Hillstone Networks

ReleaseNotes for StoneOS 5.5R10 F Releases

Version 5.5R10F

ReleaseNotes for StoneOS 5.5R10 F Releases

ReleaseNotes for StoneOS 5.5R10 F Releases contains all the release note for the F version of 5.5R10. It mainly introduces the new features of the F version, known issues and upgrading notes.

StoneOS 5.5R10F6

Release Overview

Release Date: June 28th, 2024

This release provides 16 new features and 32 merged features. This release enhances features in hardware, system, policy, VPN, SNMP, etc. The key adjustment involves the following aspects:

- More models can send monitor data such as threat logs to the cloud platform and iSource. In this release, X-series models and SG-6000-K9180/K6580 support this function.
- Support to configure the packet capture mode. By specifying the packet capture mode, you can capture data packets of all traffic on the interface or all data packets whose sessions are established and that meet the packet capture rules.
- VXLAN supports to reference the IPSec tunnel to encrypt VXLAN packets within IPSec pack-

ets. This ensures data security during VXLAN tunnel transmission.

- Optimize AD Scripting for SSO and SSO Monitor for SSO.

For description of all the functions, see New Features.

For the supplementary note for the new functions, refer to *New Features Guide for StoneOS 5.5R10F Releases*.

All released information: https://fr.hillstonenet.com/show_bug.cgi?id=43157

Inheritance & Merging Details of 5.5R10F6:

- Inherit all FRs and fixed bugs of 5.5R10F5;
- Merge all FRs, known issues, and fixed bugs of 5.5R10P6;
- Merge FR36021 from 5.5R10F1.X;
- Merge FR38570 from 55.5R10F3.X;
- Merge FR40365, FR39815, and FR40041 from 5.5R10F4.X;
- Merge FR40651 from 5.5R10F5.X;
- Merge FR39985, FR41433, FR41437, FR41445, FR41451, FR41735, FR41737, FR41739, FR41741, FR41743, FR41745, FR41747, FR41749, FR41751, FR41753, FR41755, FR41757, FR41759, FR41761, FR41763, FR41765, FR41767, FR41769, FR41771, FR41773, and FR41775 from 5.5R10P6M2.

Platforms and Images

Platform Models	Images
SG-6000- A7600/A6800/A5800/A5600/A5555/A5500/A5255/A5200/A5155- /A5100 /A3815/A3800/A3700/A3615/A3600/A3000/A2815/A2800 /A2715/A2700/A2600/A2000/A1100/A1000	SG6000-A-1- 5.5R10F6.img SG6000-A-1- 5.5R10F6-v6.img

Platform Models	Images
SG-6000-A200/A200G4B (4G)/A200W (WLAN)	SG6000-A-3-5.5R10F6.bin SG6000-A-3-5.5R10F6-v6.bin
SG-6000-X25812/X25803	SG6000-XN-5.5R10F6.img SG6000-XN-5.5R10F6-v6.img
SG-6000-X10800/X9180	SG6000-XL-5.5R10F6.bin SG6000-XL-5.5R10F6-v6.bin
SG-6000-X8180	SG6000-XM-5.5R10F6.bin SG6000-XM-5.5R10F6-v6.bin
SG-6000-X7180	SG6000-X7180-5.5R10F6.bin SG6000-X7180-5.5R10F6-v6.bin
SG-6000-X6150-GS	SG6000-X6150-GS-5.5R10F6.bin SG6000-X6150-GS-5.5R10F6-v6.bin
SG-6000-K9180	SG6000-K-1-

Platform Models	Images
	5.5R10F6.img SG6000-K-1- 5.5R10F6-v6.img
SG-6000-K2680/K2380	SG6000-K-2- 5.5R10F6.img SG6000-K-2- 5.5R10F6-v6.img
SG-6000-K6280-GS/K6580	SG6000-K-5- 5.5R10F6.img SG6000-K-5- 5.5R10F6-v6.img
SG-6000-K5680/K3680-GS/K3280/K2580/K2560/K1280	SG6000-K-4- 5.5R10F6.img SG6000-K-4- 5.5R10F6-v6.img
SG-6000-E5960/E5760 /E5660 /E5560 /E5568 /E5260 /E5268/E3965 /E5168	SG6000-M-2- 5.5R10F6.bin SG6000-M-2- 5.5R10F6-v6.bin
SG-6000-A2200 /A1800 /A1600 /E6360 /E6368 /E6160 /E6168 /E3960 /E3968 /E3662 /E3660 /E3668 /E2860 /E2868 /E2800 /E2300 /E1700/E1606 /E1600 /E1100 (WLAN) /E1100 (WLAN+3G-WCDMA) /E1100 (WLAN+3G-CDMA) /E1100 (3G-WCDMA)/E1100 (3G-CDMA)/E1100 (4G)	SG6000-M-3- 5.5R10F6.bin SG6000-M-3- 5.5R10F6-v6.bin

Platform Models	Images
/E1100 (WLAN+4G)	
SG-6000-VM01 /VM02 /VM04 /VM08	ARM: SG6000-CloudEdge-5.5R10F6-ARM-CLOUD.q-cow2/img SG6000-CloudEdge-5.5R10F6-ARM-CLOUD-v6.q-cow2/img SG6000-CloudEdge-5.5R10F6-ARM-KVM.qcow2/img SG6000-CloudEdge-5.5R10F6-ARM-KVM-v6.q-cow2/img
	X86: SG6000-CloudEdge-5.5R10F6 SG6000-

Platform Models	Images
	CloudEdge-5.5R10F6-v6 (Select the format based on requirements of different clouds. The formats include .img, .ova, .vhd, .qcow2, and .vmdk.)

New Features

ID	Description	Platform
Hardware		
41433	Support the Jumbo Frame function by SG-6000-K6280-GS.	K6280-GS
System		
39985	If the newly received TCP SYN packet matches a session that is in DELAYINVALIDATE, the system will delete that matched session and at the same time create a new session with the same quintuple for subsequent packet forwarding.	A, K, X, E, CloudEdge
41735	Support to obtain the SN of the power module by using the **show environment power** command.	A (A3800 and later), X8180, X9180, X10800,

ID	Description	Platform
		X25812, K9180
	Support to obtain the SN of fan by using the **show environment fan** command.	A (A3800 and later), X25812, X8180
41741	Support to disable or re-enable the specified SSH algorithm by using the CLI to avoid the impact on your business due to the security vulnerability of the SSH algorithm.	A, K, X, E, CloudEdge
38570	The device can act as an NTP server to provide the clock synchronization service to other clients.	A, K, X, E, CloudEdge
41745	Support email-based deployment. The administrator configures this function on HSM and sends the deployment configuration information to the email address of the deployment personnel via URL by email, implementing ZTP.	A (except A200G4B), K, X, E, CloudEdge
41747	Support to obtain the PN of the power module by using the **show environment power** command.	A (A3800 and later), X8180, X9180, X10800, K9180
	Support to obtain the PN of fan by using the **show environment fan** command.	A (A3800 and later), X8180
	Support to obtain the PN of the transceiver module by using the **show transceiver** command.	A, K, X, E, CloudEdge

ID	Description	Platform
41755	X8180 devices' 10GE (SFP+) optical port supports the **sfp-to-copper** command to reduce data rate optical to 100M.	X8180
41765	Supports to periodically refresh the output of the show command.	A, K, X, E, CloudEdge
35753/39056/39058	More models can send monitor data such as threat logs to the cloud platform and iSource. In this release, X-series models and SG-6000-K9180/K6580 support this function.	K9180, K6580, X
38556	Support to monitor and view the storage usage of Docker on the device.	A (except A2200, A1800, A1600, A200, A200G4B, A200W), CloudEdge
Network		
33389	Support to enable/disable the function of session termination log recording the TCP status via CLI.	A, K, X, E, CloudEdge
	The session details page support to clearing sessions and display the TCP status.	
	Support to clear the number of failed session resource allocations via CLI.	
35041	In scenarios where there is a device between the FTP server and the firewall that supports NAT but	

ID	Description	Platform
	not ALG, and the device has performed NAT translation on the FTP server, you can enable/disable the use of the server's external IP address to establish data connections to ensure normal data transmission.	
41808	Support to configure the VPN fragmentation method in global network parameters.	
	Support to view the currently used VPN fragmentation method.	
Policy		
41753	Add the Delay Address Update Time function. After you modify multiple addresses in the address book at a time, the system does not immediately synchronize the modified addresses to the policy referencing the address book. Instead, synchronization occurs after a specified delay period. This avoids slow configuration deployment due to frequent updates in address book members and improves the efficiency of updating policy configuration.	A, K, X, E, CloudEdge
41761	Support to configure session timeout in the policy rule. After the timeout period is reached, the session is disconnected.	
	Support to filter persistent-connection sessions on the session details page.	
38671	Support to configure the number of times of automatically detecting ARP table entries or disabling ARP automatic detection.	A, K, X, E, CloudEdge

ID	Description	Platform
Object		
41757	Support the **show track** command to view the configuration information of all track objects in the system.	A, K, X, E, CloudEdge
41767	Support a large number of NAT rules referencing the same object. When the referenced objecy changes, no IPC message blocking will occur.	
	Optimize the configuration deployment rate when a large number of NAT rules reference the same object.	
38974	• Support to bind **exclude port** based on SNAT rules. • Support to configure **exclude port group** via WebUI and bind **exclude port group** to the virtual router and SNAT rules.	A, K, X, E, CloudEdge
Authentication		
39815	HTTP(S) SMS gateway supports to configure the ESB protocol subtype to enable integration with the ESB SMS platform.	A, K, X, E, CloudEdge
40651	Optimize the AD Scripting for SSO and SSO Monitor for SSO functions. • Support the combined use of AD Scripting for SSO and SSO Monitor for SSO functions, where SSO Monitor users kick out of AD Script users when SSO Monitor users come	A, E, CloudEdge

ID	Description	Platform
	online. • AD Scripting for SSO parameters support to multiple firewall IP addresses. • AD Scripting for SSO support to track changes of user IP address.	
	Increase the maximum number of authenticated users that can be configured on some A-series devices.	A2710, A2700
Diagnosis		
36021	Support to configure the packet capture mode. By specifying the packet capture mode, you can capture data packets of all traffic on the interface or all data packets whose sessions are established and that meet the packet capture rules.	A, K, X, E, CloudEdge
HA		
41759	HA A/P mode supports to configure the HA base virtual MAC, which can reduce the maintenance difficulty on the basis of avoiding the duplication of system-generated HA base virtual MAC addresses.	A, K, X, E, CloudEdge
41775	In the scenario where both SNAT and DNAT are configured, the SIP call mechanism is optimized when a switchover is performed in HA A/P mode.	
Log		
41773	Session logs can be aggregated by source IP address and destination IP address.	A, X(only for

ID	Description	Platform
		devices of the above series installed with SSD), K, CloudEdge
VPN		
38128	VXLAN supports to reference the IPSec tunnel to encrypt VXLAN packets within IPSec packets. This ensures data security during VXLAN tunnel transmission.	A, K, X, E, CloudEdge
Threat Prevention		
41445	Support to upgrade certain A-series devices to the full-data IPS signature database.	A200, A200G4B, A200W, A1000, A1100
41437	Support to upgrade certain E-series devices to the full-data IPS signature database.	E1606, E1700, E2300, E2800, E2860, E2868, E3662, E3668, E3960, E3968, E3965, E5168, E5260, E5268, E5560, E5568, E5660, E5760, E5960

ID	Description	Platform
RESTful API		
41769	Allow you to configure address books based on geological country location by using RESTful API.	A, K, X, E, CloudEdge
41771	Support to query the total number of ARP entries and the number of used ARP entries by using RESTful API;	
	Support to query details about ARP entries by using RESTful API.	
33389	Support to clear all sessions or sessions of specified conditions by using RESTful API.	A, K, X, E, CloudEdge
	Support to view the TCP status of session details by using RESTful API.	
41759	Support to configure and view HA basic virtual MAC by using RESTful API.	A, K, X, E, CloudEdge
41808	Support to configure and view the VPN fragmentation method by using RESTful API.	A, K, X, E, CloudEdge
SNMP		
41451	Support to obtain traffic and session information of the top 32 users and top 32 applications in different time periods by using SNMP.	A, K, X, E, CloudEdge
41737	Support to obtain traffic and session information of address book in different time periods by using SNMP.	
41735	Support to obtain the overall power of the device by using SNMP.	A (A3800 and later), X8180,

ID	Description	Platform
		X9180, X10800, X25812, K9180
41751	Support to obtain the maximum bandwidth of the logical interface of the device by using SNMP.	A, K, X, E, CloudEdge
41763	Supports to get the real-time CPU core utilization and average utilization of CPU core in the last 1 minute/1 hour by using SNMP.	A, K9180, K6280-GS, K5680, K3680, K3280, K2680, K2580, K2560, K2380, X10800, X8180, E, CloudEdge
33389	Support to retrieve the total number of session resource allocation failures for the entire device by using the SNMP.	A, K, X, E, CloudEdge
29630	Support to view NAT rule hit statistics by using SNMP.	
41151	Support to retrieve alarm messages for OSPF/OSPFv3/BGP neighbor status and BFD session status change to DOWN by using SNMP.	

ID	Description	Platform
41157	Support to retrieve alarm messages for abnormal system process by using SNMP.	
41159	Support to retrieve the current concurrent connections and new session rate of NAT session by using SNMP.	

