACL entries (that is, ACL lines).

Q. How does the Look Ahead Fragmentation (prefragmentation, or LAF) affect performance?

A. LAF is enabled by default but can be selectively disabled through the command-line interface (CLI) (refer to the *Installation and Configuration Guide* for details). When enabled, LAF checks to see if the packet – when combined with IPsec, GRE, and even NAT-Traversal (NAT-T) headers – would exceed the MTU. If so, the Cisco XR 12000 IPsec VPN SPA automatically fragments the packet prior to encryption, sparing the peer IPsec device cycles from having to reassemble the packet.

Management

Q. What IPsec-related MIBs are supported on the Cisco XR 12000 Series Router?

A. The Cisco XR 12000 IPsec VPN SPA and associated Cisco IOS software support the following IPsec MIBs:

- CISCO-IPSEC MIB
- CISCO-IPSEC-FLOW-MONITOR MIB
- CISCO-IPSEC-POLICY-MAP-MIB

Q. Can XML be used for configuring and monitoring IPsec on the Cisco XR 12000 Series Router?

A. Yes.

Additional Information

Q. Where can I find the Cisco IOS XR Software System Security Configuration Guide?

A. You can find it at: http://www.cisco.com/univercd/cc/td/doc/product/ioxsoft/iox34/cgcr34/sc_c34/index.htm.

Q. Where can I find the Cisco IOS XR Software System Security Command Reference?

A. You can find it at: http://www.cisco.com/univercd/cc/td/doc/product/ioxsoft/iox34/cgcr34/sc_r34/index.htm.

Multi-Service Blade

Q. What are the important characteristics of the Cisco XR 12000 Multi-Service Blade?

A. The primary characteristics follow:

- 10-Gbps service card with superior packet processing capability (refer to Figure 2)
- High-performance architecture comprising network processors and CPU farms to support a wide range of services, including SBC for voice and video (telepresence, etc.) applications and security services
- Configurable within any slots for the Cisco XR 12000 Series Routers in all form factors
- Initial set of services that includes SBC and virtual firewall
- Option to add up to two additional daughter cards to the blade baseboard to provide any additional hardware support needed for future applications

Figure 2. Cisco XR 12000 Multi-Service Blade

Integrated Session Border Control on Multi-Service Blade

Q. What is session border control on the Cisco XR 12000 Series?

A. A general description follows:

The Cisco XR 12000 is the first carrier router to offer integrated session border control functions. The Cisco XR 12000 Session Border Controller (SBC) builds on the secure virtualization, continuous system operation, and multiservice scale provided by the market-leading Cisco XR 12000 Series. With the integration of session border control functions into Layer 2 and Layer 3 services provided by the Cisco XR 12000 Series, the Cisco XR 12000 SBC eliminates the need for overlay networks and standalone appliances. The Cisco XR 12000 SBC provides an open and flexible architecture for all service provider deployments, whether for peering or for customer access. With its ability to handle unified and distributed signaling deployments, the Cisco XR 12000 SBC provides superior deployment flexibility to cable, wireline, and wireless service providers.

The Cisco XR 12000 SBC application takes advantage of the advanced hardware processing capabilities of the Cisco XR 12000 Multi-Service Blade to provide a flexible, scalable, and feature-rich implementation (Figure 1). The integration of the SBC into the Cisco XR 12000 Series routers facilitates the deployment of advanced services that require a combination of Layer 2 and Layer 3 functions (QoS, security, VPN interconnect, etc.) and session border control functions.

Q. Which Cisco XR 12000 Series chassis and line cards support the SBC function?

A. SBC functions are available on all Cisco XR 12000 Series chassis and work in conjunction with any of the line cards supported on the Cisco XR 12000 Series.

Q. Do we need to account for an effect on the Cisco XR 12000 Series control or data-plane functions by the introduction of the SBC on the same chassis?

