riverbed

Major Features in SteelConnect EX Release 21.2.1

This document describes the major features introduced in Release 21.2.1 for SteelConnect EX Analytics, SteelConnect EX Director, and SteelConnect EX OS and Controller devices.

System and Hardware

Internet Speed Tests

You can run speed tests for SteelConnect EX OS and Controller devices from a Director node using predeployed internet speed-test servers. To run an internet speed test, you need only an internet connection over a WAN link to reach the internet speed-test server, eliminating the need to deploy an independent speed-test server.

MLPPP on T1/E1 Interfaces

T1/E1 NIC interfaces support multilink PPP (MLPPP) on T1/E1 CSG Series NIC interfaces. MLPPP allows you to bundle separate PPP links into one bundled PPP interface to provide one higher-speed connection across a WAN. An MLPPP link acts as a single logical interface, requiring only one IP address, which simplifies network design while load-balancing traffic across member links. SteelConnect EX OS and Controller devices support a rich set of Layer 3 through Layer 7 functions on MLPPP interfaces.

The SteelConnect EX MLPPP implementation is fully compliant with the MLPPP standard as defined in RFC1990, and it is interoperable with other vendors' equipment.

OS Security Packages for Ubuntu 18.04–Based SteelConnect EX OS and Controller Images

SteelConnect EX provides two sets of SteelConnect EX OS and Controller images: one based on Ubuntu 14.04 and the other based on Ubuntu 18.04.

Previously, SteelConnect EX provided Ubuntu OS security packages (SPacks) for Ubuntu 14.04–based SteelConnect EX OS and Controller images. Now, SteelConnect EX also provides OS SPacks for the Ubuntu 18.04–based SteelConnect EX OS and Controller images.

Note: OS SPacks for Ubuntu 18.04–based SteelConnect EX OS and Controller images are not compatible for the images based on Ubuntu 14.04. We recommend that you keep your systems up to date with the latest OS SPacks.

When new OS SPacks are available, Riverbed sends announcement emails with details about the OS SPack and instructions about how to download and apply the OS SPack on all SteelConnect EX OS and Controller devices. A single OS SPack may contain one or more security updates or patches. The application process applies all OS-level security patches that are part of a single package.

PPP PAP and CHAP on T1/E1 Interfaces

You can configure the T1/E1 authentication protocol and associated password using the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) authentication methods for PPP. PAP and CHAP are fully compliant with the standards, and they have been successfully tested for interoperability with other vendors' equipment.

PPP has a built-in mechanism to authenticate its peer using either PAP or CHAP. When a PPP connection is established, each end can request the other to authenticate itself. If the authentication fails, the connection is terminated. Authentication must be successful before starting NCP (Layer 3 protocol) negotiation and to complete the successful bring up of PPP.

PAP authentication uses a clear-text username and an optionally encrypted password to authenticate the PPP peer. This technique is vulnerable to eavesdroppers who may try to obtain the password by listening in by wiretapping the actual line as clear-text authentication happens.

CHAP authentication does not have these deficiencies. With CHAP, the authenticator sends a randomly generated challenge string to the client, along with its hostname. The client uses the hostname to look up the appropriate secret, combines it with the challenge, and encrypts the string using a one-way hashing function. The result is returned to the server along with the client's hostname. The server then performs the same computation and acknowledges the client if it arrives at the same result. Another feature of CHAP is that it does not require the client to authenticate itself only at startup, but also sends challenges at regular intervals to ensure that the client has not been replaced by an intruder, for example, by just switching phone lines. For these reasons, CHAP authentication is preferred over PAP authentication.

PoE Power Management Support on CSG Platforms

On SteelConnect EX CSG platforms, you can configure PoE parameters on PoE interfaces. Configurable PoE parameters include enabling and disabling PoE, per-port granular power controls, with a granularity of 0.5 W, and statically and automatically defined maximum values. When configuring PoE, you can enable the PoE interface for the port to provide power to a connected device. When a new device connects on a higher-priority port, a lower-priority port is powered off automatically if the overall power budget of the NIC is exceeded. The SteelConnect EX OS and Controller software provides operational commands to monitor PoE operations, including power status, consumption, and PoE standard in use.

Proxy ARP and Proxy NDP

Ethernet interfaces on SteelConnect EX OS and Controller devices support proxy ARP (for IPv4) and proxy NDP (for IPv6).

The ARP and NDP protocols translate IP addresses to MAC addresses to enable communications between hosts on the same subnet of the TCP/IP stack. Hosts connected on a LAN use ARP for both unicast traffic and on direct connections. The host sends an ARP request that includes the IP address of the receiver to request the receiver's MAC address. NDP supports router discovery, presence, and DHCP options. By default, ARP and NDP are enabled on device network interfaces.

Proxy ARP and proxy NDP provide local responses, allowing SteelConnect EX OS and Controller devices to reduce the amount of broadcast traffic over Layer 2 networks such as EVPN across SD-WAN and VXLAN.

QAT and SSL-TLS Proxy

In Release 20.1, SteelConnect EX added support for Intel QAT on Rangeley, Denverton embedded QAT blocks, and Coleto Creek cards with dedicated QAT processors. In Release 21.2.1, SteelConnect EX adds support for offloading the SSL/TLS encryption and decryption functions to QAT for hardware-based acceleration for these cryptographic functions. Offloading these functions to QAT increases the SSL/TLS proxy performance.

The SteelConnect EX QAT support includes built-in QAT functions on Intel SoC processors and a PCI bus attached QAT modules. The SteelConnect EX OS and Controller software automatically detects the presence of an embedded QAT module. Depending on the hardware platform, QAT is either enabled or disabled by default.

Secure Boot

UEFI secure boot is a verification mechanism for ensuring that a SteelConnect EX OS and Controller device boots only software components that are trusted by the original equipment manufacturer (OEM), which, in this case, is Riverbed. The UEFI secure boot verifies the software components sequentially, starting with verifying the signature of the boot loader. Secure boot is supported on CSG700 series appliances running Ubuntu 18.04.