Known Issues

ID	Description	Platform
SSL VPN		
323249	When 360 Security Guard is installed on the PC, errors may be reported when you log in to the ZTNA or VPN client. Recommendation: Add "" directory to trusted zone.	A, K, E, X, CloudEdge
329424	If you want to install an earlier version of the SSL VPN client after the new version of the SSL VPN client is installed, uninstall the existing new version of the SSL VPN client first.	
287915	The resource list can be displayed on the latest version of the SSL VPN client (such as Windows/Android/IOS). If the number of resources in the list exceeds 20, compatibility issues may occur on the SSL VPN client of an earlier version. Solution: Upgrade the SSL VPN client (such as Windows/Android/IOS) to the latest version.	A, K, E, X, CloudEdge
333797/333798	If the device is not installed with an SSL VPN license and ZTNA license, the number of SSL VPN/ZTNA authorized users that you view by using the CLI and by using the WebUI may be inconsistent. Solution: The actual number of authorized users displayed on the	A, K, E, X, CloudEdge

ID	Description	Platform
	WebUI shall prevail.	
329186	When you log in to the latest version of the SSL VPN client for Android, you may not be able to select an installed certificate for connection configuration. Solution: Manually select an installed certificate.	A, K, E, X, CloudEdge
335090	If you install and use the latest version of the SSL VPN client for Windows on a low-specification PC, packet sending and receiving may be abnormal and the SSL VPN client may be disconnected when you download files.	A, K, E, X, CloudEdge
327602	When you uninstall the SSL VPN client for macOS, the client icon may be not removed from Launchpad and Dock.	A, K, E, X, CloudEdge
313034	If a default route is configured in the tunnel route for the firewall, you may not be able to access internal resources when you connect to the firewall by using the SSL VPN client for Android.	A, E, X, CloudEdge
334346/332-965	When the SSL VPN client for macOS is running, you may not be able to open the SSL VPN client UI or the SSL VPN client may be disconnected and not be able to be reconnected after waking up the MAC that is sleeping.	A, K, E, X, CloudEdge
335092	After the SPA function is enabled, the latest version of the Hillstone Secure Connect client may not be able to be automatically updated. Solution: After the SPA function is enabled, manually update the Hillstone Secure Connect client.	A, K, E, X, CloudEdge
323920	When PC in Windows 7 SP1 and later use the new Hillstone Secure	A, K, E,

ID	Description	Platform
	Connect client, an connection error may occur. Solution: For users of PC in Windows 7 SP1 and later, please visit https://sccup-date.hill-stonenet.com:1338/sslvpn/win7/download?patch=Windows6.1-KB2533623-x86 or https://sccup-date.hill-stonenet.com:1338/sslvpn/win7/download?patch=windows6.1-kb4474419-v3-x86 to download the patch package and manually install the patch.	X, CloudEd-ge
Network		
382629	Do not support to configure the wildcard "*" to match all domain names individually. For example, if you want to match ABC.com, you can not configure "*". Instead, you can configure "*.com".	A, K, E, X, CloudEd-ge
QoS		
251079	QoS does not support the user rate limit in the Peer-mode asym-metric routing scenario.	A, K, E, X, CloudEd-ge
Policy		
332856	When you add an aggregate policy, you cannot use the **aggregate-rule**{ **name** *name* | *id*} [**top** | **before** {**name***rule-name*| *id*} | **after** {**name***rule-name*| *id*}] command to specify the position of policy members within the aggregate policy.	A, K, E, X, CloudEd-ge

ID	Description	Platform
RESTful API		
348396	An error may occur when you view a single predefined application by using RESTful API.	A, K, E, X, CloudEdge
HA		
286815	When the backup device is upgraded from 5.5R6 to 5.5R10 in the HA AP environment while the master device is still in the 5.5R6 version, the backup device might not synchronize the user group and role information of online users on the master device.	A, K, E, X, CloudEdge
330370	In an HA AP environment, when upgrading the device from 5.5R6 to 5.5R10, if the backup device is upgraded to 5.5R10 while the master device is in 5.5R6, the backup device may fail to synchronize the Webauth online users from the master device.	
CloudEdge		
310941	If the system is not restarted after the installation of the new version of the platform license, previous version of the VSN platform license can still be viewed through CLI and its displayed VSN is incorrect.	CloudEdge

StoneOS 5.5R10F5

Release Overview

Release Date: March 22, 2024

This release provides 4 new features and 60 merged features. The key adjustment involves the following aspects:

- **Network**: IOC-A-F-4SFP+, IOC-A-F-8SFP+, and IOC-A-F-8GE support port mirroring. This function allows you to mirror the traffic of one interface to another interface (analytic interface) for analysis and monitoring.
- **Authentication**: Support to enable/disable SSL certificate verification. When the firewall is connected to the Active Directory/LDAP server by using SSL encryption, if you cannot obtain the server certificate, you can disable the SSL certificate verification function. This way, the firewall can be successfully connected to the authentication server without the need to import the certificate.
- **Threat Prevention**: Optimize the mechanism for generating service blacklist, real IP blacklist, MAC blacklist, IP reputation database logs of perimeter traffic filtering. Ensure that distributed devices send logs from the main control board so that each hit record generates only one aggregated log per minute.
- In addition, RESTful API is enhanced.

For description of all the functions, see New Features.

For the supplementary note for the new functions, refer to *New Features Guide for StoneOS 5.5R10F Releases*.

All released information: https://fr.hillstonenet.com/show_bug.cgi?id=40733

Inheritance & Merging Details of 5.5R10F5:

- Inherit all FRs and fixed bugs of 5.5R10F4;
- Merge all FRs, known issues, and fixed bugs of 5.5R10P5;
- Merge FR37812 and FR38301 from 5.5R10F3.X;
- Merge FR38691, FR38695, FR38699, and FR39511 from 5.5R10F4.X;
- Merge FR38559 from 5.5R10P4.X;

Platforms and Images

Platform Models	Images
SG-6000-A7600/A6800/A5860/A5800/A5660/A5600/A5560	SG6000-A-1-

Platform Models	Images
/A5555/A5500/A5260/A5255/A5200/A5160/A5155/A5100 /A3815/A3800/A3700/A3615/A3600/A3000/A2815/A2800 /A2715/A2700/A2600/A2000/A1100/A1000	5.5R10F5.img SG6000-A-1-5.5R10F5-v6.img
SG-6000-A200/A200G4 (4G)/A200W (WLAN) /A200WG4 (WLAN+4G)	SG6000-A-3-5.5R10F5.bin SG6000-A-3-5.5R10F5-v6.bin
SG-6000-X25812/X25803	SG6000-XN-5.5R10F5.img SG6000-XN-5.5R10F5-v6.img
SG-6000-X10800/X9180	SG6000-XL-5.5R10F5.bin SG6000-XL-5.5R10F5-v6.bin
SG-6000-X8180	SG6000-XM-5.5R10F5.bin SG6000-XM-5.5R10F5-v6.bin
SG-6000-X7180	SG6000-X7180-5.5R10F5.bin SG6000-X7180-5.5R10F5-v6.bin
SG-6000-E5960/E5760 /E5660 /E5560 /E5568 /E5260 /E5268/E3965 /E5168	SG6000-M-2-5.5R10F5.bin SG6000-M-2-5.5R10F5-

Platform Models	Images
	v6.bin
SG-6000-A2200 /A1800 /A1600 /E6360 /E6368 /E6160 /E6168 /E3960 /E3968 /E3662 /E3660 /E3668 /E2860 /E2868 /E2800 /E2300 /E1700/E1606 /E1600 /E1100 (WLAN) /E1100 (WLAN+3G-WCDMA) /E1100 (WLAN+3G-CDMA) /E1100 (3G-WCDMA) /E1100 (3G-CDMA) /E1100 (4G) /E1100 (WLAN+4G)	SG6000-M-3-5.5R10F5.bin SG6000-M-3-5.5R10F5-v6.bin
SG-6000-VM01 /VM02 /VM04 /VM08	SG6000-CloudEdge-5.5R10F5 SG6000-CloudEdge-5.5R10F5-v6

New Features

ID	Description	Platform
Hardware		
39205	Support the 2U Bypass modules IOC-A-4MM-BE and IOC-A-4SM-BE for A-series.	A5860, A5660, A5560, A5260, A5160
33051	Support to switch the working mode of the SIOM module for different business scenarios to enhance device performance.	X
WebUI		

ID	Description	Platform
39197	The session details page of policy/NAT/user monitor supports to display the number of sent packets, the number of received packets, sent traffic, and received traffic.	A, X, E, CloudEdge
System		
39239	Optimize the function of connecting to Hillstone cloud platform, including: • Optimize the configuration page of the "Log Report" and "Monitor Data Report" functions. You can configure these functions on CloudView and receive the function configuration deployed from CloudView. • Update the user experience plan by adding *Description for Uploaded Content*, which can be viewed on the WebUI. • Expand the control scope	A, X, E, CloudEdge

ID	Description	Platform
	of the cloud configuration function. With the cloud configuration function enabled, you can modify the upload type of firewall logs and monitoring data.	
39235	Support to use the **show ssh** command to view the number of SSH users that are currently online.	
39189	Add the retry mechanism after configuration deployment fails. This reduces the number of direct error reports and manual retries and improves the success rate of configuration deployment.	
	Add the **exec retrytime** command, which is used to specify the maximum retry time of configuration deployment. Default value: 5 seconds.	
36289	Add the **fragment centralized-mode** command, which is used to configure whether IP fragmented packets are reassembled	X

ID	Description	Platform
	in the IOM/SIOM module to enable normal traffic forwarding when fragmented packets enter the device from different IOM/SIOM modules.	
Network		
37259	IOC-A-F-4SFP+, IOC-A-F-8SFP+, and IOC-A-F-8GE supports port mirroring, which allows you to mirror the traffic of one interface to another interface (analytic interface) for analysis and monitoring.	SG-6000-A3815/A3615/A2815/A2715
Policy		
39241	The session limit function supports to limit the number of new sessions per second.	A, X, E, CloudEdge
Object		
39225	Add the ordered address book function. You can save address members based on their configuration orders.	A, X, E, CloudEdge
NAT		
39191	The NAT function supports to reference an ordered address	A, X, E, CloudEdge

ID	Description	Platform
	book to realize one-to-one translation of multiple IP addresses in a single NAT rule based on the specified IP order.	
Routing		
38301	Support the BGP Route Reflector function.	A, X, E, CloudEdge
Authentication		
35529	Support to enable/disable SSL certificate verification. When the firewall is connected to the Active Directory/LDAP server by using SSL encryption, if you cannot obtain the server certificate, you can disable the SSL certificate verification function. This way, the firewall can be successfully connected to the authentication server without the need to import the certificate.	A, X, E, CloudEdge
ALG		
38559	Support SIP Record-Route in multi-URI format for ALG.	A, X, E, CloudEdge
39245	After the device is enabled with	

ID	Description	Platform
	the DNS ALG function, the system supports to configure whether DNAT participates DNS rewriting by using the WebUI or CLI. This prevents DNS response packets from mistakenly matching DNAT rules when only DNS rewriting rules need to be matched, resulting in abnormal service access.	
HA		
39135/39213 / 39215/39217/ 39219/39221/ 39223	Optimize the HA batch synchronization mechanism. When the configuration of the backup device is more than that of the main device is more than that of the master device or the configuration order is not consistent with that of the master device, the batch synchronization can be successful.	A, X, E, CloudEdge
39187	Support to monitor the working status of HA master and backup devices by using BFD, and realize fast master/backup switchover when the device	

ID	Description	Platform
	fails.	
VPN		
39185	In the SSL VPN SMS authentication scenario, the SMS gateway of the SGIP protocol type supports the configuration of SMS templates.	A, X, E, CloudEdge
License		
39127	Optimize the trial license expiration rules of Intrusion Prevention, Anti Virus, Botnet Prevention. If you apply for a Version 3 trial license, the functions become unavailable after expiration. Note: You can use the **show license** *license-name* command to view the license version.	A, X, E, CloudEdge
Monitor		
38691	• Support the Language content language field for report tasks. You can specify the language type of the report content, which can be Chinese or English;	A, X, E, CloudEdge

ID	Description	Platform
	• Support a predefined time period for the statistical time period of data of reports that are immediately generated; • Support to create, delete, edit, and query report templates by using the RESTful API; • Support to create, delete, edit, and query report tasks by using the RESTful API; • Support to query report status and stop report task by using the RESTful API; • Support to query the generation record of report files by using the RESTful API.	
	• Support to query and delete existing report files and modify the status of report files by using the	CloudEdge, E (only for devices that are installed with SSD), A1600/A1800/A2200 installed with SSD and other A-series models (except

ID	Description	Platform
	RESTful API.	A200/A200G4/A200W/A200WG4）, X8180/X25812/X25803
Log		
37812	• Support to store URL logs of certain devices to the local disk. • Support to configure the percentage of disk space occupied by URL logs.	CloudEdge, A (except A2200, A1800, and A1600), X
39133	Support to display attack results on the threat log and threat event pages and view log entries of specified attack results through filter conditions.	A, X, E, CloudEdge
39261	For threat logs related to weak password, the administrator can view weak password details in the threat logs.	
39157	Support to display the attacker IP and victim IP in threat logs.	
	Support to filter and view logs based on the attacker and victim.	
	Support to block an attacker IP by adding it to blacklist.	
39139	Support to view threat logs of	

ID	Description	Platform
	specified associated accounts and authenticated users through filter conditions.	
	Support to display usernames used in attacks in the threat log.	
38903	Support to configure the log ID format as hexadecimal or decimal by using the CLI. The default format is decimal.	
37325	Support to configure different Facility fields for event logs and traffic logs to distinguish between them.	
39169	Support to display threat data in threat logs.	A, E (only for devices that are installed with SSD), X25812, X25803, X8180, CloudEdge
Threat Prevention		
38749	Optimize the mechanism for generating service blacklist, real IP blacklist, MAC blacklist, IP reputation database logs of perimeter traffic filtering. Ensure that distributed devices send logs from the main control board so that each hit record generates only one aggregated log per minute.	X

ID	Description	Platform
39137/39165/39163	Support to map the detected suspicious behaviors to the MITRE ATT&CK® model and display MITRE ATT&CK® tactic and technical information in threat Logs and iCenter > Threat, helping you identify suspicious behaviors in a better way.	A, X, E, CloudEdge
	Support to upgrade the MITRE ATT&CK®Knowledge Base.	
39151/39153	Support the HTTP Plain Text Detection function. The system checks the password field in the HTTP packet. If the password is not encrypted, an alarm log is generated.	
	Support the HTTP password protection function. You can customize fields that tell information about the username, password, successful login, and failed login in the actual HTTP packet.	
39161	Optimize the detection rate of the IPS engine.	
39181/39211	Support to configure the IPS	

ID	Description	Platform
	HTTP multiple decoding function by using the CLI, which can decode HTTP messages encoded by URL or Unicode to enhance the detection and protection capability of the system.	
39141	Optimize the IPS engine to support base64 encoding scanning and parsing.	
38899	Support the IPS packet capture function for the X8180, X25803, and X25812 platforms.	X8180, X25803, X25812
RESTful API		
39087	Support to create, query, update, renew, delete, enable, and disable API Token by using the RESTful API.	A, X, E, CloudEdge
38695	Support to create, query, renew, and delete application groups and application filtering groups by using the RESTful API.	
38699	Support to configure iQoS by using the RESTful API.	
39511	Support to configure links and view sampled traffic information	

ID	Description	Platform
	of interfaces, including latency, packet loss rate, and jitter, by using the RESTful API.	
39197	Support to obtain the number of sent packets, received packets, sent traffic, and received traffic of sessions by using RESTful API.	
39245	Support to enable or disable the DNAT participating in DNS rewriting function by using RESTful API.	
SNMP		
39235	Support to obtain the number of current SSH connections and maximum SSH connections by using SNMP.	A, X, E, CloudEdge

Known Issues

ID	Description	Platform
SSL VPN		
323249	When 360 Security Guard is installed on the PC, errors may be reported when you log in to the ZTNA or VPN client. Recommendation: Add "" directory to trusted zone.	A, E, X, CloudEdge
329424	If you want to install an earlier version of the SSL VPN client after	

ID	Description	Platform
	the new version of the SSL VPN client is installed, uninstall the existing new version of the SSL VPN client first.	
287915	The resource list can be displayed on the latest version of the SSL VPN client (such as Windows/Android/IOS). If the number of resources in the list exceeds 20, compatibility issues may occur on the SSL VPN client of an earlier version. Solution: Upgrade the SSL VPN client (such as Windows/Android/IOS) to the latest version.	A, E, X, CloudEdge
333797/333798	If the device is not installed with an SSL VPN license and ZTNA license, the number of SSL VPN/ZTNA authorized users that you view by using the CLI and by using the WebUI may be inconsistent. Solution: The actual number of authorized users displayed on the WebUI shall prevail.	A, E, X, CloudEdge
329186	When you log in to the latest version of the SSL VPN client for Android, you may not be able to select an installed certificate for connection configuration. Solution: Manually select an installed certificate.	A, E, X, CloudEdge
335090	If you install and use the latest version of the SSL VPN client for Windows on a low-specification PC, packet sending and receiving may be abnormal and the SSL VPN client may be disconnected when you download files.	A, E, X, CloudEdge
327602	When you uninstall the SSL VPN client for macOS, the client icon may be not removed from Launchpad and Dock.	A, E, X, CloudEdge
313034	If a default route is configured in the tunnel route for the firewall,	A, E, X,