A. No. The SBC does not affect any of the Cisco XR 12000 Series functions, scale, or performance.

Q. What additional hardware is needed to enable the SBC?

A. The Cisco XR 12000 Multi-Service Blade provides all the required hardware support for enabling the SBC.

Q. Is there any limit on the number of Cisco XR 12000 Multi-Service Blade cards that can be placed in a chassis?

A. No. This number is limited only by the total number of line card slots available on the chassis.

Q. What are the main advantages of the Cisco XR 12000 Series Router that make it ideal for handling business services?

A. Cisco XR 12000 Series Router is the world's premier business services platform offering the following main advantages:

- The IP NGN foundation for business VPN – Resilient IP/MPLS with integrated security; fully distributed architecture for scale and performance with services; and scalable platform for future service evolution
- Integrated business services over Ethernet – Business services with common capability over different access media (Layer 2 and Layer 3 VPN, Virtual Private LAN Services (VPLS), Frame Relay, ATM, and pseudowire); managed security with managed IPsec VPN, virtual firewalls, and session border control for business voice and telepresence
- Unmatched QoS and multicast for business VPN SLA – Includes best-in-class voice, video, data performance, and scale

Virtual Firewall on Multi-Service Blade

General

Q. What are the common deployment applications for the Cisco Network-Based Security Services solution?

A. Using the Cisco Network-Based Security Services solution, which combines virtual firewall and network-based IPsec VPN services, service providers can support the multiple applications and use the network-edge devices to provide security services to multiple customers at the same time.

Application examples follow:

- Internet access – The firewall can be deployed to support Internet offload for VPN customers. It provides the ability to apply individual firewall policies per customer.
- Site-to-site firewall access – The solution can be used to provide site-to-site firewall service, allow users to apply policies on a per-site basis, and control access between locally connected sites as well as between the sites and the rest of the VPN.
- Shared services access – The firewall can be used as an interface between the VPN customers and any shared services offered by the provider that they access.

Q. Does the Cisco XR 12000 virtual firewall require special hardware?

A. Yes, the Cisco XR 12000 virtual firewall is based on the Cisco XR 12000 Multi-Service Blade hardware (part number XR-12K-MSB) to provide enhanced security features with rich stateful inspection firewall services.

Please refer to the multiservice blade data sheet for more information: http://www.cisco.com/en/US/prod/collateral/routers/ps6342/product_data_sheet0900aecd8057f45b.html

Q. Can I apply virtual security contexts to a customer-facing interface?

A. Yes, the innovative Router Service Packet Path (RSPP) scheme enables a simple way to attach security contexts to the broad set of Cisco XR 12000 interfaces and subinterfaces. Similar to other type of polices that can be applied to the Cisco XR 12000 interfaces (such as QoS), the security context policy can be attached to any interface without an effect on dynamic routes protocols.

Q. Can I use single security contexts to protect multiple customer interfaces?

A. Yes, multiple customer-facing interfaces can be attached to a single security context.

Q. Can I use the Cisco XR 12000 virtual firewall between Virtual Route Forwarding (VRF) instances?

A. Yes, the VRF-aware service infrastructure (VASI) enables transparent insertion of services to inter-VRF traffic.

Q. Does the Multi-Service Blade support VRF-aware Network Address Translation (NAT)?

A. Yes, each security context can be used for such application. Static and dynamic NAT and Port Address Translation (PAT) are supported.

Q. What is a VASI interface?

A. The VASI infrastructure provides the ability to configure a VASI pair interface, a routable dual virtual interface for inter-VRF binding that provides the ability to easily apply services on the inter-VRF traffic.

Q. Does the Cisco XR 12000 virtual firewall support URL filtering?

A. No, only basic URL filtering is available, without the option to connect to an external device such as Websense and N2H2.

Performance and Scalability

Q. Can I use multiple multiservice blades in a single Cisco XR 12000 chassis?

A. Yes. The total numbers of contexts and interfaces are subject to the overall Cisco IOS XR Software scalability capabilities.

Q. How many security contexts are supported per multiservice blade?

A. Cisco IOS XR Software Release 3.5 supports 250 virtual firewall contexts; future releases will scale up to 500 contexts.