When the appliance starts, the firmware checks the signature of the first boot software, which then checks the signature of the next boot software, and so on, including the kernel and low-level drivers of the operating system. If the signatures are valid, the appliance boots, and the firmware turns control over to the operating system. Providing a secure handoff allows secure boot to act as an interface between the SteelConnect EX OS and Controller software and the firmware.

Enabling and configuring secure boot protects appliances from malware attacks and infection. Secure boot detects any tampering of key OS files by validating digital signatures. Secure boot also acts as a gatekeeper for sensitive credentials.

Security Package Enhancements

You can upgrade an application protocol bundle. The application engine protocol bundle is a database that contains 3600+ signatures that are used to detect and identify applications. It is included in the SPacks. When you first deploy headend and branch network components, an SPack is preinstalled on a Director node based on your subscription type.

TPM 2.0

Trusted Platform Module (TPM) technology provides hardware-based, security-related functions. A TPM chip is a secure crypto processor that helps with actions such as generating, storing, and limiting the use of cryptographic keys. Releases prior to Release 21.2.1 provide support for TPM1.2, which is used to protect private keys for certificates.

Release 21.2.1 adds support for TPM2.0 for SteelConnect EX OS and Controller devices that have a TPM2.0 chip and that are running with an Ubuntu (Bionic) image.

TPM for Protecting Sensitive Data

Sensitive data, such as user passwords and preshared keys in VPN profiles, are protected using per-device encryption keys. The TPM module facilitates secure generation of cryptographic keys in the hardware. In Release 21.2.1, the encryption keys are further protected by hardware-based TPM cryptographic keys on SteelConnect EX OS and Controller devices having either a TPM1.2 or TPM2.0 chip. The TPM cryptographic key provides dual protection (software-based and hardware-based) for the sensitive data.

TWAMP-Light

Two-Way Active Measurement Protocol (TWAMP) Light provides multivendor, interoperable probes on LAN interfaces, WAN interfaces, and IKEv2-based IPsec tunnels.

A TWAMP-light probe measures performance parameters of IP networks by sending test packets and monitoring their experience in the network. The SteelConnect EX OS and Controller TWAMP-light implementation is fully compatible with the standard as defined in Appendix I of RFC 5357.

TWAMP-light has many of the characteristics of TWAMP. However, the session reflector does not necessarily have knowledge of the session state. The TWAMP-light session reflector simply copies the sequence number of the received packet to the sequence number field of the reflected packet, while generating timestamp values to facilitate the collection of two-way metrics, such as latency, jitter, and packet loss, in a multivendor deployment. The SteelConnect EX OS and Controller implementation of TWAMP-light supports both stateful and stateless reflectors. A stateful reflector generates its own sequences, which do not need to match those of the sender. For a stateless reflector, the reflector copies the sender's sequence number to its own sequence number in reflected packets.

Other vendors support TWAMP-light, including Cisco, Huawei, Juniper Networks, and Nokia. When you can configure TWAMP-light on SteelConnect EX OS and Controller devices to measure network characteristics, other vendors' equipment can respond to or reflect the probe. You can configure other vendors' equipment to generate probes to which the SteelConnect EX OS and Controller device responds.

USGv6 Compliance

The United States National Institute of Standards and Technology (NIST) developed the USGv6 technical infrastructure, including standards and testing, to support wide-scale adoption of IPv6 in the U.S. Government (USG). USGv6 is a technical standards profile to help the U.S. government acquire IPv6-enabled networked information technology.

The USGv6 profile includes protocol specifications published by the Internet Engineering Task Force (IETF) that encompass basic IPv6 functionality and that define specific requirements and key optional capabilities for routing, security, IP multicast, network management, and quality of service. The profile also includes the NIST requirements for IPv6-aware firewalls and intrusion detection systems (IDSs).

The USGv6 program has established a robust testing infrastructure so that IPv6 products can be tested by accredited laboratories using standardized test methods for compliance to profile requirements and for interoperability.

As part of Release 21.2, Riverbed has placed extra focus to comply with the USGv6 testing scope and criteria. Riverbed has also initiated testing and certification of the SteelConnect EX solution for USGv6 compliance.

SteelConnect EX Analytics Features

Analytics Cluster Redundancy

You can configure Analytics cluster redundancy. There are two redundancy options:

- Active-backup mode—In active-backup mode, the secondary (backup) cluster is used only when the primary cluster goes down. The application delivery controller (ADC) load balancer on the Controllers steers the log connections to the secondary cluster during data center failure. When the primary data center comes back up, the ADC switches the connections back to the primary cluster. The secondary cluster may have collected data for the duration of the time of failure. The secondary cluster may run the database or just perform the log collection function. You can use cron scripts on the secondary cluster to ship logs back to the primary cluster when it comes back up.
- Active-active mode—In active-active mode, both primary and secondary clusters receive log data from SteelConnect EX OS and Controller devices. The ADCs on the Controllers have separate virtual IP addresses (VIPs) for the primary and secondary clusters. There is no backup pool configured on the VIPs. During normal conditions, both clusters will have the same data. During failure, the cluster that is down may not have the data for the period of failure. Data will not be synced between the clusters. You may need to connect to both the clusters to compare the data during failure scenarios.

Analytics Log Collector Nodes Accept Newer IPFIX Template Version

Analytics log collector nodes can accept logs from SteelConnect EX OS and Controller devices running IPFIX versions newer than the version known on the Analytics log collector node.

Analytics Platform Alarms

Analytics platform–related alarms provide real-time status about services and activities that require attention. These alarms are logged locally on the hosts, and they can also be streamed to third-party remote collectors, including Director nodes.