ID	Description	Platform
	you may not be able to access internal resources when you connect to the firewall by using the SSL VPN client for Android.	CloudEdge
334346/332-965	When the SSL VPN client for macOS is running, you may not be able to open the SSL VPN client UI or the SSL VPN client may be disconnected and not be able to be reconnected after waking up the MAC that is sleeping.	A, E, X, CloudEdge,
335092	After the SPA function is enabled, the latest version of the Hillstone Secure Connect client may not be able to be automatically updated. Solution: After the SPA function is enabled, manually update the Hillstone Secure Connect client.	A, E, X, CloudEdge
323920	When PC in Windows 7 SP1 and later use the new Hillstone Secure Connect client, an connection error may occur. Solution: For users of PC in Windows 7 SP1 and later, please visit https://sccup-date.hillstonenet.com:1338/sslvpn/win7/download?patch=Windows6.1-KB2533623-x86 or https://sccup-date.hillstonenet.com:1338/sslvpn/win7/download?patch=windows6.1-kb4474419-v3-x86 to download the patch package and manually install the patch.	A, E, X, CloudEdge
Network		
382629	Do not support to configure the wildcard "*" to match all domain names individually. For example, if you want to match ABC.com, you can not configure "*". Instead, you can configure "*.com".	A, E, X, CloudEdge

ID	Description	Platform
QoS		
251079	QoS does not support the user rate limit in the Peer-mode asymmetric routing scenario.	A, E, X, CloudEdge
Policy		
332856	When you add an aggregate policy, you cannot use the **aggregate-rule** { **name** *name* | *id*} [**top** | **before** {**name***rule-name*| *id*} | **after** {**name***rule-name*| *id*}] command to specify the position of policy members within the aggregate policy.	A, E, X, CloudEdge
RESTful API		
348396	An error may occur when you view a single predefined application by using RESTful API.	A, E, X, CloudEdge
HA		
286815	When the backup device is upgraded from 5.5R6 to 5.5R10 in the HA AP environment while the master device is still in the 5.5R6 version, the backup device might not synchronize the user group and role information of online users on the master device.	A, E, X, CloudEdge
330370	In an HA AP environment, when upgrading the device from 5.5R6 to 5.5R10, if the backup device is upgraded to 5.5R10 while the master device is in 5.5R6, the backup device may fail to synchronize the Webauth online users from the master device.	
CloudEdge		
310941	If the system is not restarted after the installation of the new version of the platform license, previous version of the VSN platform	CloudEdge

ID	Description	Platform
	license can still be viewed through CLI and its displayed VSN is incorrect.	

StoneOS 5.5R10F4

Release Overview

Release Date: December 22, 2023

This release provides 43 new features and 79 merged features. The key adjustment involves the following aspects:

- **IoT endpoint identification function is enhanced**: The IoT security protection function supports the local IoT asset identification capability. The firewall extracts IoT device fingerprint information from network traffic and sends it to the local asset identification module. By using multiple identification techniques to identify IoT devices, the local asset identification module returns identification results to the firewall.
- **ZTNA capability is enhanced**: For application resources, you can configure consecutive ports, which facilitates policy configuration for administrators; support to automatically obtain the icon of application resources, which will be displayed on the ZTNA Portal page; support to configure ChineseOS endpoint tags, which allows you to manage endpoint information about the ChineseOSs Kylin V10 and UOS 20.
- Support to configure the OAuth2 authentication server. You can use OAuth2 authentication in the user access scenarios of SSL VPN, ZTNA, and WebAuth.
- Add the container management function, which allows you to create, start/stop. and remove a container and import image files.

- The firewall can be worked with Honeypot. With the deployment environment of the firewall, you can construct various service traps, diverting network attack traffic to honeypot services, thereby conducting attack forensics, ultimately strengthening the protection of real assets.
- Support continuous proactive detection of links. You can continuously detect the latency, packet loss, and jitter data of the links for the destination IP address/domain name.
- The URL filtering module supports the Restful API function. You can use this function to implement custom development work of automated O&M. This simplifies the maintenance process of Internet behavior control.
- After 30 days of disconnection between CloudEdge and LMS, the device is optimized to lock configuration instead of automatic restart.

For description of all the functions, see New Features.

For the supplementary note for the new functions, refer to *New Features Guide for StoneOS 5.5R10 F Releases*.

All released information: https://fr.hillstonenet.com/show_bug.cgi?id=39099

Inheritance & Merging Details of 5.5R10F4:

- Inherit all FRs and fixed bugs of 5.5R10F3;
- Merge all FRs, known issues, and fixed bugs of 5.5R10P4;
- Merge FR34797 from 5.5R10P3;

Platforms and Images

Platform Models	Images
SG-6000-A5555/A5500/A5255/A5200/A5155/A5100 /A3800/A3700/A3600/A3000/A2800 /A2700/A2600/A2000/A1100/A1000 /A7600/A6800/A5860/A5800/A5660/A5600/A5560/	SG6000-A-1-5.5R10F4.img SG6000-A-1-5.5R10F4-v6.img

Platform Models	Images
SG-6000-A200/A200G4 (4G)/A200W (WLAN) /A200WG4 (WLAN+4G)	SG6000-A-3-5.5R10F4.bin SG6000-A-3-5.5R10F4-v6.bin
SG-6000-X25812/X25803	SG6000-XN-5.5R10F4.img SG6000-XN-5.5R10F4-v6.img
SG-6000-X10800/X9180	SG6000-XL-5.5R10F4.bin SG6000-XL-5.5R10F4-v6.bin
SG-6000-X8180	SG6000-XM-5.5R10F4.bin SG6000-XM-5.5R10F4-v6.bin
SG-6000-X7180	SG6000-X7180-5.5R10F4.bin SG6000-X7180-5.5R10F4-v6.bin
SG-6000-X6150-GS	SG6000-X6150-GS-5.5R10F4.bin SG6000-X6150-GS-5.5R10F4-v6.bin
SG-6000-E5960/E5760 /E5660 /E5560 /E5568 /E5260 /E5268/E3965 /E5168	SG6000-M-2-5.5R10F4.bin SG6000-M-2-5.5R10F4-v6.bin
SG-6000-E6360 /E6368 /E6160 /E6168 /E3960 /E3968 /E3662 /E3660 /E3668 /E2860 /E2868 /E2800 /E2300 /E1700/E1606 /E1600 /E1100 (WLAN) /E1100 (WLAN+3G-WCDMA) /E1100 (WLAN+3G-CDMA) /E1100 (3G-WCDMA) /E1100 (3G-CDMA) /E1100 (4G)	SG6000-M-3-5.5R10F4.bin SG6000-M-3-5.5R10F4-v6.bin

Platform Models	Images
/E1100 (WLAN+4G)	
SG-6000-VM01 /VM02 /VM04 /VM08	SG6000-CloudEdge-5.5R10F4 SG6000-CloudEdge-5.5R10F4-v6

New Features

ID	Description	Platform
Hardware		
36579	For X-series, support the high-end distributed firewall SG-6000-X25803, which supports two SCM expansion slots, two power modules, and supports three general expansion slots (for SIOM modules).	X25803
36839	Support the A-series platforms SG-6000-A5860, SG-6000-A5660, SG-6000-A5560, SG-6000-A5260, and SG-6000-A5160.	A5860, A5660, A5560
32496	For 1GE(SFP) optical port of certain A-series devices, you can set the data rate to 100 Mbps. After the data	A5500/A5200/A5100/A3800/A3700/A360-0/ A3000/A2800/A2700

ID	Description	Platform
	rate of the optical port is backward switched, it can be inserted only into the 1GE (SFP) single-mode transceiver module and corresponding optical fibers.	
System		
36591	Support the feedback template. When you use the device, if you find that the information in the license is different from the actual information or encounter other issues related to license, you can use the template to enter a feedback, and then copy and send the feedback to the email address.	A, X, E, CloudEdge
36743	• Add the **exec ssh generate-host-key rsa modulus** {**1024** | **2048** | **4096**} command, which is used to specify the length of the key generated	

ID	Description	Platform
	by the RSA algorithm. • Support to view the number of bits of the key generated by the RSA algorithm and various algorithms supported by the SSH protocol by using the **show ssh** command.	
36521	Support to configure the IPv6 address when CloudEdge is connected to LMS.	CloudEdge
36543	VSYS supports DHCP ZTP.	A
34281	Support to connect to iSource. After the firewall device is connected to iSource as a network device, it supports to send threat logs and evidence packets to iSource for analysis.	A, E, X, CloudEdge
27416/37341	Support the Docker man-	A

ID	Description	Platform
	agement function. You can create Docker, allocate system resources for Docker, import Docker image file, and run container application based on Docker in the system.	
29058/34005/31650/32980/34207/34211/34209	• Support to upload IoT asset data information in the device to iSource. • Support to upload IoT report data and IoT asset data to Hillstone cloud platform.	A, E, X
Policy		
36593	When services are referenced by policy rules, you can filter policy rules by service content with a fuzzy search.	A, E, X, CloudEdge
	A service contains information such as protocol type and port number. You can filter service by service con-	

ID	Description	Platform
	tent such as name, protocol type, and port number with a fuzzy search.	
36657	Support policy for access control of HTTP/HTTPS based on domain/host book without DNS.	A, X, E, CloudEdge
29058/34005/31650/32980/34207/34211/34209	Support to configure a policy rule based on device object.	A, E, X
NAT		
36669	Expand the range of translated IP addresses for SNAT/BNAT rules in dynamic port mode.	A, X, E, CloudEdge
Monitor		
36703	Long-term monitor statistics can be ranked by "Concurrent Sessions" and "New Sessions". You can query statistics based on concurrent sessions and new sessions of IP/application.	A (only for devices that are installed with SSD)

ID	Description	Platform
29969	Support to perform persistent link quality detection by using link detection rule, including latency, jitter, and packet loss rate.	A, E, X, CloudEdge
Routing		
29749	Support to configure the multicast service reflection (MSR) function on the Vif interface.	A, E, CloudEdge
36859	Support to configure the multicast source address of non-direct multicast source, which ensures that the multicast source DR and multicast source multicast across network segments.	A, E, X, CloudEdge
IPv6		
36557	Optimize the refreshing mechanism for IPv6 ND table entries. You can configure the aging time of ND table entries. ND table entries that exceed the aging time can be either	A, E, X, CloudEdge

ID	Description	Platform
	deleted directly or subjected to validity detection.	
AAA Server		
33185	• The system allows you to configure an OAuth2 server. • Webauth supports OAuth2 authentication.	A, E, X, CloudEdge
VPN		
33723	Hillstone Secure Connect client supports OAuth2 authentication.	A, E, X, CloudEdge
35629	Optimize the SSL VPN and ZTNA function. You can specify user group or role when configuring tunnel route. After you successfully log in to the SSL VPN/ZTNA client, the firewall will distribute the tunnel route of the user group or role to which the user belongs.	
32641	L2TP VPN supports user	

ID	Description	Platform
	going offline alarm. You can configure an L2TP VPN instance to reference a user going offline alarm profile, which enables you to monitor offline users.	
	Support to query the number of L2TP VPN online users by using SNMP.	
	Support to query L2TP VPN online user by using "public IP".	
ZTNA		
29000	Support to configure an endpoint tag of ChineseOS; Support to manage endpoint items of ChineseOS Kylin V10 and UOS 20.	A, E, X, CloudEdge
35263	Support to upload the logo image of application resource or automatically obtain the logo image by configuring a URL. The logo image will be displayed on the ZTNA Portal page.	

ID	Description	Platform
31579	Support to configure a port range for application resource entries of ZTNA.	
Cloud Platform		
30073	Support to upload UDP DNS traffic to the cloud.	A, E, CloudEdge
User Authentication		
34797	The maximum number of authenticated users of SSO Monitor increases from 4,096 to 8,096.	E2860, E2868
RESTful API		
36583	Support to export the signature database list file of the device in the .csv format by using RESTful API.	A, E, X, CloudEdge
36551	Support to view the real-time utilization of each CPU of the device by using RESTful API.	
36657	Add the domain and domain_book fields to the policy configuration interface.	

ID	Description	Platform
36671	Support to enable reverse shell detection and protection by using RESTful API.	
36673	Support to cancel or restore configuring direct route first by using RESTful API.	
34325/35049	Support custom statistical set for any data type and organization structure by using RESTful API.	
33288	• Support to configure custom URL type, URL, URL blacklist/whitelist, and URL filtering template by using Restful API. • Support to query predefined URL type and predefined keyword type by using Restful API.	
33220	Support to configure the contain self-traffic function	

ID	Description	Platform
	of packet capture by using RESTful API.	
34301	Support to configure the response traceroute function by using RESTful API.	
35627	Support to configure a custom HA MAC address of interface by using RESTful API.	
36411	Support to configure the first data proxy function of interface by using RESTful API.	
36441	Support to configure the Virtual Wire function of tunnel interface by using RESTful API.	
Log		
36631	• Support to store NAT logs and session logs to the local database. • Support to configure the percentage of	A and X (only for devices that are installed with SSD), CloudEdge

ID	Description	Platform
	disk space occupied by NAT logs and session logs.	
35781	Add filter conditions "AAA:user@host" and "application" for session logs; Support to view session logs of user or application of specified AAA server by using the WebUI.	A, E, X, CloudEdge
33269	• Add the SMS Send Type field for log configuration. You can select SMS Gateway or SMS Modem. • Besides SMS modem, you can send SMS messages of log messages to mobile phone by using SMS gateway.	A, E, X, CloudEdge
Threat Prevention		
36683	Support to manually import/export, automatically import, query, and delete the botnet pre-	A, X, CloudEdge

ID	Description	Platform
	vention blacklist library.	
36687	Optimize the name of threat logs and threat events of botnet prevention.	A, X, E, CloudEdge
36699	Increase the capacity of botnet prevention blacklist and whitelist library, and manage this capacity by using the shared resource configuration method.	
36691	• Optimize the intrusion prevention/detection profile configuration page, which consists of the basic information, vulnerability protection, web protection, password protection, and abnormal traffic sections. In addition, a navigation bar is added. • Support to	A, E, X, CloudEdge

ID	Description	Platform
	enable/disable the brute force function of all types of protocols at one click. • Support to configure suspicious UA detection by using the WebUI.	
36695	The Attack Defense function supports to block network scan behaviors.	
33244	Add the honeypot function. The firewall can interact with Hillstone Deception Decoy System (Honeypot). By connecting the honeypot system to the firewall device and configuring trap rules, attacker IP addresses that match the trap rules are diverted to the honeypot system for containment. This prevents attacks on your real business environment.	
36663	• Support to enable	A (except A200), X25803, X25812,