Q. What is the maximum throughput per multiservice blade with virtual firewall?

A. Each multiservice blade can scale up to 8 Gbps or 2 mpps.

Q. What is the maximum number of Layer 4 connections per second that a single multiservice blade can process?

A. Each multiservice blade can scale up to 150,000 connections per second.

Q. What is the maximum number of connection per second with Layer 7 inspections that can be processed in a single multiservice blade?

A. Each multiservice blade can scale up to 15,000 connections per second with HTTP inspection.

Q. How many access list entries (ACEs) are supported per single multiservice blade?

A. Each multiservice blade can support 250,000 ACEs.

Q. How many VASI pair interfaces can be configured on a single multiservice blade?

A. Up to 500 VASI pairs can be configured on a single blade.

Q. Is the number of virtual interfaces independent of the number of interfaces in the chassis?

A. No, the total number of interfaces in the chassis is subject to the overall Cisco IOS XR Software scale capabilities.

Q. What is the maximum number of interfaces supported on a single multiservice blade?

A. Up to 2000 interfaces can be supported. Note that each VASI pair consumes 2 interfaces, each firewall management interface (FMI) consumes 1 interface, and each interface protected by firewall contexts consumes 1 interface.

Management

Q. What Simple Network Management Protocol (SNMP) versions does the Cisco XR 12000 virtual firewall support?

A. SNMPv1, v2c, and v3 are supported.

Q. What is FMI?

A. FMI is a firewall management interface that can be configured under each security context to provide a virtualized management interface. The FMI can be used to connect management devises such as Telnet, Secure Shell (SSH) Protocol clients, authentication, authorization, and accounting (AAA) servers, etc.

Q. What options are available to configure and monitor security contexts?

A. Each security context is virtualized with its own management IP address and can be configured or monitored with the following options:

- Telnet – Through a command-line interface (CLI)
- SNMP for monitoring – Read-only MIBs
- AAA – Lightweight Directory Access Protocol (LDAP), TACACS, and RADIUS
- Syslog
- SSH
- Extensible Markup Language (XML)

Q. What is RBAC?

A. Role-based access control (RBAC) enables the option to assign different roles within specific security contexts with different levels of rights and capabilities to each person working within a context, ensuring that each team can operate almost completely separately.

High Availability

Q. What data is replicated by the failover process?

A. Connections:

- The goal of connection replication is to synchronize eligible connections so that a failover does not disrupt existing connections.
- Very short-term connections cannot be synchronized; TCP connections that are terminated or “proxied” are not eligible.

Q. The Cisco XR 12000 Series supports route processor failover. How does it affect firewalls?

A. Route processor failover is a platform feature and is totally transparent to the firewall. No firewall-specific configuration is required to support this type of failover.

Q. What are the triggers for multiservice blade switchover?

A. The triggers are:

- Service location configuration change (Cisco IOS XR Software)
- An active multiservice blade has detected some anomaly (such as a Linux process crash)
- “Heartbeat” loss (hardware failure, etc.)
- Auto-revert (preferred active node becomes operational)

Q. How do you connect to the active and or standby location of a context for management purposes?

A. Connecting to security context is available from:

- Indirect access from the route processor – After you have connected to the route processor, you can attach your session to a specific multiservice blade and access each of the security context configurations and statistics.

- Direct access to the security context IP address – Each security context can be configured with a management interface (FMI) with a dedicated IP address. A separate IP address (peer's IP address) is available for direct access to the standby contexts.

Note that FMI is required on both the preferred active and preferred standby security contexts.

Q. When failover occurs, do I need to switch my direct management access to the standby contexts?

A. No, this happens automatically. The FMI can be configured to always send traffic to the active (or standby) location. The IP address of the active security context is preserved during switchover.

Additional Information

Q. Where can I find more information about the Cisco XR 12000 Series?

A. For more information about the Cisco XR 12000 Series, visit: http://www.cisco.com/go/12000.

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 C67-397331-00 03/07