Data Plane Availability Report

The data plane availability report shows whether a branch has connectivity to any other remote branches other than Controller nodes. To display the data plane availability charts, select the Availability tab of a site. The new service uptime report shows how long the device has been up. You can use the information in this report to determine whether there were any local issues, such as service restarts and device reboots.

Last Month Time Selector

In the day/time selector, you can choose the last month. The last month is the previous calendar month. For example, if today is February 15, the last month report provides data for January, from January 1 through 31.

LEF Collector Group List

Log export functionality (LEF) on SteelConnect EX OS and Controller devices is used to send various service-specific logs, such as SD-WAN, CGNAT, security, and system logs, to a destination collector. These services refer to a LEF profile, which points to a destination collector or a collector group. A LEF collector group is a container for one or more collectors which are in active-backup mode. Logs are sent to one of the active collectors in the collector group. You can send logs to multiple destination collectors for high availability or for serving different applications by configuring a collector group list. A LEF profile can refer to a collector, collector group, or collector group list. A collector group list is a list of collector groups. Logs are sent to the active collector of each of the collector groups in the list.

Log Archive Management

After logs are processed on Analytics log collector nodes, the logs are compressed and stored in gzip files in the Analytics archive directory on the node where they were received. You can restore or delete archived logs from SteelConnect EX Director. You can also view the dates of the oldest and newest log archive file and the number of log archive files.

Log Collector Connection Eviction Optimizations

Analytics local log collectors processes the logs received from client connections. By default, each local collector has a maximum connection limit set to 512. When this limit is reach, the log collector stops accepting new connections. You can increase the maximum number of connections. However, doing so can overload the log collector node, especially if all the connections are carrying active data. To reduce the number of connections, you can now use the connection eviction feature on Analytics log collector nodes. Connection eviction closes unused connections so that the Analytics log collector node can make space for active connections from CPEs.

Log Export From Analytics Reporting Tool

The Analytics reporting tool includes a feature to export logs. After generating a report containing logs, you can export the logs to a compressed file from the GUI. The report is then available for download.

SD-WAN Application Report Enhancements

Traffic type and forwarding class are new fields in logs sent from SteelConnect EX OS and Controller devices. When displaying SD-WAN site application information for a specific SteelConnect EX OS and Controller device, you can drill down to display. usage per traffic type and forwarding class. Traffic type can be SDWAN or DIA. Forwarding class can be one of the 16 forwarding classes, for example: fc_ef, fc_be, fc_nc, or fc_af.

SD-WAN Site Tag Enhancements

SD-WAN reports allow you to filter based on site tags to get reports for a subset of sites for a tenant. The same concept extends to generating reports for sites with matching tags.

Secure Access Report Enhancements

The secure access report provides details of the number of registered users per gateway, client OS, client OS version, client version, and location.

Statistics Rollup

The Analytics platform receives large volumes of data every 5 minutes from SteelConnect EX OS and Controller devices. Reports with source IP and destination IP addresses typically take up large amounts of storage and computing resources. You can configure SteelConnect EX OS and Controller devices to send only the top-N of these types of reports to reduce the number of records sent and processed. However, there can still be a large number of unique records over an hour or a day.

Statistics rollup provides a mechanism to reduce the volume of stored data by performing aggregation and computing the top-N for the hour and day. Rollup can now be done for firewall sources and destination statistics reports. Migration cron jobs are run automatically on the Analytics nodes to migrate existing data to new roll tables.

Synchronized Charts for Path Status

A new synchronized chart option displays multiple time-series charts for SD-WAN path status for charts containing the same zoom level and time range. This helps in visualizing various metrics of the paths at the same time. Metrics for all paths between branches are displayed.

System Anomalies Report

SteelConnect EX Analytics dashboards now offer a SteelConnect EX OS and Controller device anomalies chart. Appliance anomalies include CPU load exceeded, memory load exceeded, and worker thread busy (LCORE detection). You can drill down to display additional charts showing each of the anomalies over time.

Threshold-Based Reporting

The Analytics reporting tool can now filter based on conditions set per report type. Some examples are usage reports when bandwidth exceeds a certain threshold, sites or links with low availability, and sites whose violations exceed a limit.

TWAMP Reports

The Two-Way Active Measurement Protocol, defined in RFC 5357, is used to measure metrics such as delay, delay variation, and loss between two IP endpoints that support the TWAMP sender and receiver functionality. The metrics are exported to Analytics nodes. SteelConnect EX Analytics dashboards now offer a TWAMP metrics chart for a tenant or SteelConnect EX OS and Controller device. You can drill down to display additional charts showing metrics over time.

WiFi Statistics

SteelConnect EX Analytics now offers WiFi statistics dashboards. For multitenant devices, these reports are part of the provider organization. The dashboard displays devices and connected clients for a specified time range. You can drill down to display additional charts showing each of the anomalies over time. You can drill down into the chart to view details of all clients connected to the appliance.

SteelConnect EX Director Features

Cloud API Enhancements

SteelConnect EX Director integrates with Azure virtual WAN and AWS Transit Gateway APIs. The API integration allows you to use the Director portal to discover the Virtual WAN and Transit Gateway services and to create site-to-site tunnels.

In Release 21.2.1, the API integration supports scenarios where the branch is behind a NAT.

SteelConnect EX SASE-Hosted Director and CMS Connector for Site-to-Site Tunnels

You can create a SteelConnect EX Director-managed IPsec site-to-site tunnel between a provider Director node and a tenant Director node so that the tenant can use services available from the provider Director node as if the services were available directly from the tenant Director node. These services include:

- On-ramp to SaaS providers, such as Google, Office, Box, and SalesForce
- Cloud Service Gateways (CSGs)

- Application reverse proxies
- Titan hubs

VMS Enhancements

In Release 21.1.1, Riverbed introduced VMS, an intelligent, high-performance message processing and streaming server. VMS uses gRPCs and protocol buffers (protobuf) to implement fast and efficient processing of high volumes of information distributed across the network. VMS can use plug-ins and specialized receptors to listen to information sources. After VMS gathers and normalizes the information, it is distributed to SteelConnect EX OS and Controller on-premises devices. SteelConnect EX OS and Controller devices can also make gRPC calls to the VMS server to request information.