ID	Description	Platform
	and disable the intelligence file engine detection function. • Support to update and download the anti-virus intelligence file engine database. • Support to import the anti-virus intelligence file engine database file from your PC.	CloudEdge
	• Support to distribute CPU resources for intelligence file engine by using the CLI. • Support to enable and disable the intelligence file engine multi-process function by using the CLI.	A (except A200), CloudEdge
36513	• Support to replace	A, X

ID	Description	Platform
	the IP address in the DNS response packet with the Sink-hole IP address. When the com-promised host accesses the IP address again, this host can be detected by using the source IP address of gen-erating logs; • Support to view the family of DGA domains by using threat logs and iCenter; • Support to upload DGA detection res-ults to the cloud plat-form, where the model is continually optimized to further eliminate false pos-itives; • Optimize the detec-	

ID	Description	Platform
	tion rate of DGA domains based on root type and normal domain deformation; Reduce the false positive rate of domain names in the whitelist. Note: You need to upgrade to the latest signature database.	
DNS		
36601	• Support to add IPv6 DNS mapping entries to the cache. You can view, edit, and delete them. • Support exact search for IPv4 and IPv6 domains, which helps you filter DNS cache information of the specified domain.	A, E, X, CloudEdge
36837	Support to configure the maximum interval for the	

ID	Description	Platform
	device to send DNS requests to the DNS server by using the **ip domain interval-time** command.	
36597	• Support to configure TTL for a single domain that is resolved in active mode when the TTL value exceeds the specified value, the system sends a DNS request to the DNS server again. • Support to configure TTL for manually added DNS mapping entries. When the device enables the DNS proxy function, this TTL value is returned to the client if the DNS request hits the local cache.	
36595	Expand the custom retention time range of DNS res-	

ID	Description	Platform
	olution configuration to 60 to 86,400 seconds.	
36835	Support to configure the UDP packet length that can be parsed by DNS snooping in active mode by using the CLI.	
36759	Support the Secure DNS function. Integrated with 360 Secure DNS service, the firewall enhances the detection and protection capabilities of malicious domains while improving the transmission security.	A, E, X, CloudEdge
Interface		
36547	• Support to view the total received packets and sent packets of interfaces by using RestFul API. • Support to view the total received packets and sent packets of interfaces on the homepage of the	A, E, X, CloudEdge

ID	Description	Platform
	WebUI.	
35627	Support to configure the custom HA MAC address of interface, which is used to forward traffic of the master device in HA scenarios.	
36411	Support to enable the first data proxy function of interface, which is used to obtain and record domain information in HTTP/HTTPS packets of interface traffic.	
36441	Optimize the Virtual Wire configuration. You can configure the tunnel interface as a Virtual Wire interface pair.	
Network		
32310	Support the application layer fast forward function. When only the Intrusion Prevention function at the application layer is enabled and the protocol max scan	A7600, A6800, X

ID	Description	Platform
	length configured in IPS Profile is reached, traffic at the application layer will no longer be forwarded to the SSM module or CPU for parsing and processing. This enhances the device performance.	
33220	Optimize the online packet capture task. After you enable the contain self-traffic function, captured packets contain traffic sent and received by the device itself.	A, E, X, CloudEdge
34301	Support to enable/disable the response Traceroute function, which is used to prevent the device from responding to traceroute traffic that does not belong to the device itself. This way, the IP address of the device is hidden, which reduces the possibility of the device being dis-covered and attacked.	

ID	Description	Platform
SMS Gateway		
33271	Support to configure the HTTP(S) SMS gateway attribute to an array object. The parameter will be stored in array.	A, E, X, CloudEdge
32841	Support to configure a node name for the HTTP (S) SMS gateway attribute. The "ZGC" protocol sub-type is added, which allows you to connect the Hill-stone device to the ZGC SMS platform.	
MIB		
35733	Add the time attribute to trap information, which is used to indicate the time when the trap information occurs.	A, E, X, CloudEdge
36571	Support the trap inform-ation that fan, temperature, and power supply return to normal.	A (except A1100, A1000, A200, A200W, A200G4, and A200WG4), E
	Support the trap inform-ation that temperature and	A1100, A1000, A200, A200W, A200G4, A200WG4

ID	Description	Platform
	power supply return to normal.	
36573	Support the trap information that CPU utilization, memory status, disk space, and interface bandwidth utilization return to normal.	A, CloudEdge, E
	Support the trap information of disk utilization. **Note**: Only devices installed with SSD support the trap information of disk utilization.	A, E
CloudEdge		
37217	After 30 days of disconnection between CloudEdge and LMS, the device is optimized to lock configuration instead of automatic restart.	CloudEdge
Object		
29058/34005/31650/32980/34207/34211/34209	Add the device object configuration. You can categorize one or more IoT devices into a device col-	A, E, X

ID	Description	Platform
	lection based on multiple dimensions of the device (including the man-ufacturer, type, model, and operating system of the device). In addition, you can view IP details of IoT device that is mapped based on device object attribute.	
IoT Monitor		
29058/34005/31650/32980/34207/34211/34209	• Optimize the asset identification type and the type of IoT devices that can be identified. The local asset identification type is supported. • Support the "external" local asset identification. You can install an asset identification pro-gram on the virtual machine and identify IoT assets by using	A, E, X

ID	Description	Platform
	the asset identification system deployed on the virtual machine. • Optimize the identification list. Support to configure identification list of the IP, MAC, or IP/MAC types. For security zones that are enabled with the IoT monitor function and bound with identification list, the system can identify IoT devices for its traffic based on the identification list. • Support to identify IoT devices for security zone traffic based on identification list. Support to reference the	

ID	Description	Platform
	MAC address in the traffic. • Support to parse IoT monitor traffic of DHCP and HTTP.	
	Support the built-in local asset identification. You can use the Docker management function of firewall to deploy the asset identification system within the firewall, which enables you to identify IoT assets.	A (A2600 and later)

Known Issues

ID	Description	Platform
SSL VPN		
323249	When 360 Security Guard is installed on the PC, errors may be reported when you log in to the ZTNA or VPN client. Recommendation: Add "" directory to trusted zone.	A, E, X, CloudEdge
329424	If you want to install an earlier version of the SSL VPN client after the new version of the SSL VPN client is installed, uninstall the existing new version of the SSL VPN client first.	
287915	The resource list can be displayed on the latest version of the SSL	A, E, X,

ID	Description	Platform
	VPN client (such as Windows/Android/IOS). If the number of resources in the list exceeds 20, compatibility issues may occur on the SSL VPN client of an earlier version. Solution: Upgrade the SSL VPN client (such as Windows/Android/IOS) to the latest version.	CloudEdge
333797/333798	If the device is not installed with an SSL VPN license and ZTNA license, the number of SSL VPN/ZTNA authorized users that you view by using the CLI and by using the WebUI may be inconsistent. Solution: The actual number of authorized users displayed on the WebUI shall prevail.	A, E, X, CloudEdge
329186	When you log in to the latest version of the SSL VPN client for Android, you may not be able to select an installed certificate for connection configuration. Solution: Manually select an installed certificate.	A, E, X, CloudEdge
335090	If you install and use the latest version of the SSL VPN client for Windows on a low-specification PC, packet sending and receiving may be abnormal and the SSL VPN client may be disconnected when you download files.	A, E, X, CloudEdge
327602	When you uninstall the SSL VPN client for macOS, the client icon may be not removed from Launchpad and Dock.	A, E, X, CloudEdge
313034	If a default route is configured in the tunnel route for the firewall, you may not be able to access internal resources when you connect to the firewall by using the SSL VPN client for Android.	A, E, X, CloudEdge
334346/332-	When the SSL VPN client for macOS is running, you may not be	A, E, X,

ID	Description	Platform
965	able to open the SSL VPN client UI or the SSL VPN client may be disconnected and not be able to be reconnected after waking up the MAC that is sleeping.	CloudEdge,
335092	After the SPA function is enabled, the latest version of the Hillstone Secure Connect client may not be able to be automatically updated. Solution: After the SPA function is enabled, manually update the Hillstone Secure Connect client.	A, E, X, CloudEdge
323920	When PC in Windows 7 SP1 and later use the new Hillstone Secure Connect client, an connection error may occur. Solution: For users of PC in Windows 7 SP1 and later, please visit https://sccup-date.hillstonenet.com:1338/sslvpn/win7/download?patch=Windows6.1-KB2533623-x86 or https://sccup-date.hillstonenet.com:1338/sslvpn/win7/download?patch=windows6.1-kb4474419-v3-x86 to download the patch package and manually install the patch.	A, E, X, CloudEdge
Network		
382629	Do not support to configure the wildcard "*" to match all domain names individually. For example, if you want to match ABC.com, you can not configure "*". Instead, you can configure "*.com".	A, E, X, CloudEdge
QoS		
251079	QoS does not support the user rate limit in the Peer-mode asymmetric routing scenario.	A, E, X, CloudEd-

ID	Description	Platform
		ge
Policy		
332856	When you add an aggregate policy, you cannot use the **aggregate-rule**{ **name** *name* | *id*} [**top** | **before** {**name***rule-name*| *id*} | **after** {**name***rule-name*| *id*}] command to specify the position of policy members within the aggregate policy.	A, E, X, CloudEdge
RESTful API		
348396	An error may occur when you view a single predefined application by using RESTful API.	A, E, X, CloudEdge
HA		
286815	When the backup device is upgraded from 5.5R6 to 5.5R10 in the HA AP environment while the master device is still in the 5.5R6 version, the backup device might not synchronize the user group and role information of online users on the master device.	A, E, X, CloudEdge
330370	In an HA AP environment, when upgrading the device from 5.5R6 to 5.5R10, if the backup device is upgraded to 5.5R10 while the master device is in 5.5R6, the backup device may fail to synchronize the Webauth online users from the master device.	
CloudEdge		
310941	If the system is not restarted after the installation of the new version of the platform license, previous version of the VSN platform license can still be viewed through CLI and its displayed VSN is incorrect.	CloudEdge

StoneOS 5.5R10F3

Release Overview

Release Date: September 28, 2023

This release provides 13 new features and 134 merged features. The key adjustment involves the following aspects: in terms of system, the firewall supports to connect to and log in to other SSH or Telnet servers as an SSH or Telnet client; in terms of object, you can customize geographical location of the IP address based on your requirements; in terms of authentication, you can reference the configured certificate chain in the system in the HTTPS Web authentication scenario; in terms of cloud platform, the system can execute corresponding configuration commands based on the configuration scripts deployed by the cloud platform or HSM, and the system can upload interface statistics to CloudView; in terms of CloudEdge, you can specify the HA peer IP address and next-hop gateway to implement HA negotiation and synchronization across Layer-3 network, and you can deploy HA Peer Actve-Actve(A/A) mode on Alibaba Cloud to implement HA negotiation and synchronization across availability zones (AZs). In addition, logging and RESTful API are enhanced.

For description of all the functions, see New Features.

For the supplementary note for the new functions, refer to *New Features Guide for StoneOS 5.5R10 F Releases*.

All released information: https://fr.hillstonenet.com/show_bug.cgi?id=37445

Inheritance & Merging Details of 5.5R10F3:

- Inherit all FRs and fixed bugs of 5.5R10F2;
- Merge all FRs and fixed bugs of 5.5R10P3;
- FR34135 is merged from 5.5R9F1.7;
- FR32946 is merged from 5.5R10F1.X;
- FR32838 is merged from 5.5R9F2.X;

Platforms and Images

Platform Models	Images
SG-6000-A7600/A6800/A5800/A5600/A5550/A5500/A5250/A5200/A5150/A5100/A3800/A3700/A3600/A3000/A2800/A2700/A2600/A2000/A1100/A1000	SG6000-A-1-5.5R10F3.img SG6000-A-1-5.5R10F3-v6.img
SG-6000-A200/A200G4 (4G)/A200W (WLAN)/A200WG4 (WLAN+4G)	SG6000-A-3-5.5R10F3.bin SG6000-A-3-5.5R10F3-v6.bin
SG-6000-X20812	SG6000-XN-5.5R10F3.img SG6000-XN-5.5R10F3-v6.img
SG-6000-X10800/X9180	SG6000-XL-5.5R10F3.bin SG6000-XL-5.5R10F3-v6.bin
SG-6000-X8180	SG6000-XM-5.5R10F3.bin SG6000-XM-5.5R10F3-v6.bin
SG-6000-X7180	SG6000-X7180-5.5R10F3.bin SG6000-X7180-5.5R10F3-v6.bin

Platform Models	Images
SG-6000-X6150-GS	SG6000-X6150-GS-5.5R10F3.bin SG6000-X6150-GS-5.5R10F3-v6.bin
SG-6000-E5960/E5760 /E5660 /E5560 /E5568 /E5260 /E5268/E3965 /E5168	SG6000-M-2-5.5R10F3.bin SG6000-M-2-5.5R10F3-v6.bin
SG-6000-VM01 /VM02/VM04 /VM08	SG6000-CloudEdge-5.5R10F3 SG6000-CloudEdge-5.5R10F3-v6

New Features

ID	Description	Platform
Hardware		
34579	Support the X-series platform SG-6000-X20812.	X20812
34581	Support the A-series platform SG-6000-A5550, SG-6000-A5250, and SG-6000-A5150.	A
System		
32838	The firewall can connect to and log in to other SSH or Telnet servers as an SSH or Telnet client.	A, E, X, CloudEdge

ID	Description	Platform
34725	Support to view SNMP OID statistics details and status by enabling/disabling the SNMP OID statistics function.	
34885	Support to specify the CPU threshold for automatic backup of configuration files to the FTP server. After specifying the threshold, when the CPU utilization exceeds the threshold, configuration files will not be sent to the FTP server during that cycle. The system will wait until the next cycle to send configuration files again.	
34599	• Support to configure HTTP content security policy to improve Web security. • Support to view the configuration of content security policy by using the **show http** command.	
34707	Support DHCP ZTP. For A-series devices, the default configuration of the ethernet0/3 interface of factory default device is enhanced. Specifically, the zone configuration is added and DHCP configuration and Option 60 configuration are enabled for the default configuration. Once the device is powered on, it automatically obtains and loads the configuration file via DHCP to complete automatic deployment.	A
	Support the function of enabling or disabling the DHCP client to carry Option 60 (vendor class	A, E, X, CloudEdge

ID	Description	Platform
	identifier) by using the CLI; Support to customize Option 60.	
Object		
29675/32730	• Support the custom IP geolocation function. You can customize the geographical location of IP addresses. For example, when the geographical location of the IP address is invalid, you can customize this information. • When you query the geographical location of IP addresses, the system preferentially queries the custom geographical location.	A, E, X, CloudEdge
Policy		
34497	Security policy can match post-DNAT destination address.	A, E, X, CloudEdge
NAT		
34849	SNAT supports the NPTv6 mode to implement IPv6 address translation.	A, X, E, CloudEdge
SNMP		
34723	• Support to download the MIB file to your PC by using the WebUI. • Support to export the MIB file to a specified server by using the CLI.	A, X, E, CloudEdge
34851	Support to obtain the BGP neighbor information	

ID	Description	Platform
	by using SNMP, including the IP address, status, AS number, and instance VRouter of the BGP neighbor.	
Network		
34821	After enabling the Layer 4 check function, the system checks TCP protocol packets flowing through Layer 4. If an exception is detected from a TCP packet, this packet is dropped.	A, E, X, CloudEdge
34809	Support to configure the same MAC address for the Layer-3 tunnel interface by cloning the MAC address.	CloudEdge
34709	X-series devices support to prioritize BGP, Track ICMP, and Track DNS packets to enhance device stability.	X
Authentication		
33357	Support to reference the configured certificate chain in the system in HTTPS Web authentication scenarios.	A, E, X, CloudEdge
VPN		
34807/34815	Support to configure the Layer-3 tunnel interface for VXLAN.	CloudEdge
	In non-root VSYS, the egress interface of the VXLAN static tunnel can be configured as a sub-interface.	A, E, X, CloudEdge
34775	• Support to configure the IPSec-XAUTH	

ID	Description	Platform
	IPv6 address pool. • Support to filter dial-in users by dial-in user-name and private IP address. • Support to view the IPv6 address of dialed-in user on the authenticated user page of monitor.	
34799/34865	• Support to manually check the update on the Windows/Linux/macOS client. • Support to view the download source of the client by using the **show secure-connect client-info** command. • Support to configure the download source of the Windows/Linux/macOS client by using the **secure-connect update-url** command.	
ZTNA		
34731	Support to output logs of endpoint tags to device hard disks.	X20812
HA		
34559	Support to obtain the device status of the HA group in HA Active-Passive (A/P) mode by using SNMP, including the HA status of the peer device, HA status of the master device and backup device, and the number of master/backup	A, X, E, CloudEdge

ID	Description	Platform
	status changes.	
34863	• Add the dedicated virtual router "ha-link-vr" for HA, and the zone HA is bound to "ha-link-vr" by default. • The virtual router "ha-link-vr" cannot be modified or deleted.	
34729	Support to configure IPv6 address for virtual IP address of the HSVRP group.	
Threat Prevention		
34873	Support IP verification. For defense against DNS Reply Flood and DNS Query Flood attacks, when the number of DNS packets exceeds the threshold, dynamic verification is applied to source IP addresses. Traffic from verified IP addresses is allowed for a specified period; For the SYN-Proxy and SYN-Cookie functions, when the number of SYN packets exceeds the threshold, successfully proxy-verified IP addresses are directly allowed instead of being redundantly proxied within a specified period.	A, E, X, CloudEdge
Monitor		
34557	• Support to view the total rate of new IPv4/IPv6 sessions or the total number of concurrent IPv4/IPv6 sessions by using the WebUI; • Support to view the total rate of new	A, E, X, CloudEdge

ID	Description	Platform
	IPv4/IPv6 sessions or the total number of concurrent IPv4/IPv6 sessions by using SNMP.	
34845	• The device monitor supports to collect statistics for and display total traffic, interface traffic, and zone traffic of IPv4 and IPv6 respectively. • Support to view IPv4 or IPv6 statistics of specified statistical set by using CLI. • Support to view IPv4/IPv6 or non-IP packet traffic of the specified interface. Support to view traffic statistics of the specified interface within the last 30 days. • Support to obtain the total IPv4 or IPv6 traffic rate, ingress interface IPv4 or IPv6 traffic rate, egress interface IPv4 or IPv6 traffic rate by using SNMP.	
Diagnosis		
34801	• Support to configure the packet capture task in non-root VSYS. • Support to configure the total number of packets that can be captured for the packet capture task. During the effective period (packet capture time) of the packet capture task, if the number of packets captured	A, E, X, CloudEdge

ID	Description	Platform
	reaches the configured number, the system automatically stops capturing packets. • Support to configure the maximum percentage of memory that the packet capture file can use for devices without hard disks. When the percentage of memory usage exceeds the upper limit, the system automatically stops capturing packets.	
34881	X-series devices support the data packet path detection function.	X
Cloud Platform		
29695	Support to execute command configuration based on the configuration script deployed by the cloud platform or HSM.	A, E, X, CloudEdge
34135	Support to upload interface statistics to CloudView, including the maximum upstream rate, maximum downstream rate, average upstream rate, and average downstream rate of each interface. Support to upload statistics based on the upload cycle of CloudView.	
34787/34789	Unify the control tunnel and data transmission tunnel between the device and cloud platform and support to synchronize full threat information to the cloud platform. This improves the efficiency of security operations.	A, E, CloudEdge

ID	Description	Platform
34495	Support to install all license files by using CloudView and upload the latest license to CloudView when the license changes.	A, E, X, CloudEdge
34785	Support to upload configuration files to CloudView and restore configuration files by using CloudView.	
34769	Support to upload the maximum number of SNAT rules that can be configured and the number of configured rules to the cloud platform.	
34779	Support to upload the ARP table, MAC table, session resource usage to the cloud platform. Note: For X-series devices, only the total sessions of all business modules can be uploaded.	
34777	Support to upload the policy rule resource usage to the cloud platform, including the number of policy rules that can be configured and the number of configured policy rules.	
34771	Support to upload the utilization and temperature of each CPU, the total memory size, and the used memory size to the cloud platform.	X
34735/34773/34783/34781/34499	• Support to upload monitor data of specified type to the cloud platform, including the traffic ranking, session ranking, URL ranking, device information, and VPN statistics. • Support to upload logs of specified type to	A, E, CloudEdge

ID	Description	Platform
	the cloud platform, including event logs, threat logs, configuration logs, network logs, cloud sandbox logs, operation logs, content filtering logs, online behavior auditing logs, session logs, and NAT logs.	
RESTful API		
34399	Support to create, edit, delete, and query intrusion prevention whitelist by using RESTful API.	A, E, X, CloudEdge
34409	Support to query hotspot threat intelligence by using RESTful API. You can filter hotspot threat intelligence, configure hotspot threat intelligence, and enable hotspot threat intelligence push by publish time.	
34413	Support to aggregate botnet prevention logs by using RESTful API.	
34407	Support to query top 10 threats by using RESTful API, and support to filter top 10 threats by destination IP address, source IP address, threat name, and time.	A, E, X, CloudEdge
34411	Support to delete NICs by using RESTful API.	
33229	Support to bind and unbind SSL VPN user and host ID by using RESTful API.	
34821	Support to enable/disable the function of checking TCP protocol packets flowing through Layer 4 by using RESTful API.	

ID	Description	Platform
34801	• Support to deploy and delete packet capture tasks and packet capture filtering rules, and query packet capture status by using RESTful API. • Support to query and deploy the global configuration of packet capture by using RESTful API, including the memory usage threshold and maximum percentage of available memory usage. • Support to enable/disable packet capture by using RESTful API.	
34815	Support to bind the VXLAN tunnel to Layer-3 zone by using RESTful API.	CloudEdge
34819	Support to view the packet loss ranking of each module and the total number of packets lost of all modules by using RESTful API.	A, CloudEdge
34533	Support to add/delete/edit aggregate policy, add/delete member for aggregate policy, and view hit analysis results by using RESTful API.	A, E, X, CloudEdge
34535	Support to add/delete/edit zone, view the zone list and zone details, and import/export zone certificate by using RESTful API.	
34829	Support to upgrade version by using RESTful API.	
34833	Support to configure/modify/delete VSYS quota	

ID	Description	Platform
	and view the VSYS configuration list by using RESTful API.	
34541	Support to configure/export debug logs and view debug log configuration by using RESTful API.	
34839	Support to add/edit IPv4 address book based on country/area by using RESTful API.	
34843	• Support to view/edit the geography signature database by using RESTful API. • Support to locally and remotely upgrade the geography signature database by using RESTful API.	
34561	Support to view/add/delete IPv6 neighbor cache table by using RESTful API.	
Capacity		
34727	The total number of NAT that can be configured within all VSYS is consistent with the number of NAT that can be configured for the device.	A, E, X, CloudEdge
34871	Optimize the VSYS capacity logic. The number of VSYS that can be configured for the device does not contain the root VSYS.	
Log		
32946	• Support to view the destination interface of session logs by using WebUI; • Support to view session logs of specified	A, E, X, CloudEdge

ID	Description	Platform
	source interface or destination interface by using WebUI.	
34571	• For device without hard disks, event logs, configuration logs, and network logs can be stored to EMMC. • For device with hard disks, event logs, configuration logs, network logs, and threat logs can be stored to hard disks.	X20812
CloudEdge		
29095	Support to implement HA negotiation and synchronization across Layer-3 networks by specifying the HA peer IP address and next-hop gateway.	CloudEdge
32100	Support to deploy HA Peer Actve-Actve(A/A) mode on Alibaba Cloud to implement HA negotiation and synchronization across AZs.	

Known Issues

ID	Description	Platform
SSL VPN		
323249	When 360 Security Guard is installed on the PC, errors may be reported when you log in to the ZTNA or VPN client. Recommendation: Add "" directory to trusted zone.	A, E, X, CloudEdge
329424	If you want to install an earlier version of the SSL VPN client after the new version of the SSL VPN client is installed, uninstall the	

ID	Description	Platform
	existing new version of the SSL VPN client first.	
287915	The resource list can be displayed on the latest version of the SSL VPN client (such as Windows/Android/IOS). If the number of resources in the list exceeds 20, compatibility issues may occur on the SSL VPN client of an earlier version. Solution: Upgrade the SSL VPN client (such as Windows/Android/IOS) to the latest version.	A, E, X, CloudEdge
333797/333798	If the device is not installed with an SSL VPN license and ZTNA license, the number of SSL VPN/ZTNA authorized users that you view by using the CLI and by using the WebUI may be inconsistent. Solution: The actual number of authorized users displayed on the WebUI shall prevail.	A, E, X, CloudEdge
329186	When you log in to the latest version of the SSL VPN client for Android, you may not be able to select an installed certificate for connection configuration. Solution: Manually select an installed certificate.	A, E, X, CloudEdge
335090	If you install and use the latest version of the SSL VPN client for Windows on a low-specification PC, packet sending and receiving may be abnormal and the SSL VPN client may be disconnected when you download files.	A, E, X, CloudEdge
327602	When you uninstall the SSL VPN client for macOS, the client icon may be not removed from Launchpad and Dock.	A, E, X, CloudEdge
313034	If a default route is configured in the tunnel route for the firewall, you may not be able to access internal resources when you connect	A, E, X, CloudEd-

ID	Description	Platform
	to the firewall by using the SSL VPN client for Android.	ge
334346/332-965	When the SSL VPN client for macOS is running, you may not be able to open the SSL VPN client UI or the SSL VPN client may be disconnected and not be able to be reconnected after waking up the MAC that is sleeping.	A, E, X, CloudEd-ge,
335092	After the SPA function is enabled, the latest version of the Hill-stone Secure Connect client may not be able to be automatically updated. Solution: After the SPA function is enabled, manually update the Hillstone Secure Connect client.	A, E, X, CloudEd-ge
323920	An connection error may occur when Windows 7 SP1 and later ver-sion use the new Hillstone Secure Connect client. Solution: For users of Windows 7 SP1 and later versions, visit https://sccup-date.hill-stonenet.com:1338/sslvpn/win7/download?patch=Windows6.1-KB2533623-x86 or https://sccup-date.hill-stonenet.com:1338/sslvpn/win7/download?patch=windows6.1-kb4474419-v3-x86 to download the patch package as required and manually install the package.	A, E, X, CloudEd-ge
QoS		
251079	QoS does not support the user rate limit in the Peer-mode asym-metric routing scenario.	A, E, X, CloudEd-ge

ID	Description	Platform
Policy		
332856	You cannot specify the position of policy members in aggregated policy by using the **aggregate-rule**{ **name** *name* | *id*} [**top** | **before** {**name***rule-name*| *id*} | **after** {**name***rule-name*| *id*}] command.	A, E, X, CloudEdge
RESTful API		
348396	An error may occur when you view a single predefined application by using RESTful API.	A, E, X, CloudEdge
HA		
286815	When the backup device is upgraded from 5.5R6 to 5.5R10 in the HA AP environment while the master device is still in the 5.5R6 version, the backup device might not synchronize the user group and role information of online users on the master device.	A, E, X, CloudEdge
330370	When the backup device is upgraded from 5.5R6 to 5.5R10 in the HA AP environment while the master device is still in the 5.5R6 version, the backup device might not synchronize the Webauth online user information on the master device.	
CloudEdge		
310941	If the system is not restarted after the installation of the new version of the platform license, previous version of the VSN platform license can still be viewed through CLI and its displayed VSN is incorrect.	CloudEdge

StoneOS 5.5R10F2

Release Overview

Release Date: June 26, 2023

This release provides 9 new features and 13 merged features. The key adjustment involves the address book function and HA function. The address book function is enhanced. When you configure an address book of the Country/Region type, if you select CN China, you can further configure the province and city. In the meantime, you can add or exclude address book members in batches; The HA function is enhanced. The system supports the VRRP function, which allows for mutual negotiation with other manufacturer's devices that support the standard VRRP protocol, and enables timely switching of business traffic to a backup device in case of failure in the default gateway of the network. This implements redundant backup of the gateway and ensures reliable network communication.

For description of all the functions, see New Features.

For the supplementary note for the new functions, refer to *New Features Guide for StoneOS 5.5R10 F Releases*.

All released information: https://fr.hillstonenet.com/show_bug.cgi?id=34949

Inheritance & Merging Details of 5.5R10F2:

- Inherit all FRs and fixed bugs of 5.5R10F1;
- Merge all FRs and fixed bugs of 5.5R10P2;
- FR31298 is merged from 5.5R9T;
- FR33677 is merged from 5.5R10F1.X;
- FR30772 is merged from 5.5R9F4.X;
- FR31348 and FR30698 are merged from 5.5R9F5.X;
- FR33155 are merged from 5.5R9F6.X;
- FR30690 is merged from 5.5R10B.