In Release 21.2.1, SteelConnect EX provides the following VMS enhancements:

- High availability for VMS infrastructure and VMS containers.
- Admin container for VMS, which allows you to manage services and the VMS deployment. The admin container includes Rest API capabilities provided by VMS so that you can manage the VMS features and infrastructure.
- Passive authentication—SteelConnect EX OS and Controller devices use VMS to support passive authentication, using it to check and confirm user identity without requiring any specific action to authenticate users. For passive authentication, VMS handles high volumes of streamed data and disseminates this data to SteelConnect EX OS and Controller devices deployed across anetwork.

Workflow Support for Interfaces

In Release 21.1, SteelConnect EX introduced support for T1/E1 and ADSL2+/VDSL2+ interfaces, and you could configure them from the Director Configuration tab.

In Releases 21.2.1, you can configure these interfaces using Workflows, making configuration of the interfaces easier and integrating the interface configuration in the SD-WAN Workflows.

SteelConnect EX OS and Controller Device Features

Layer 2

EVPN Multihoming

You can deploy EVPN multihoming for MPLS-based EVPNs over SD-WAN and for VXLAN EVPNs in data center and campus environments.

The SteelConnect EX OS and Controller EVPN multihoming provides high availability (HA), operating in all-active and single-active modes. You can deploy with a single-active forwarding node or all-active forwarding nodes without concern about Layer 2 loops. The SteelConnect EX OS and Controller EVN multihoming eliminates the need for proprietary technologies such as MC-LAG, virtual chassis, and VPC.

The SteelConnect EX OS and Controller VXLAN EVPN multihoming allows more than two Ethernet switches or WAN edge devices to participate in a redundancy group. It also provides an all-active Layer 2 solution, which can use all LAN underlay or WAN interfaces for Layer 2 forwarding.

The SteelConnect EX OS and Controller EVPN multihoming solution is fully RFC-compliant, and it is fully interoperable with other vendor solutions.

Layer 2 Fragmentation and Reassembly across SD-WANTunnels

As part of its Layer 2 solution, the SteelConnect EX OS and Controller software can transport large Layer 2 frames over WANs while the underlying WAN network can have smaller MTUs (such as 1500 byte MTUs for Internet traffic).

You can configure the SteelConnect EX OS and Controller software can be configured to use its native VXLAN function at each SD-WAN tunnel endpoint to encapsulate Layer 2 frames into Layer 3 so that the Layer 3–encapsulated Layer 2 frames can be fragmented before they are placed into encrypted SD-WAN tunnels (by means of a logical tunnel interface.) The larger Layer 2 frame is placed in a VXLAN header and is identified by a VNID that is specific to the network segment across SD- WAN section of the network. The VXLAN-encapsulated Layer 2 frame is then fragmented by the SteelConnect EX OS and Controller software and encrypted based on the IPsec SA and sequence numbers specific for the SD-WAN peering, and finally, it is transmitted to the other side of the SD-WAN tunnel.

The received encrypted SD-WAN packet is first decrypted. A subsequent lookup results in reassembly of the Layer 3 packet, and then VXLAN lookup and decapsulation of the transported (reconstructed) Layer 2 frame. The reconstructed Layer 2 frame is then forwarded to its destination. The execution of the entire fragmentation and reassembly process is operation completely transparent to end devices.

This operation is supported for Layer 2 unicast and Layer 2 broadcast, unknown and multicast (BUM) frames.

Policy and Traffic Management for Layer 2 Flows

For Layer 2 flows, you can configure the following policy and traffic management:

- SD-WAN policy and traffic management capabilities such as Layer 2 traffic pinning and Layer 2 flow management across SD-WAN tunnels. You can use existing Layer 3 SD-WAN flow policies on Layer 2 flows as well or create new flow policies.
- Filtering based on MAC address, IP address, URL, VLAN, application, and service, to allow you to drop, forward, and accept Layer 2 traffic.

Note that packet cloning and FEC for Layer 2 flows are not supported.

Virtual Extensible LAN (VXLAN)

SteelConnect EX OS and Controller devices support Virtual Extensible LAN (VXLAN). VXLAN is a network virtualization technology that attempts to address some of Layer 2 limitations by encapsulating Layer 2 frames within Layer 3 and then routing through the underlay using Layer 3 routing techniques, thus making use of Layer 3 data plane and control plane capabilities.

While Layer 2 has advantages, such as local broadcasting and discovery, being able to use the same IP subnet across member devices, and direct communication without using routing functions, traditional Layer 2 technologies also have some disadvantages. Well-known disadvantages of traditional Layer 2 include no built-in prevention for network loops, no TTL support, scaling limitations, and slow convergence on the data plane based learning and forwarding. These limitations translate to restrictions in topology and in how you can deploy and use Layer 2, including restrictions in topology and usage of parallel network paths. To address some of these challenges, various vendors had developed proprietary technologies such as MC-LAG, virtual chassis, stacked Ethernet switch solutions, VPC, OTV, and TRILL. While these acted as point solutions, they did not address the overall problem or the shortcomings of Layer 2.

VXLAN was proposed as a solution to this the same set of problems and VM mobility needs for the data center and, later, for other parts of the network, such as campuses. VXLAN uses a VLAN-like technique to encapsulate OSI Layer 2 Ethernet frames within UDP datagrams, using UDP port 4789 as the default IANA-assigned destination port number. VXLAN endpoints, which terminate VXLAN tunnels and may be either virtual or physical switch ports, are known as VXLAN tunnel endpoints (VTEPs).