Platforms and Images

Platform Models	Images
SG-6000-A7600/A6800/A5800/A5600/A5500/A5200 /A5100/A3800/A3700/A3600 /A3000/A2800/A2700/A2600/A2000/A1100/A1000	SG6000-A-1-5.5R10F2.img SG6000-A-1-5.5R10F2-v6.img
SG-6000-A200/A200W (WLAN)	SG6000-A-3-5.5R10F2.bin SG6000-A-3-5.5R10F2-v6.bin
SG-6000-X10800/X9180	SG6000-XL-5.5R10F2.bin SG6000-XL-5.5R10F2-v6.bin
SG-6000-X8180	SG6000-XM-5.5R10F2.bin SG6000-XM-5.5R10F2-v6.bin
SG-6000-X7180	SG6000-X7180-5.5R10F2.bin SG6000-X7180-5.5R10F2-v6.bin
SG-6000-X6150-GS	SG6000-X6150-GS-5.5R10F2.bin SG6000-X6150-GS-5.5R10F2-v6.bin
SG-6000-E5960/E5760 /E5660 /E5560 /E5568 /E5260 /E5268/E3965 /E5168	SG6000-M-2-5.5R10F2.bin SG6000-M-2-5.5R10F2-v6.bin
SG-6000-E6360 /E6368 /E6160 /E6168 /E3960 /E3968 /E3662 /E3660 /E3668 /E2860 /E2868 /E2800 /E2300 /E1700/E1606 /E1600 /E1100 (WLAN) /E1100 (WLAN+3G-WCDMA)	SG6000-M-3-5.5R10F2.bin SG6000-M-3-5.5R10F2-v6.bin

Platform Models	Images
/E1100 (WLAN+3G-CDMA) /E1100 (3G-WCDMA) /E1100 (3G-CDMA) /E1100 (4G) /E1100 (WLAN+4G)	
SG-6000-VM01 /VM02 /VM04 /VM08	SG6000-CloudEdge-5.5R10F2 SG6000-CloudEdge-5.5R10F2-v6

New Features

ID	Description	Platform
System		
33495	X7180 devices support CPU cache error monitoring alarm function. When the number of CPU Cache Error reaches the specified alarm threshold, the device will generate logs.	X7180
Object		
20494	When you create/edit an address book, you can perform the following operations: • Add or exclude address book members in batches; • Query address book member based on the address book member type or content filtering;	A, E, X, CloudEdge
26501	• Enhance the IP geographical database by annotating the geographical information of IP addresses within China to the provincial	

ID	Description	Platform
	and city levels; • Allow you to view the geographical location of the IP address by running the **show geoip-info** command; • Allow you to upgrade the IP geographical database by using WebUI.	
30222	When you configure an address book of the Country/Region type, if you select CN China, you can further configure the province and city.	
30221/30223/30224	The policy rule, static IP blacklist of perimeter traffic filtering (PTF), and policy-based route can reference address book configured with province and city.	
Policy		
32682	Support to configure custom attributes for policy and query policy based on the attributes.	A, E, X, CloudEdge
VPN/ZTNA		
30690	Support the SSL VPN/ZTNA dedicated line function. After you log in to SSL VPN/ZTNA, you can access only internal network resources of specified network segment in the tunnel routing but not Internet resources.	A, E, X, CloudEdge
HA		
30772	Support the VRRP function. The VRRP function	A, E, CloudEdge

ID	Description	Platform
	adopts the standard VRRP protocol, allowing for mutual negotiation with other manufacturer's devices that support the standard VRRP protocol. When the default gateway of network fails, the VRRP function can switch business traffic to the backup device in a timely manner to implement redundant backup of the gateway and ensures reliable network communication. The VRRP function does not support configuration synchronization or session synchronization. It only provides redundant backup in case of gateway failures.	
Authentication		
30698	StoneOS can actively query the user group and role mapping of authenticated users on the AD/LDAP server by using SSO Monitor to implement network access control based on user groups and roles.	A, E, X, CloudEdge
31348	Support the SSO Web function. The SSO Web client (a third-party authentication system) can send user login/logout messages and user information update messages to the system via HTTP(S) RESTful API. The system extracts user authentication information from the messages and can actively query the user group and role mapping of authenticated users on the AD/LDAP server. This enables SSO and network access control	A, E, X, CloudEdge

ID	Description	Platform
	based on user groups and roles.	
Threat Prevention		
33499	Adds hot threat intelligence to X-series devices.	X
Monitoring and Logs		
30225/30623	Support to view source and destination regions of threat logs and filter threat logs based on the source and destination regions.	A, E, X, CloudEdge
33497	Adds the function of importing logs and reports to local hard disk toX8180 devices, supported log types include event logs, threat logs, network logs, and configuration logs.	X8180
33501	Logs sent to the Syslog Server display host name, rather than device SN.	A, E, X, CloudEdge
RESTful API		
33677	Allow you to create, edit, delete, and query micro-policy.	A, E, X, CloudEdge

Known Issues

ID	Description	Platform
SSL VPN		
323249	When 360 Security Guard is installed on the PC, errors may be reported when you log in to the ZTNA or VPN client. Recommendation: Add "" directory to trusted zone.	A, E, X, CloudEdge

ID	Description	Platform
329424	If you want to install an earlier version of the SSL VPN client after the new version of the SSL VPN client is installed, uninstall the existing new version of the SSL VPN client first.	
287915	The resource list can be displayed on the latest version of the SSL VPN client (such as Windows/Android/IOS). If the number of resources in the list exceeds 20, compatibility issues may occur on the SSL VPN client of an earlier version. Solution: Upgrade the SSL VPN client (such as Windows/Android/IOS) to the latest version.	A, E, X, CloudEdge
333797/333798	If the device is not installed with an SSL VPN license and ZTNA license, the number of SSL VPN/ZTNA authorized users that you view by using the CLI and by using the WebUI may be inconsistent. Solution: The actual number of authorized users displayed on the WebUI shall prevail.	A, E, X, CloudEdge
329186	When you log in to the latest version of the SSL VPN client for Android, you may not be able to select an installed certificate for connection configuration. Solution: Manually select an installed certificate.	A, E, X, CloudEdge
335090	If you install and use the latest version of the SSL VPN client for Windows on a low-specification PC, packet sending and receiving may be abnormal and the SSL VPN client may be disconnected when you download files.	A, E, X, CloudEdge

ID	Description	Platform
327602	When you uninstall the SSL VPN client for macOS, the client icon may be not removed from Launchpad and Dock.	A, E, X, CloudEdge
313034	If a default route is configured in the tunnel route for the firewall, you may not be able to access internal resources when you connect to the firewall by using the SSL VPN client for Android.	A, E, X, CloudEdge
334346/332965	When the SSL VPN client for macOS is running, you may not be able to open the SSL VPN client UI or the SSL VPN client may be disconnected and not be able to be reconnected after waking up the MAC that is sleeping.	A, E, X, CloudEdge,
335092	After the SPA function is enabled, the latest version of the Hillstone Secure Connect client may not be able to be automatically updated. Solution: After the SPA function is enabled, manually update the Hillstone Secure Connect client.	A, E, X, CloudEdge
QoS		
251079	QoS does not support the user rate limit in the Peer-mode asymmetric routing scenario.	A, E, X, CloudEdge
HA		
286815	When the backup device is upgraded from 5.5R6 to 5.5R10 in the HA AP environment while the master device is still in the 5.5R6 version, the backup device might not synchronize the user group and role information of online users on the master device.	A, E, X, CloudEdge

ID	Description	Platform
CloudEdge		
310941	If the system is not restarted after the installation of the new version of the platform license, previous version of the VSN platform license can still be viewed through CLI and its displayed VSN is incorrect.	CloudEdge

StoneOS 5.5R10F1

Release Overview

Release Date: May 6, 2023

This release provides 5 new features and 107 merged features. The key functions include:

- Add the **OSPF GR** function. In a network environment running the OSPF protocol, OSPF GR can ensure that network traffic is not interrupted during HA switchover;
- Optimize **the method to obtain DNS proxy server in the DNS proxy rule**. You can automatically obtain the DNS server configured by the system or learned through DHCP as the DNS proxy server by using Use System;
- Enhance the **Authentication** function. You can create AD/LDAP accounts and configure account expiration, configure expiration time for locally synchronized AD/LDAP accounts, and import or export AD/LDAP accounts;
- Enhance the **IPv6 over IPv4 Tunnel** function. You can configure the IPv6 over IPv4 tunnel by using WebUI, including automatic 6to4 tunnel, manual 6to4 tunnel, ISATAP tunnel, and 6RD tunnel;
- Enhance the **SSL VPN and ZTNA** function. You can specify the allowed types of the SSL VPN/ZTNA client, which can be one or more of the Windows client, Android client, iOS client, macOS client, and Linux client.

For description of all the functions, see New Features.

The supplementary note for the new functions refer to *New Features Guide for StoneOS 5.5R10 F Releases*.

All released information: https://fr.hillstonenet.com/show_bug.cgi?id=33364

Inheritance & Merging Details of 5.5R10F1:

- Inherit all FRs and fixed bugs of 5.5R10;
- Merge all FRs and fixed bugs of 5.5R10P1;
- FR27137 is merged from 5.5R8B;
- FR28717 is merged from 5.5R8P11M7;
- FR31250, FR29993, FR31113, and FR30819 are merged from 5.5R9F4.X;
- FR31248, FR30703, FR31434, and FR30700 are merged from 5.5R9F5.X;
- FR31928, FR31929, FR31930, FR31931, FR28335, FR31932, FR31933, FR31935, FR31936, FR31937, FR31938, FR31939, FR31940, FR31941, FR31942, FR31943, FR28151, FR28153, FR31944, FR32043, FR31945, FR31946, FR28812, FR28816, FR28818, and FR31947 are merged from 5.5R9F3;
- FR31949, FR31950, FR31951, FR28386, FR28336, FR28553, FR28568, FR28633, FR31952, FR31953, FR29373, FR29366, FR29357, FR29359, FR29582, FR31954, FR31955, FR31956, FR31957, FR31958, FR31959, FR31960, FR31961, FR31964, FR31962, FR31963, FR28614, FR31966, FR31967, FR31968, FR31969, FR31970, FR31971, FR31972, FR31973, FR31975, FR31976, FR31977, FR31978, and FR31979 are merged from 5.5R9F4;
- FR29024, FR29580, FR31980, FR29690, FR29789, FR31981, FR31982, FR30490, FR31983, FR28438, FR28440, FR31984, FR31985, FR31987, FR31988, FR31989, FR31990, FR31991, FR31992, FR31993, FR31994, FR31995, and FR31996 are merged from 5.5R9F5;

- FR31997, FR31998, FR31999, FR32000, and FR32001 are merged from 5.5R9F6;
- FR32644 and FR32645 are merged from 5.5R10P1.

Platforms and Images

Platform Models	Images
SG-6000-A7600/A6800/A5800/A5600/A5500 /A5200/A5100/A3800/A3700/A3600 /A3000/A2800/A2700/A2600 /A2000/A1100/A1000	SG6000-A-1-5.5R10F1.img SG6000-A-1-5.5R10F1-v6.img
SG-6000-A200/A200W (WLAN)	SG6000-A-3-5.5R10F1.bin SG6000-A-3-5.5R10F1-v6.bin
SG-6000-X10800/X9180	SG6000-XL-5.5R10F1.bin SG6000-XL-5.5R10F1-v6.bin
SG-6000-X8180	SG6000-XM-5.5R10F1.bin SG6000-XM-5.5R10F1-v6.bin
SG-6000-X7180	SG6000-X7180-5.5R10F1.bin SG6000-X7180-5.5R10F1-v6.bin
SG-6000-X6150-GS	SG6000-X6150-GS-5.5R10F1.bin SG6000-X6150-GS-5.5R10F1-v6.bin
SG-6000-E5960/E5760/E5560 /E5568 /E5260/E5268/E3965/E5168	SG6000-M-2-5.5R10F1.bin SG6000-M-2-5.5R10F1-v6.bin
SG-6000-E6360/E6368/E6160/E6168/E3960/E3968 /E3662/E3660/E3668/E2860/E2868 /E2800 /E2300/E1700/E1606/E1600/E1100 (WLAN)	SG6000-M-3-5.5R10F1.bin SG6000-M-3-5.5R10F1-v6.bin

Platform Models	Images
/E1100 (WLAN+3G-WCDMA) /E1100 (WLAN+3G-CDMA) /E1100 (3G-WCDMA) /E1100 (3G-CDMA)/E1100 (4G) /E1100 (WLAN+4G)	
SG-6000-VM01/VM02/VM04 /VM08	SG6000-CloudEdge-5.5R10F1 SG6000-CloudEdge-5.5R10F1-v6

New Features

ID	Description	Platform
Hardware		
29580	On the SG-6000-X9180 device where a 1 TB hard disk is installed, the disk capacity shows 930 G when the hard disk information is viewed through the WebUI or the **show disk** command.	X9180
31999	A-series devices supports 4 T SSD.	A (only for A-series devices that are installed with SSD)
System		
31930	Allow you to use the configuration file with the latest timestamp in the USB flash drive as the system boot file.	A, E, X, CloudEdge
31993/31994	Support to shut down E-series device through the **shutdown** command.	E
29993	Support to upgrade multiple signature databases	A, E, X, CloudEdge

ID	Description	Platform
	with the same software version and same-series device by using local upgrade.	
27137	Support the TSO/LRO function. By using NIC, TCP data is aggregated or sliced for forwarding. This improves the system's ability to receive TCP packets and reduces CPU load.	CloudEdge
31949	Add the SSL proxy domain whitelist signature database and support automatic updates for the database.	A, E, X, CloudEdge
29359	Allow you to upload the reason why an IPsec-VPN connection is closed to HSM.	
31984	The WebUI of devices for overseas markets supports Portuguese.	A (except A200/A200W)
31992	Support for inconsistent Engine ID of the master and backup devices, ensuring trap host can receive trap alarms during the HA switchover with SNMPv3 Trap function enabled.	A, E, X, CloudEdge
31995	Support to export tech-support files of all hardware modules via the **export tech-support** command.	X
31996	Support for custom modification of the product name on the login page.	A, E, X, CloudEdge
31998	10 G interfaces support Auto Tuning. If the interface status is abnormal, the interface parameters can be adjusted through Auto Tuning to	A (except A200/A200W), X (except X7180)

ID	Description	Platform
	effectively reduce the bit error ratio (BER) of the receiving end.	
32001	Support to disable or enable TCP packet timestamp through CLI.	A, E, X
Routing		
21986	Support the **OSPF GR** function. In a network environment running the OSPF protocol, OSPF GR can ensure that network traffic is not interrupted during HA switchover.	A, E, X, CloudEdge
31953	Support MLD and IPv6 PIM multicast functions.	
31983	Support to configure PIM and PIMv6 through WebUI.	
31964	• For route entries that meet the match conditions, you can configure communities attributes based on the tag value of static routes when these static routes are referenced by BGP. At most 8 communities attributes can be configured. • Display the custom communities attribute in the AA:NN format when you use the show command to view the BGP communities attribute.	
Policy		
31928	Support the Traffic Statistics function of Policy Assistant, which can be used to collect statistics	A, E, X, CloudEdge

ID	Description	Platform
	of the traffic extracted by Policy Assistant, including the number of hits, the number of upstream packets, the number of downstream packets, the number of upstream bytes, and the number of downstream bytes.	
31929	Support the Traffic Statistics function of policies, which can be used to collect statistics of the system traffic that hits policy rules, including the number of upstream packets, the number of downstream packets, the number of upstream bytes, and the number of downstream bytes.	
28440	Commands can be used to: • view statistics on policy rule hits, including rule ID, hit counts, first-hit time, last-hit time, days since last-hit time, policy created time, and policy status (enabled/disabled); • filter/clear, and sort statistics on policy rule hits.	
31985	Add the filtering condition User. When filtering policies by User, you can perform fuzzy query against user/ user group/ role or precise query against user/ user group to filter out policies.	
31962	Allow you to add a single IP address to the dynamic IP blacklist and specify the blocked	

ID	Description	Platform
	period with session limit.	
Network		
31946	The interface that uses DHCP to obtain a dynamic IP address can send option 26 request packets to the server. This way, MTU assigned by the server can be obtained.	A, E, X, CloudEdge
31950	Add the local ARP proxy function. You can view whether the local ARP proxy of an interface is enabled by using the CLI.	
28633	The system name in the device LLDP information can change with the configured host name.	
31980/31978	A-series devices support external 4G modules of ZTE MF79U and MF833V.	SG-6000-A5800/A5600 /A5500/A5200/A5100 /A3800/A3700/A3600 /A3000/A2800/A2700 /A2600/A2000/A1100 /A1000/A200 /A200W
29024	You can configure Use System for the DNS proxy server to automatically obtain the DNS server.	A, E, X, CloudEdge
28438	Commands can be used to: • view NAT rule hit counts; • view statistics on NAT rule hits, including rule ID, hit counts, first-hit time, last-hit	

ID	Description	Platform
	time, days since last-hit time, rule created time, and rule status (enabled/disabled); • filter/clear, and sort statistics on NAT rule hits.	
Object		
28386	Allow you to import or export custom address books, custom applications/application groups, custom services/service groups.	A, E, X, CloudEdge
28336	Allow you to add description of members to an address book.	
Authentication		
31434	Support to simplify the Authentication function. The system uses the authentication method configured in the device (configured by running the **auth-method {plain | digest-md5}** command) to connect with the Active-Directory/LDAP server and no longer queries the encryption method of the server.	A, E, X, CloudEdge
31248	SSO Monitor supports to associate with configured address book. During authenticated user generation, only users within the IP range are generated.	
30700	• Support to create AD/LDAP accounts and configure expiration time; • Support to configure the expiration time of	

ID	Description	Platform
	locally synchronized AD/LDAP accounts; • Support to import/export AD/LDAP accounts.	
28151	You can configure the MAS protocol subtype for HTTP(S) SMS gateway so that the device can be connected to the mobile cloud MAS SMS platform.	
32043	SMS gateway authentication can connect to China Mobile Music SMS Platform to perform SSL VPN authentication and Web authentication.	
28614	Support SMS-based authentication for SSL VPN by using the LDAP server.	
31981	Support the role blacklist function. Users mapped to roles that are in the blacklist fail to log in. The supported authentication log in methods include SSL VPN/ZTNA/WebAuth/L2TP/802.1X/IPSec VPN (UserGroup).	
31973	Allow you to configure the EMAY protocol subtype for HTTP(s) SMS gateway, which connects the Hillstone device to the EMAY SMS platform.	
31987	In the SSL VPN SMS authentication, the system can obtain the TelephoneNumber field of the AD/LDAP server as your mobile phone number.	