VTEPs encapsulate and decapsulate Layer 2 frames in IP-UDP packets using VXLAN encapsulation, as defined in RFC 7348. After determining that the destination for a Layer 2 frame is at the remote end of a VXLAN tunnel overlay, the VXLAN on-ramp function encapsulates the Ethernet frame into the VXLAN header, setting the correct VNID value, and then transmits it over the IP (Layer 3) underlay to the VTEP that is the destination of the Layer 2 frame. At the destination, the VXLAN off-ramp function performs a lookup to determines local Layer 2 network for which the frame is destined, decapsulates the VXLAN frame, and transmit it over the wire with the appropriate Layer 2 headers (that is, VLANs).

VXLAN is the result of evolution of efforts to standardize on an overlay encapsulation protocol. It increases scalability to up to 16 million logical networks and allows for Layer 2 adjacencies across IP networks. Multicast or unicast with ingress head-end replication (HER) is used to flood Layer 2 broadcast, unknown unicast, and multicast (BUM) traffic.

VXLAN uses several techniques to learn and distribute reachability information. On the LAN and VLAN ports, it uses traditional data plane learning and forwarding methods, and between VXLAN peers it uses control plane based (MP-BGP) EVPN to exchange reachability information. MP-BGP–based EVPN has been expanded to carry VNID values with different route types, to carry Layer 2 and the associated Layer 3 reachability information so that the appropriate Layer 2 and Layer 3 forwarding decisions can be made across VXLAN connections.

For more details about VXLAN control plane protocols and encapsulations, see the VXLAN RFCs.

For the SteelConnect EX OS and Controller VXLAN implementation, on the LAN or underlay ports, the SteelConnect EX OS and Controller software uses data plane learning and forwarding, and across VXLAN peers it uses standards-based EVPN VXLAN reachability exchange and forwarding capabilities. The SteelConnect EX OS and Controller implementation is natively part of virtual switches and bridge domains, allowing you to make full use of the rich set of the SteelConnect EX OS and Controller Layer 2 features for LAN and WAN.

The SteelConnect EX OS and Controller VXLAN implementation makes full use of Layer 3, and Layer 4 through Layer 7 SteelConnect EX OS and Controller features using IRB interfaces, allowing you to seamlessly configure Layer 3 routing and Layer 4 through Layer 7 services functions together with VXLANs. The SteelConnect EX OS and Controller VXLAN implementation does not have the types of lookup restrictions that may exist in other vendors' implementations, so you have complete flexibility to apply on-ramp and off-ramp functions after Layer 2, Layer 3, and Layer 4 through Layer 7 lookups and network function chaining.

The SteelConnect EX OS and Controller VXLAN implementation interoperates with third-party, standards-compliant VXLAN devices and software- defined networking (SDN) solutions.

The SteelConnect EX OS and Controller VXLAN solution allows you to address use cases such as the following:

- In virtualized data centers or campus environments, you can use SteelConnect EX OS and Controller devices and VXLAN to connect WAN edge devices seamlessly to each overlay instance (for example, for each tenant), eliminating the need to create an on- ramp or off-ramp device and eliminating the need for additional provisioning for VLAN-based handoff to or from the WAN edge. In this case, the SteelConnect EX OS and Controller VXLAN solution provides a seamless gateway function between WAN overlays, such as SD-WAN or WAN underlays, and VXLAN running on the data center or campus LAN. In this role, the SteelConnect EX OS and Controller device can also provide full set of security functions in the gateway itself. You can also make full use of the underlying Ethernet switch network, configuring all its interfaces as VXLAN tunnels and having them terminate on SteelConnect EX OS and Controller devices at the edges of the network, such as virtualized servers. This also achieves seamless VM mobility and Layer 2 and Layer 3 connectivity within a virtualized data center.
- As an extension of the previous use case, you can deploy combination of the SteelConnect EX OS and Controller EVPN solution across the SD- WAN network, with VXLAN running in the data center, to provide Layer 2 connectivity between WAN sites and virtualized servers within the data center that host various applications. The SteelConnect EX OS and Controller solution provides seamless stitching between SD-WAN overlays and VXLAN overlays on the edge of the data center for Layer 2 connectivity from branches all the way to the virtualized workloads in the data center. This method of connection allows clients and applications to share the same subnet, so it is suitable for autodiscovery, VM mobility, and disaster recovery.
- SteelConnect EX OS and Controller devices can communicate with third-party (access layer) Ethernet switching solutions using VXLAN overlays across aggregation or core layers of campus or enterprise Ethernet networks. In this use case, as a SteelConnect EX OS and Controller device receives packets from the WAN, via SD-WAN overlays or from WAN underlays, it encapsulates traffic to VXLAN and sends it to the access layer Ethernet switches, which can then implement the VXLAN off-ramp function and forward the traffic to Ethernet-attached devices. In the reverse direction, for WAN, NGFW, or UTM use cases, an access or edge Ethernet switch can encapsulate the traffic into the appropriate VXLAN instance (that is, VNID) and send to a SteelConnect EX OS and Controller device. You can deploy a variant of this solution using third-party WiFi APs.
- The SteelConnect EX OS and Controller VXLAN solution can provide a load-balancing Layer 2 handoff to other third-party equipment while Ethernet LAGs may be in prevalent use in underlays.

Platform

Traffic Policing for Source IP Address Per Originating Device

You can police traffic generated by endstations. Each endstation is organized by source IP address (that is, by a /32 address). Policing allows you to rate-limit traffic generated by endstations so that WAN bandwidth can be shared more fairly among the endstations on a LAN.

SD-WAN

Codec, MOS Scoring, and Policy-Based Traffic Management Enhancements

In releases prior to Release 21.1, SteelConnect EX Secure SD-WAN supported detection of MOS score for over 120 video/voice and audio codecs and popular applications, including Microsoft Office Teams and Google Talk. In a bookended scenario (that is, for sessions over the SD-WAN overlay), the MOS score is used as an SLA condition for

selecting a path. If the SLA is violated, that is, if the MOS score violates a predefined threshold, the video/voice or audio session is switched to alternate path.

Release 21.2.1, Secure SD-WAN supports additional popular uCAAS applications, including Cisco Webex, and Ring Central, and Zoom. You can configure all MOS detection, reporting, and traffic engine options for these new uCAAS applications.

Riverbed Compatibility Mode

When customers require that SD-WAN devices be deployed together with WAN optimization devices, there are challenges unique to having the two coexist in the same deployment. If you deploy them in a cascaded form with the WAN optimization device closest to the WAN and the SD-WAN device closest to the LAN, the SD-WAN device loses visibility into the WAN interface's state and it may lose some other features, such as flexible topologies and dynamic traffic steering changes, while the WAN optimization device is unable to optimize IPsec-encapsulated traffic. If you switch the cascaded positions of the two so that the WAN optimization product faces the LAN and the SD-WAN product faces the WAN, the SD-WAN device may not be able to recognize any applications because flows have been processed by the WAN optimization functions, thus reducing the value of the SD-WAN devices. In such deployments, WAN optimization replaces the original packet headers or content with only the unique or required data (that is, byte- or block-level data) after the deduplication. The post-WAN optimization data that needs to be transmitted over the WAN to the other WAN optimization peer device may also be compressed, which ordinarily makes it impossible for an SD-WAN device to figure out the application or relation to the original flow.

The SteelConnect EX OS and Controller software Riverbed compatibility mode allows you to deploy WAN optimization and SD-WAN products together while retaining the full functionality of each product, allowing you to make full use of the features and benefits of SteelConnect EX for SD-WAN and WAN Edge and Riverbed for WAN optimization. Riverbed Technology and Versa Networks worked together to develop interoperability features that are implemented in Riverbed-Versa service chaining. The SteelConnect EX OS and Controller software now includes the service-chaining enhancements to recognize and manage flows after they have been optimized by the Riverbed SteelHead WAN optimization.

To enable this synergistic mode of operation, you must place the Riverbed SteelHead WAN optimization product (either the physical platform or VM) in a new service chain type specialized on Riverbed compatibility mode. In this mode of deployment, the SteelConnect EX OS and Controller device acts as both a LAN-facing and a WAN-facing router or gateway, while the Riverbed SteelHead device connects to a SteelConnect EX OS and Controller device through a service-chaining interface and provides WAN optimization. This arrangement allows the SteelConnect EX OS and Controller device to receive LAN traffic and to perform initial flow processing, including ingress lookups, and to apply policies. The SteelConnect EX OS and Controller device then hands off the packets of each flow to the Riverbed SteelHead device, and it receives the packets back after the Riverbed SteelHead device has performed its optimization process.

Packets in a flow that are received after the WAN optimization are recognized by specific headers, and they are processed further by the SteelConnect EX OS and Controller device and then forwarded to the WAN, thus making full use of the SteelConnect EX SD- WAN functions. You can think of this as a U-turn type of topology, in which the traffic starts at the SteelConnect EX OS and Controller device, is passed to the Riverbed SteelHead device, and is then

returned to the SteelConnect EX OS and Controller device. In this type of deployment, you can configure the Riverbed SteelHead WAN optimization in either transparent or non-transparent mode. Note that for these deployments, you must deploy the Riverbed SteelHead platform or VM in a service chain and you must place the Riverbed SteelHead device on the “side" of the SteelConnect EX OS and Controller device.

The SteelConnect EX OS and Controller software uses 5-tuple information to identify each flow on the LAN-facing interfaces. During its initial processing, the SteelConnect EX OS and Controller software makes a note of the ingress interface and trust/untrust functions, identifies the application (AppID), applies security policies, and finally applies QoS policies. However, when you enable Riverbed compatibility mode, instead of processing these packets with egress-facing functions, the SteelConnect EX OS and Controller software hands these packets over to the Riverbed SteelHead device with specific headers that are critical to establishing and carrying out the service-chain functions. To understand the details of this, let's first look at how Riverbed SteelHead function operates.

The Riverbed WAN optimization can operate in either transparent or non-transparent mode. In transparent mode, the WAN optimization preserves the original set of 5-tuples of the flow, while in non-transparent mode these fields are overwritten with Riverbed-specific information. The SteelConnect EX OS and Controller software compatibility mode supports both optimization modes.

If you use transparent mode, because the Riverbed SteelHead device preserves the 5-tuple on its output and the SteelConnect EX OS and Controller device preserves the 5-tuple information when forwarding traffic to the Riverbed SteelHead device and expects the original 5-tuple values back, the SteelConnect EX OS and Controller device can recognize each flow and can continue to apply policies and SD-WAN functions after the WAN optimization. In this release, SteelConnect EX has added support for QoS rewrite in transparent mode. Essentially, the SteelConnect EX OS and Controller native service-chaining function is enhanced to break out traffic from its internal service chain so that it is processed by the Riverbed SteelHead device, and then the service chains reconverge afterwards.

If you use non-transparent mode, because the original set of 5-tuple values are completely replaced by Riverbed proprietary fields, which are dynamic in nature, the SteelConnect EX OS and Controller software inserts network service headers (NSHs) before it passes the traffic to the Riverbed SteelHead device on the service-chain interface. The Riverbed SteelHead device preserves the NSH headers during the WAN optimization. The NSH header carries important information, such as service chain index that resides in base NSH fields and TLV-based extensions that encode the flow ID, session index, receive interface index, CoS rewrite rules, and other important information so that when the SteelConnect EX OS and Controller device receives the WAN-optimized flow, it can apply the correct set of SD-WAN decisions on the flows.

Riverbed compatibility mode also supports scenarios that include application cloud deployments.