ID	Description	Platform
	When you log in to SSL VPN, the system sends an SMS verification code to that phone number.	
32645	The authentication level of the AD server is increased after the CVE-2021-26414 patch is updated. Therefore, the authentication level of the firewall is increased accordingly to ensure successful connection between the client and the server.	
30490	Support the expiration notification of the local server account. When the local server account is about to expire, the system displays a message on the Web authentication login page, indicating the remaining valid days of the account.	
30338	SSL VPN and ZTNA supports the notification of local account expiration. If the system uses the local authentication server to authenticate user identify on the SSL VPN/ZTNA client, when a user whose account is about to expire logs in to SSL VPN/ZTNA by using the client, a dialog box appears to prompt you that how many days are remained before the expiration date.	
SNMP		
31250	Allow you to query information about transceiver module by using SNMP, including the current temperature, transmit supply voltage, transmit bias current, transmit optical power, and receive	A200/A200W

ID	Description	Platform
	optical power.	
28717	IPv6 SNMP, including the IPv6 SNMP host, trap host and V3 users, can be configured on WebUI.	A, E, X, CloudEdge
VPN/ZTNA		
29476	You can specify the allowed types of the SSL VPN/ZTNA client, which can be one or more of the Windows client, Android client, iOS client, macOS client, and Linux client.	A, E, X, CloudEdge
31966	Allow you to check the registry value by using host compliance check. Add the value name and value data fields.	
29789	Support to configure the forced offline schedule. When the schedule takes effect, the system forces online SSL VPN/ZTNA users to log out.	
Threat Prevention		
28568	Add the anti-virus whitelist. You can add the URL/MD5 value to the whitelist to reduce false positives.	A, E, X, CloudEdge
31997	AD threats and AD threat logs supports to display details of flood attacks.	
IPv6		
23314	You can configure the IPv6 over IPv4 tunnel by using WebUI, including automatic 6to4 tunnel, manual 6to4 tunnel, ISATAP tunnel, and 6RD	A, E, X, CloudEdge

ID	Description	Platform
	tunnel.	
IoT		
30232	The system supports to connect with the pro-active detection module, which can be used to identify network video surveillance devices.	A, E, X
31957	X series supports the IoT function.	X
31958	Support to save custom IoT device information after a system restart.	A
31961	Support licenses for IoT video monitoring, provide the IoT policy function, and authorize the maximum number of IoT devices that can enable monitoring.	A, E, X
SLB		
30703	Allow you to configure the SLB server priority and minimum number of active real servers. The system checks from high priority to low priority according to the configured minimum number of working servers. When the number of working servers within the current priority range meets the minimum requirement, the working servers within that priority range will participate in traffic distribution. If the minimum number of working servers is not met, or if the status of one of the servers becomes unreachable resulting in the number of working servers in the current priority	A, E, X, CloudEdge

ID	Description	Platform
	range being less than the minimum threshold, the system will continue to check the servers in the next lower priority range until the minimum number of working servers is met.	
Monitoring and Logs		
31113	Support to display policy name of session logs.	A, E, X, CloudEdge
31944	Support to store session logs and NAT logs to the local disk.	A (only for devices with hard disks equipped)
31951	Display CPU/memory utilization trend charts on Device Monitor.	A, E, X
31952	Display statistics and online statistics of IoT devices on reports and add an online device trend chart to the IoT Monitor tab.	A, E, X
31954	Optimize the IoT Monitor page by adding the screening monitoring mode page.	
31955	Identify and monitor multiple types of devices from more manufacturers by using the IoT monitor function.	
31956	Allow you to configure the area where monitor devices reside by using the IoT function.	
31959	Display offline device manufacturers and device types on the Summary page of IoT Monitor.	
29690	SG-6000-X9180 supports to store logs, including events logs, threats logs, configuration logs,	X9180 (for devices with hard disk)

ID	Description	Platform
	network logs, and cloud sandbox logs, to the device hard disk.	
Cloud Platform		
31941	Allow you to upload source IP address, destination IP address, and application-based traffic statistics to CloudView.	A, E, CloudEdge
31942	Allow you to upload more comprehensive threat information to CloudView.	A, E, X, CloudEdge
31960	Allow you to upload device IoT data to CloudView.	A, E, X
31967	Allow you to upload interface traffic and rate data of the device to CloudView over a specified period of time and dynamically configure the upload schedule.	A, E, X, CloudEdge
31968	Allow you to upload the device startup time and bypass module status to CloudView.	A (except A200), E2800
31969	Allow you to upload the number of online SSL VPN users to CloudView.	A, E, X, CloudEdge
31971	Allow you to upload evidence information written in threat logs of the intrusion prevention module to CloudView.	A, E, X10800, CloudEdge
31972	Allow you upload the number of online users based on IP address to CloudView.	
31990	Support to remotely upgrade the system version of firewall devices through CloudView.	A, E, X, CloudEdge

ID	Description	Platform
RESTful API		
31931	Allow you to create, edit, query, and delete a local user/user group by using RESTful API.	A, E, X, CloudEdge
31933	Allow you to query the address book whose members are non-address book entries and query the address book whose members are address book entries respectively by using RESTful API.	
31935	Allow you to query the items associated with address book entries, services, and service groups by using RESTful API.	
31936	Allow you to query the ID of the policy rule that references a zone by using RESTful API.	
31937	Allow you to clear the hit number of multiple policy rules at a time by using RESTful API.	
31938	Allow you to query multiple policy rules based on multiple IDs at a time by using RESTful API.	
31939	Allow you to import or export policy rules, address entries, custom applications/application groups, and custom services/service groups by using RESTful API.	
29373	Allow you to view total outbound traffic and inbound traffic of the device by using RESTful API operations.	
29366	Allow you to send shutdown commands by using RESTful API operations.	

ID	Description	Platform
29357	Allow you to obtain the HA status and perform HA active/standby switchover by using RESTful API operations.	
	CloudEdge supports the HA Peer Active-Active (A/A) mode.	CloudEdge
29582	Allow you to obtain disk usage by using RESTful API operations.	
28553	• Allow you to create, edit, delete, and query the botnet prevention rule by using RESTful API operations; • Allow you to edit or query the botnet prevention global settings by using RESTful API operations; • Allow you to create, delete, and query the exceptional list and blocked list of the botnet module by using RESTful API operations; • Allow you to configure the botnet prevention function in Non-root VSYS; • Support the predefined botnet prevention rules: predef_critical and predef_default.	A, E, X, CloudEdge
Capacity		
32000	The number of physical interfaces support by a interface group upgrades from 8 to 16.	A, E, X, CloudEdge

ID	Description	Platform
31963	Scale the number of secondary IP addresses that can be assigned to an interface to 32.	
28335	Increase the number of static routes and BGP routes in the device.	X10800, X9180, X8180
28153	Increase the maximum number of online AD Agent users supported by X series to 100,000.	X7180, X8180, X10800, X9180

Known Issues

ID	Description	Platform
SSL VPN		
323249	When 360 Security Guard is installed on the PC, errors may be reported when you log in to the ZTNA or VPN client. Recommendation: Add "" directory to trusted zone.	A, E, X, CloudEdge
329424	If you want to install an earlier version of the SSL VPN client after the new version of the SSL VPN client is installed, uninstall the existing new version of the SSL VPN client first.	
287915	The resource list can be displayed on the latest version of the SSL VPN client (such as Windows/Android/IOS). If the number of resources in the list exceeds 20, compatibility issues may occur on the SSL VPN client of an earlier version. Solution: Upgrade the SSL VPN client (such as Windows/Android/IOS) to the latest version.	A, E, X, CloudEdge

ID	Description	Platform
333797/333798	If the device is not installed with an SSL VPN license and ZTNA license, the number of SSL VPN/ZTNA authorized users that you view by using the CLI and by using the WebUI may be inconsistent. Solution: The actual number of authorized users displayed on the WebUI shall prevail.	A, E, X, CloudEdge
329186	When you log in to the latest version of the SSL VPN client for Android, you may not be able to select an installed certificate for connection configuration. Solution: Manually select an installed certificate.	A, E, X, CloudEdge
335090	If you install and use the latest version of the SSL VPN client for Windows on a low-specification PC, packet sending and receiving may be abnormal and the SSL VPN client may be disconnected when you download files.	A, E, X, CloudEdge
327602	When you uninstall the SSL VPN client for macOS, the client icon may be not removed from Launchpad and Dock.	A, E, X, CloudEdge
313034	If a default route is configured in the tunnel route for the firewall, you may not be able to access internal resources when you connect to the firewall by using the SSL VPN client for Android.	A, E, X, CloudEdge
334346/332965	When the SSL VPN client for macOS is running, you may not be able to open the SSL VPN client UI or the SSL VPN client may be disconnected and not be able to be reconnected after waking up the MAC that is	A, E, X, CloudEdge,

ID	Description	Platform
	sleeping.	
335092	After the SPA function is enabled, the latest version of the Hillstone Secure Connect client may not be able to be automatically updated. Solution: After the SPA function is enabled, manually update the Hillstone Secure Connect client.	A, E, X, CloudEdge
QoS		
251079	QoS does not support the user rate limit in the Peer-mode asymmetric routing scenario.	A, E, X, CloudEdge
HA		
286815	When the backup device is upgraded from 5.5R6 to 5.5R10 in the HA AP environment while the master device is still in the 5.5R6 version, the backup device might not synchronize the user group and role information of online users on the master device.	A, E, X, CloudEdge
CloudEdge		
310941	If the system is not restarted after the installation of the new version of the platform license, previous version of the VSN platform license can still be viewed through CLI and its displayed VSN is incorrect.	CloudEdge

Explorer Compatibility

The following browsers have passed compatibility tests:

- IE11
- Chrome 45 and later

Getting Help

Hillstone provides the following guides to help you understand our products. Visit https://-docs.hillstonenet.com to download guides.

- Hillstone SG-6000 Hardware Reference Guides (A -Series | E-Series | X-Series)
- Hillstone SG-6000 Expansion Modules Reference Guides (E-Series | X-Series)
- StoneOS WebUI User Guide (A-Series | E-Series | X-Series | CloudEdge)
- StoneOS CLI User Guide
- StoneOS Getting Started Guide (A-Series | E-Series | X-Series)
- StoneOS Cookbook
- StoneOS Log Messages Reference Guide
- StoneOS SNMP MIB Reference Guide
- Troubleshooting Guide
- CloudEdge Deployment Guide

Website: https://www.hillstonenet.com

Service Line: 1-800-889-9860

Appendix: Upgrading Notes

The appendix includes Upgrading Notes for Each Platform, Upgrading Notes for Each Module, Upgrading in HA Environment and Verifying the Upgrading.

It's strongly recommended that you upgrade to a neighbor version instead of upgrading across several versions. If you upgrade across several versions, please compare the configurations before and after

the upgrade carefully. Due to network environment diversities and specific requirements, please call 1-800-889-9860 before an upgrade.

Upgrading Notes for Each Platform

Upgrading Notes for E/X Platform

For different versions of E/X platform, note the following matters:

- To upgrade 5.0R4 or lower versions to 5.5R10 and later, Hillstone recommends you, according to related guidebooks, to first upgrade to the latest P version of 5.5R4, and then upgrade to 5.5R10 and later.
- To upgrade 5.5R1 or higher versions to 5.5R10, Hillstone recommends you, according to related guidebooks, to first upgrade to the latest P version of 5.5R4, 5.5R6 or 5.5R7, and then upgrade to 5.5R10 and later.

Upgrading Notes for CloudEdge Platform

- Only releases the firmware of StoneOS 5.5R10, if you need to upgrade StoneOS to 5.5R10 and later, note the following matters:
    - 5.5R8P11/5.5R9P4/5.5R9F4 and later can be directly upgraded to 5.5R10 and later;
    - All previous R/F/M/P versions earlier than 5.5R8P11, and all previous R/F/M/P versions earlier than 5.5R9P4, please upgrade to 5.5R8P11/5.5R9P4/5.5R9F4 and later versions, and then upgrade to 5.5R10 and later.
    - If you need the upgrade file in 5.5R10.img format, please visit https://images-en.hillstonenet.com/login to get the file.
- Upgrading system from 5.5R2 or lower versions to 5.5R9 and later is not supported. The reasons are as follows:

    - The default license in 5.5R1/5.5R2 is valid permanently, but only supports part of functions. However, the default license in 5.5R7 or higher versions is only valid for 30 days and supports all functions. Therefore, errors may occur when upgrading to 5.5R10 is performed.
    - Due to the default license is not pre-installed in the .img system file, it may not be valid for 30 days after upgrade.

  To upgrade 5.5R2 or lower versions to 5.5R10 and later, Hillstone recommends you, according to related guidebooks, to first upgrade to 5.5R6P12.2, and then upgrade to 5.5R9P4/5.5R9F4 and later, and finally upgrade to 5.5R10 and later.