SD-WAN Policy Enhancements

SD-WAN policy has been enhanced for the following:

- SD-WAN policy rules have been enhanced to allow matches based on the destination zone.
- DNS resolution-based path affinity configuration is available for each forwarding profile. Prior to Release 21.2.1, DNS resolution-based path affinity was configurable only at the system level. In Releases 21.2.1, you can configure session-pinning/domain-app-cache in the forwarding profile. To use DNS resolution-based path affinity in a forwarding profile, you must disable the system-level setting. Note that if you enable the DNS resolution-based path

affinity at the system level, path affinity is enabled for all forwarding profiles regardless of any profile-level configurations.

- Alarms for next-hop SLA—If you configure an SLA profile for next hops, an alarm (nexthop-sla-not-met) is generated when the next-hop SLA is not met. The alarm is cleared when the next-hop SLA returns to compliance state.

SD-WAN Traffic Steering Enhancements

SD-WAN traffic steering has been enhanced to include path bandwidth monitoring, which is used in traffic intelligent traffic load-balancing scenarios, and remote site interface bandwidth information exchange as the SD-WAN path weight factor in traffic steering decisions across alternative paths.

There are two new DIA traffic load-balancing methods:

- Weighted round-robin (WRR)
- High available bandwidth

You can perform SD-WAN DIA traffic steering based on monitored circuit bandwidth. The bandwidth monitor calculates the available uplink and downlink bandwidth of the WAN circuit towards a speed-test server based on the server's IP address, and then uses these values in policy-based forwarding (PBF) as the WAN circuit reference bandwidth in traffic load balancing.

You can configure SD-WAN traffic steering to monitor path bandwidth. The bandwidth monitor calculates the available path bandwidth towards remote SD-WAN sites and uses these values as the path reference bandwidth when steering traffic across multiple paths toward that remote branch.

In an active-active setup, cross-connect links can inherit a paired site's configured uplink and downlink bandwidth, and they use it as reference bandwidth for the corresponding cross-connect links. In this way, no additional shaping or interface uplink or downlink configuration on the cross-connect links.

Security

802.1 X NAC Enhancements

Starting with Release 20.2, the SteelConnect EX OS and Controller software has supported native 802.1X NAC. In Release 21.2, multiple supplicants can share the same interface and each supplicant can be assigned to a different VLAN or network instance based on device credentials and security policies. You can configure an authentication server to dynamically assign VLANs to bridge access ports using the 802.1X device authentication flow, to provide granular management of shared ports that are used by multiple devices. As an example, a port on a SteelConnect EX OS and Controller device may connect to an Ethernet switch that serves multiple client devices, and now, each device can be authenticated and authorized independently for network access.

You can configure an authentication server (such as a RADIUS server) to dynamically assign VLANs to access ports using 802.1X device authentication. The following are the supported 802.1X operation modes on a per-port basis:

- Single supplicant—Authenticates only the first end device. All other end devices that later connect to the port are allowed access with no further authentication. The subsequent devices effectively piggyback on the first end device's authentication.
- Single-secure supplicant —Allows only one end device to connect to the port at a time. No other end device can connect until the first device logs out.
- Multiple supplicant—Allows multiple end devices to connect the port, and each end device is authenticated individually.

The NAC enhancements allow you to admit devices but separate their traffic from other devices based on security and network access policies. The SteelConnect EX OS and Controller software can assign VLANs based on authentication success and device type and class as administered by the RADIUS server, guest VLANs (that is, providing limited access for non-responsive end devices that are not 802.1X-enabled), or based on configuration driven attributes.

You can apply such granular NAC policies and traffic management capabilities to network-attached devices such as IoT, guest, enterprise-issued end-user devices, and other types of corporate devices.

The 802.1X enhancements are fully compatible with all the other SteelConnect EX OS and Controller Layer 2, Layer 3, Layer 4, and Layer 7 features.

Firewall Rules Management Enhancements

Security rules define the policy to be applied to data traffic. Each security rule consists of match criteria and an enforcement action. The match criteria can be based on Layer 3 and Layer 4 fields, Layer 7 applications, and other traffic patterns. It is important to prioritize the order in which the rule is evaluated, from the most granular to least granular. If you configure traffic rules incorrectly, traffic that should be allowed can be blocked or, worse, traffic that should have been blocked is allowed to pass.

In releases prior to Release 21.2.1, when you create a new rule, the rule is placed at the end of all the rules and, as a result, it has the lowest priority. If this is not the correct priority, you then have to manually move the rule to the correct priority. This is a tedious tasks when a policy already has a large number of rules.

In Release 21.2.1, when you begin creating a new rule, you can choose the location of the new rule. The following options are provided:

- Create the new rule with the highest priority; that is, place the rule at the beginning of all the rules so that it is evaluated first.
- Create the new rule with the lowest priority; that is, place the rule at the end of all the rules so that it is evaluated last.
- If you select an existing rule, create the new rule above the selected rule.
- If you select an existing rule, create the new rule below the selected rule.

In releases prior to Release 21.2.1, when you add a rule, it is enabled by default. This design can cause issues, for example, when you wanted to temporarily disable a rule for debugging or other purposes. In Release 21.2.1, you can disable a rule. Specifically, you can disable rules in the following types of policies:

- Class of service (CoS) QoS policy
- CoS App QoS policy
- Layer 2 SD-WAN policy
- SD-WAN PBF policy
- Secure access gateway policy
- Secure access portal policy
- Security access policy
- Security authentication policy
- Security decryption policy
- Security DoS policy
- Service filter classifiers
- Traffic mirroring policy
- Traffic monitoring policy

Layer 7 Device Authentication and Compliance

You can authenticate client devices based on client or user certificates. To authenticate using a client certificate, you use a SteelConnect EX OS and Controller TLS proxy, which you configure in a decryption profile. In the decryption profile, you can apply Layer 7 device authentication and a decryption profile to all web traffic or to the selected web addresses requested by the client device.

The device authentication is performed as part of the TLS handshake, during which the SteelConnect EX OS and Controller TLS proxy replies with a certificate-based authentication request. To proceed, the client must provide the device or user certificate to proceed.