- From 5.5R6, after the upgrade of CloudEdge, the licenses applied through the old SN code will be invalid because the SN code is changed. You need to apply and install the licenses with the new SN code, while the licenses distributed through LMS and vLMS system do not need to be reapplied. **We strongly recommend that you back up current configuration files before upgrading.**
- From 5.5R6, the firmware of CloudEdge will be unified into one type. System will automatically identify the platform model according to the CPU license and the resource configurations of VM. After system upgrades from the versions lower than 5.5R6 to 5.5R10 and later, please note the followings:
    - After upgrading, install the corresponded CPU license and configure VM resources (vCPU and memory) of the platform model as soon as possible, otherwise, system may fail to display the corresponded platform model or start up.
    - When CPU license is installed, restart the device. If the right platform model can be displayed via the command **show version**, it means CPU license has been installed successfully.
    - Configure the VM as the required resources of CloudEdge platforms: VM01 (2vCPU/2G memory) / VM02 (2vCPU/4G memory) / VM04 (4vCPU/8G memory)/VM08

(8vCPU/16G memory). If the minimum resources do not be met before upgrade, system may fail to display the corresponded platform model or start up.

- From 5.5R4, the .img system files can be adapted to virtualization platforms automatically.
- From 5.5R4, the virtual MAC prefix of HA can be configured on CloudEdge, but the virtual MAC address will be changed after reboot.
- From 5.5R3, the system files are divided into IPv4 and IPv6 versions.
- From 5.5R1P15/5.5R2P8/5.5R3P6/5.5R4P4 and later P release, you're strongly recommended to use the 2vCPU/2GB memory to deploy CloudEdge VM01.
- From 5.5R5, at least 2vCPU/2G memory is required to deploy CloudEdge.

Upgrading Notes for Each Module

Upgrading Notes for HSM & HSA Matching Version

When connecting 5.5R10 devices to HSA or HSM, you should first upgrade HSA to 2.11.0 or higher versions, or upgrade HSM to 4.15 or higher versions.

Upgrading Notes for the SSL Proxy Function

From 5.5R9, the system changes the default value of the **Unsupported version**, **Unsupported encryption algorithms**, **Unknown Error**, and **Client verification** parameters in the SSL Proxy configuration from **Block** to **Bypass**. After the system is upgraded to 5.5R9 and later, related configurations will change. If you still want to use the **Bypass** value, manually change the configurations.

Upgrading Notes for the SSL VPN Function

1. From 5.5R9, the SSL VPN Windows client supports data transmission reliability configuration. To use the SSL VPN client of new versions (V1.4.9.1281 and later), note the following items.

The client of old versions (V1.4.9.1279 and earlier) is not affected.

- If the server enables the TCP port, the SSL VPN client of a new version can successfully connect to the server regardless of whether **Communication stability optimization** is selected.
- If the server disables the TCP port, an error will occur when the SSL VPN client of a new version with **Communication stability optimization** selected starts a connection attempt. The connection can be successfully established after this option is deselected.

2. From 5.5R10, the SSL VPN client has been reconstructed and a new version of the SSL VPN client is available for Windows, macOS, Linux, Android, and iOS. To use the SSL VPN client of new versions (V5.0.0and later), note the following item: Automatic is added to the configuration of **Communication stability optimization**. If **Auto** is selected, the system automatically selects the connection mode based on whether the TCP port is enabled on the server.
3. From 5.5R9, SSL VPN no longer supports RSA SecurID Token authentication by using the RSA server. When the system is upgraded from an earlier version to 5.5R9 or later, use other authentication methods.
4. From 5.5R10, the SSL VPN Address Pool function has been changed to the Access Address Pool function. Changes have been made on the CLI and WebUI, for example: The command **scvpn pool** *pool-name* is replaced with **access-address-pool** *pool-name*. You can select **Object** > **Access Address Pool**.on the WebUI. When the system is upgraded from an earlier version to 5.5R10 and later, the original configuration is retained and can be used normally.

Upgrading Notes for IPS Signature Database

From 5.5R8P2, IPS signature database 3.0 is supported. You can update your IPS signature database to the latest version with improved protection capability based on your requirements. The original IPS signature database 2.0 can still be used after the system is upgraded. To update IPS Signature Database, go to **System** > **Upgrade Management** > **Signature Database Update** and update it online, or download IPS signature database 3.0 for offline update.

Upgrading Notes for iQos Function

Intelligent Quality of Service (iQos) is added from version 5.5R1, and the function is enabled automatically from 5.5R2. When system with QoS configured is upgraded to 5.5R7 or higher versions, use the **exec iqos enable** command to enable iQoS (iQoS can only be configured via CLI). After iQoS is enabled, the QoS configurations will be saved but become invalid and cannot be edited. If you need to enable QoS, use the **exec iqos disable** command to disable iQoS and re-activate QoS.

From 5.5R6, iQoS can be obtained via IOM module on the X platform. Before obtaining the iQoS function via IOM module, make sure the iQoS license has been installed.

Upgrading Notes for Link Load Balancing Function

From 5.5R4, **llb outbound** related command is no longer supported, with the new command **llb rule** instead. When the system is upgraded from versions lower than 5.5R4 to 5.5R7, 5.5R8, 5.5R9, 5.5R10, and later, the old configurations will be lost, you must configure it again.

Upgrading Notes for Web Authentication Function

From 5.5R5, Web authentication function is adjusted. When the system is upgraded from versions lower than 5.5R5 to 5.5R10 and later, the custom files (such as Web authentication background images, web redirection background images) uploaded by the old version will not take effect, you must configure it again.

Upgrading Notes for IM Audit Function

From 5.5R5, IM audit function is adjusted. When the system is upgraded from versions lower than 5.5R5 to 5.5R10 and later, the old configurations will be lost, you must configure it again.

Tips: Please reconfigure it via WebUI after upgrade.

Upgrading Notes for File Filter Function

From 5.5R5, the function of file filter will no longer support filtering through file name and file size. When the system is upgraded from versions lower than 5.5R5 to 5.5R10 and later, the old configurations will be lost.

Tips: Please reconfigure it after upgrade.

Upgrading Notes for Share Access Detect Function

From 5.5R6, share access function is adjusted, the command **host share-access detect enable** of share access detect function will no longer be supported. When the system is upgraded from versions lower than 5.5R6 to 5.5R10 and later, the old configurations will be lost, you must configure the share access function again.

Upgrading Notes for AD Agent Function

To use AD Agent software to obtain user information in version earlier than StoneOS 5.5R10, you can connect the AD agent by using SSO Monitor or configure the security agent in Active-Directory server configuration mode. In StoneOS 5.5R10 and later, the system no longer supports the security agent function. When the version is upgraded to StoneOS 5.5R10 or later, the configured security agent function is automatically converted to the SSO Monitor function to connect to the AD Agent software configuration. You can run the **show user-sso client sso-monitor**[*profile-name*] command to view the configuration. The converted name of SSO Monitor Profile is the same as that of the AD server.

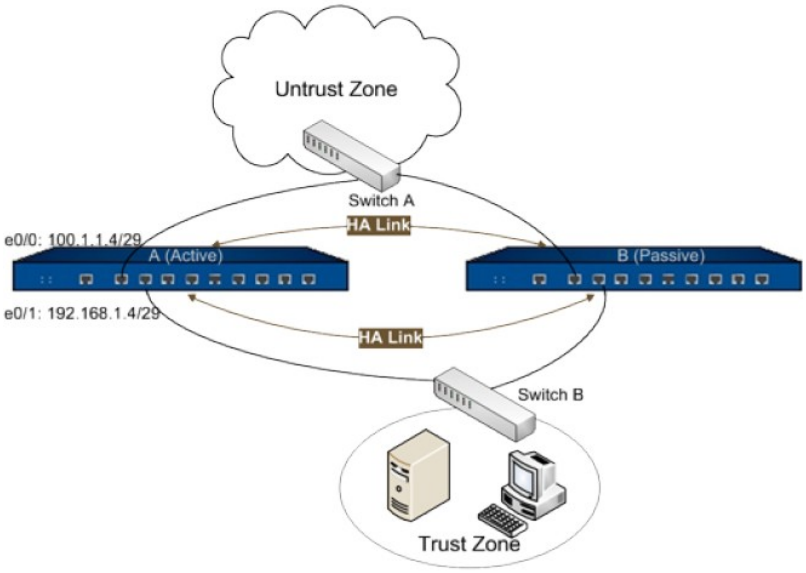
Upgrading Notes for SSO Monitor Function

From StoneOS 5.5R10, SSO Monitor can connect to multiple external servers to implement redundant backup. Therefore, the configured "**host x.x.x.x**" of SSO Monitor will be automatically converted to "**host1 x.x.x.x**" after the system is upgraded to StoneOS 5.5R10. You can run the **show user-sso client sso-monitor**[*profile-name* command to view the converted configuration. The converted name of SSO Monitor Profile is the same as that of the AD server.

Upgrading in HA Environment

Upgrading Environment

The following is the topology of HA:



Preparation Items

No.	Items	Detailed Information
1	Prepare upgrading reference guide	The upgrading reference guide has been printed or stored in the PC.
2	Prepare firmware of new version	Obtained the firmware of new version from Hillstone.
3	Check current firmware version	Select proper upgrading method according to the platform, firmware version, and upgrading notes.
4	Check device running status	• Ensure the SCM and SSM work normally • Record the running status of the modules in each slot before and after the upgrade for locating failover.
5	Deploy the upgrading environment via TFTP or FTP	Deploy the upgrading environment via TFTP or FTP in the above environment.
6	Back up configuration file	If the configurations after the upgrading differ from the previous one, compare the differences and re-configure the missed settings.

Upgrading Operations

It's strongly recommended that you upgrade to a neighbor version instead of upgrading across several versions. If you upgrade across several versions, please compare the configurations before and after the upgrade carefully. For detailed methods, refer to Verifying the Configurations. To get more help about upgrading, please call 1-800-889-9860.

Upgrading E/X Platform From 5.0 Versions to 5.5R10 and Later

1. Make sure the startup configurations files of the master device and backup device are the same before the upgrading.
2. Take the device B offline by removing the service cable from device B first and then removing the HA heartbeat cable from device B. In this case, users' traffic will be forwarded through device A.
3. When HA function of device B is disabled, upgrade device B to the latest P version of 5.5R4 according to Upgrading Notes for Each Platform.
4. After device B upgrades successfully, reconnect the HA heartbeat cable on device B and then enable HA function of device B so that device B can conduct HA negotiation with device A.
5. Wait for device B to complete HA negotiation, synchronization of configurations and sessions. Then, reconnect the service cable on device B. In this case, users' traffic will still be forwarded through device A.
6. Manually switch device B to the master device. In this case, users' traffic will be forwarded through device B.
7. Remove the service cable from device A and then remove the HA heartbeat cable from device A.
8. When HA function of device A is disabled, upgrade device A to the latest P version of 5.5R4. After device A upgrades successfully, continue to upgrade device A to 5.5R10 and later.

9. Reboot device A to make the imported image files take effect. After device A reboots successfully, the version of device A is 5.5R10 and later.
10. Reconnect the HA heartbeat cable on device A and then enable HA function of device A so that device A can conduct HA negotiation with device B.
11. Wait for device A to complete HA negotiation, synchronization of configurations and sessions. Then, reconnect the service cable on device A.
12. Manually switch device B to the backup device. In this case, users' traffic will be forwarded through device A.
13. Remove the service cable from device B first and then remove the HA heartbeat cable from device B.
14. Disable the HA function of device B and then upgrade device B to 5.5R10 and later. After device B upgrades successfully, reboot device B.
15. After device B upgrades successfully, reconnect the HA heartbeat cable on device B and then enable HA function of device B so that device B can conduct HA negotiation with device A.
16. Wait for device B to complete HA negotiation, synchronization of configurations and sessions. Then, reconnect the service cable on device B.
17. Complete the upgrading.

Upgrading A/E/X Platform From 5.5 Versions to 5.5R10 and Later

Preparations Before Upgrading

1. Back up the current configuration of device A and device B to your local computer.
2. Make sure the configurations of the master device and backup device are the same before the upgrading.

3. Make sure that current service works normally.
4. Respectively import image files of 5.5R10 to device A and device B.
5. Disable the preempt mode if it is enabled. You can enable the preempt mode when the upgrading is completed. If track objects are bound to the HA group, removing the binding. You can resume the binding when the upgrading is completed.

Upgrading Device B

1. Take the device B offline by removing the service cable from device B first and then removing the HA heartbeat cable from device B.
2. Execute the **save** command on device B to save the configuration. Then, reboot device B to make the imported image files take effect. After device B reboots successfully, check whether the version of device B and its HA configuration are correct.
3. Export the configuration of device B and compare it with the one before upgrading, making sure no configuration is lost.
4. Execute the **show ha group config** command on device A and device B to view their priority values. Make sure the priority value of device A is less than that of device B. That is to say, device A has a higher priority than device B. If the priority value of device A is larger than that of device B, modify the latter to make sure device A has a higher priority.
5. Reconnect the HA heartbeat cable on device B. Wait for device B to complete HA negotiation with device A. In this case, device A is the master device. Then, reconnect the service cable on device B.

HA Synchronization and Master/Backup Device Switchover

1. Execute the **exec ha sync all** command on master device A to manually synchronize the configuration of device A and device B.

2. Execute commands such as **show arp**, **show session generic** on master device A to check whether the ARP table, session information, etc. are synchronized.
3. Execute the **show logging alarm** command on master device A. When the prompt "Admin batch synchronization of HA group 0 has completed." appears, it suggests that configuration synchronization is completed.
4. Execute the **exec ha master switch-over** command on master device A to manually switch the master and backup devices. In this case, device B is switched to the master device.

Upgrading Device A

1. Take the device A offline by removing the service cable from device B first and then removing the HA heartbeat cable from device A. In this case, make sure the service of device B works normally.
2. Execute the **save** command on device A to save the configuration. Then, reboot device A to make the imported image files take effect. After device A reboots successfully, check whether the version of device A and its HA configuration are correct.
3. Export the configuration of device A and compare it with the one before upgrading, making sure no configuration is lost.
4. Execute the **show ha group config** command on device A and device B to view their priority values. Make sure the priority value of device A is larger than that of device B. That is to say, device A has a lower priority than device B.
5. Reconnect the HA heartbeat cable on device A. Wait for device A to complete HA negotiation with device B. In this case, device B is the master device. Then, reconnect the service cable on device A.

HA Synchronization

1. Execute the **exec ha sync all** command on device B to manually synchronize the configuration of device A and device B.
2. Execute commands such as **show arp**, **show session generic** on master device B to check whether the ARP table, session information, etc. are synchronized.
3. Execute the **show logging alarm** command on master device B. When the prompt "Admin batch synchronization of HA group 0 has completed." appears, it suggests that configuration synchronization is completed.

Completing the Upgrading

1. (Optional) Execute **exec ha master switch-over** command on device B to manually switch device A to the master device.
2. Complete the upgrading.

Verifying the Upgrading

Verifying the Upgrading for A/E/X Platform

After the upgrading completes, use the **show version** command to verify whether the system has been upgraded to the new version successfully.

Verifying the Configurations

After the upgrading completes, export the configuration file and compare it with the previous one. If some configurations miss, you can check whether the commands have changed in the new version and then re-configure the missed settings.

Verifying Basic Business

After the upgrading completes, perform some basic business to verify whether the device can work normally.