After a client device is authenticated using a certificate, the authentication is saved in the form of a cookie so that the SteelConnect EX OS and Controller device can avoid repeatedly performing authentication.

You can apply Layer 7 device authentication and compliance selectively, based on web addresses or other criteria. An example of such granular control is to decrypt the URLs of corporate applications while processing personal URLs (for example, personal banking URLs) without decryption.

Network Data Leak Prevention

It is rare to find an enterprise today that does not store critical data in digital format. One of the unwanted side effects of digitization is that it makes it very easy for the data to be exported to external storage. This can happen inadvertently when a user uploads the data by mistake. It can also be the result of the actions of malicious users trying to exfiltrate critical data.

To protect this data, you can use data leak prevention (DLP), which scans the data transiting from an internal network to external servers. The DLP platform monitors the presence of patterns such as credit card information, addresses, and national IDs, and based on the configuration and policy, the DLP platform can block the data stream.

You can configure DLP on SteelConnect EX OS and Controller devices. In conjunction with secure SD-WAN policies, DLP ensures that the data being exported does not contain any sensitive information.

SteelConnect EX OS and Controller devices can scan various protocols, including HTTP, FTP, SMTP, POP3, and IMAP, they can scan the protocol headers and payloads, including attachments, and they can detect credit card information. For attachments, SteelConnect EX OS and Controller devices can scan all Microsoft Office file formats (doc, docx, xls, xlsx, etc.) and plain-text files. You can also define the file types, minimum and maximum file sizes, filenames, keywords (for example, Top Secret) that are allowed or blocked.
You can configure keywords with regular expressions, including wildcards.

Before deploying DLP, contact Riverbed Support.

SteelConnect EX Secure Access (SCSA)

SCSA Application-Based Traffic Steering

Application-based traffic steering on the client, available for Windows 10 and MacOS clients, allows you to determine breakout traffic based on Layer7 criteria such as application name and FQDN. You can define the following for an application or FQDN:

- Tunnel the traffic, on either an encrypted or unencrypted tunnel
- Do local break out

The application name is the name of the process from which the traffic originates, specified either as the process name or fully qualified filename.

SCSA Granular User Profile Administration

SCSA provides connectivity for remote users to the SCSA server. After a user is authenticated and connected to a gateway, a Cloud Gateway applies security policy for the connection depending on many criteria, including user name, user group, and originating location.

Starting in Release 21.2.1, you can configure user profiles to apply during the registration process. You can configure the portal/registrar with different profiles based on user, user group, source address, endpoint protection, OS version, and managed or unmanaged device and compliance status from MDM. The profiles dictate the tunnel characteristics and the gateways to which users can connect. The policy is evaluated periodically, and the client configuration is updated if necessary.

After the registration succeeds, the client determines the gateway that has been downloaded from the portal. You can also configure the gateway with different profiles, using the same parameters, to determine tunnel characteristics.

SCSA One-Time Passwords

SCSA allows remote users to connect to SteelConnect EX OS and Controller devices, which can be configured as SCSA servers. A customer connects to a SCSA server using the Secure Access Service Edge (SASE) client. The SCSA server authenticates the user based on the preferred authentication method. As an additional security option, SCSA can enforce multifactor authentication.

You can configure the SteelConnect EX OS and Controller software to generate a multifactor authentication code, also called a one-time password (OTP). Prior to Release 21.2.1, the authentication code could be sent using SMS. Starting in Release 21.2.1, the authentication code can be sent using email. By forcing users to enter a dynamically generated authentication code, you can verify that the users have access to cell phones and email, as well as to enterprise credentials.

The SCSA time-based OTP mechanism generates a one-time password generator, which uses the current time as a unique factor. Time-based OTP (TOTP) assumes that the user application and server have agreed upon initialization parameters. After initialization, a new OTP is generated regularly. The server authenticates the client by challenging it to provide the current valid OTP, and a client is authenticated if it successfully provides the OTP. Because the OTP is time sensitive and has very short validity period (30 seconds to 3 minutes), time-based OTP reduces the impact of phishing and credential stealing attacks.

You can enforce time-based OTP for remote users who connect using a SASE client. When enabled, the SASE client registration procedure initializes time-based OTP. During initialization, the portal generates a QR code. Scanning the QR code initializes using an authenticator application, such as Cisco Due, Google authentication, or Microsoft authenticator.

After the authentication, each time a SASE client connects to the server, the user is prompted for an OTP. After the user enters the OTP generated by the authenticator application initialized during the registration process, the authentication is successful and the connection is accepted.

SCSA Policy for Portals and Gateways

SCSA follows a two-step establishment process:

- Registration—When a user installs a client on a new device, they must register the device. The registration phase authenticates the user with the registrar. After authentication completes, the gateway configuration, certificate, and other service configuration are downloaded to the client, and the client is then ready to connect to the gateway. The registration step is performed only once, when a device needs to be configured (or reconfigured).
- Connect—This step occurs each time user needs to set up a secure connection between the user and the gateway.

Prior to Release 21.2.1, SCSA supported only single policy for all users. There was no way to provide different configuration parameters based on user, user group, location, or other parameters.

Starting in Release 21.2.1, you can configure multiple profiles in the portal and gateway. Contextual information, such as username, user group, location, and device compliance status, is used to download and apply the appropriate profile.

SCSA SAML

Security Assertion Markup Language (SAML) is an open standard for interworking with identity providers. Popular identity providers such as Okta, PingID, and Azure Active Director (AD) SSO support SAML based interworking. From the viewpoint of single sign-on (SSO), SCSA is a service provider and Okta, PingID, and Azure AD SSOs are identity providers. SCSA supports SAML-based integration with identity providers.

Integrating SSO with SCSA has significant benefits for enterprise and end users, including:

- Improved user experience—User credentials must be entered less frequently.
- Improved security—Enterprise administrators control security parameters, such as multifactor authentication, in a single product.