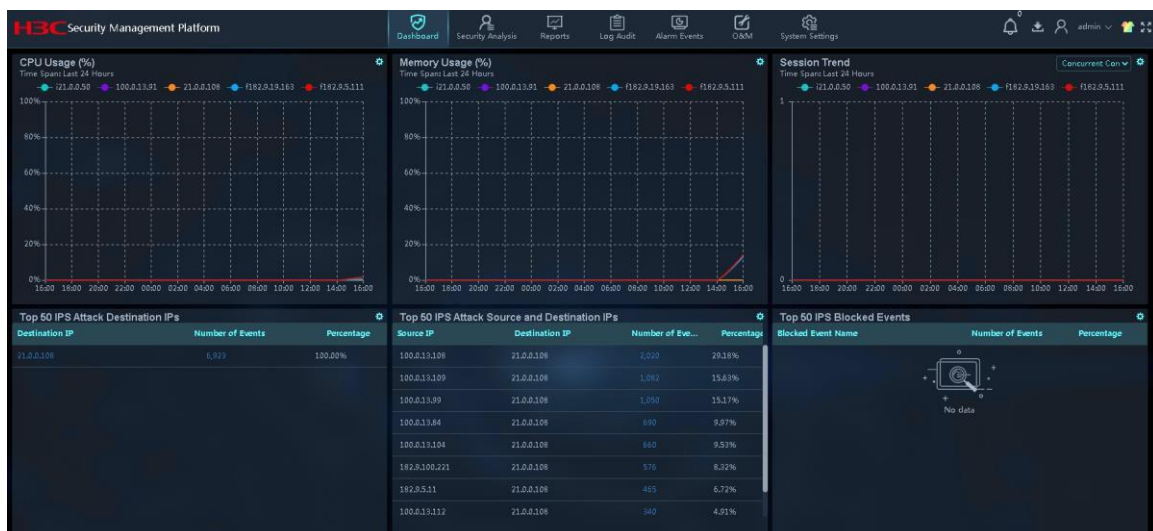




H3C SecCenter SMP Security Management Platform

Product overview

The Security Management Platform (SMP) is a platform that allows you to manage network security services. SMP is applicable to networks of all sizes. It provides centralized management of key security devices (such as firewalls and IPS devices) through the following features: real-time event monitoring, security policy deployment, threat log audit, and comprehensive statistics and analysis on security events on the whole network. SMP has the capability to operate in a high-availability (HA) cluster.



Features and highlights

Unified O&M

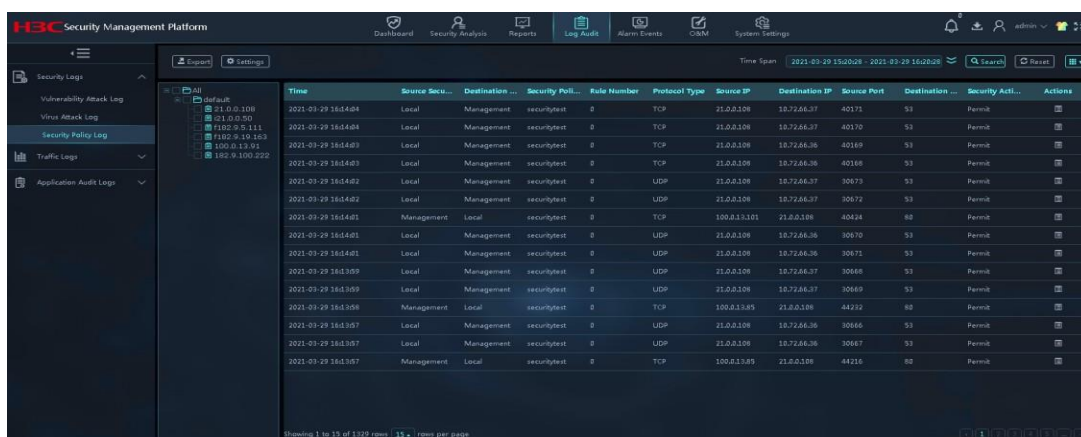
- Unified security policy management.
- Unified device performance monitoring.
- Unified security signature upgrading.
- Unified update the devices standard software.
- Unified store backups of the devices and software.
- After you synchronize security devices to the SMP global resources, you can perform the following operations:
- Add, edit, or delete security policies.
- View, synchronize, upgrade, or roll back the IPS, AV, or ARP signature libraries of the devices.
- Upload, push, delete, or search for signature files.
- Manage the file push tasks, and view the task state and running result.
- View statistics on the managed devices, including the CPU usage, memory usage, system traffic statistics, interface traffic statistics, system concurrent sessions, and system new sessions.

The screenshot displays the H3C Security Management Platform (SMP) interface. The top navigation bar includes links for Dashboard, Security Analysis, Reports, Log Audit, Alarm Events, O&M (highlighted), and System Settings. The left sidebar shows a tree view with categories: Areas, Device Groups, Monitored Assets, Security Services, Global Resources, Security Policies (selected), and Signature Libraries. The main content area is titled 'Security Policies' and 'Policy Deployment Task'. It features a table with two policies and search filters.

No.	Policy	Source Se...	Destinati...	IP Ver...	Source IP	Destinati...	Service Gr...	Time Ran...	Security A...	Content S...	Description	Logging	Statistics	Policy State	Source	State	Actions
1	policy1	t1	t1	IPv4	any	any	any	any	Permit			Enable	Enable	Enable	Manually...	Not Used	[Edit] [Delete]
2	cs	Local	Local	IPv4	any	any	any	any	Permit	IPSDefault	AVDefault	Enable	Enable	Enable	Manually...	Not Used	[Edit] [Delete]

Log audit and alarming

- IPS/FW security event logging; log searching by multiple conditions.
- IPS/FW security event logs in standard format; log information displaying by start and end time, source and destination IPs, source port, source and destination security zones, log source device name, security actions, protocol, and event severity.
- Customized log aggregation for security event alarming.
- Provide the functionality to collect and filter logs from the devices.
- SMP collects logs from devices. Based on the logs, SMP visually displays a security event's source, destination, and other details, so that administrators can know about attacks and abnormal traffic on the network. SMP also records user operations for audit and trace purposes. SMP provides powerful search. It can quickly find matching data in massive historical data from multiple dimensions, such as device, time, event severity, protocol, security action, and source/destination IP.

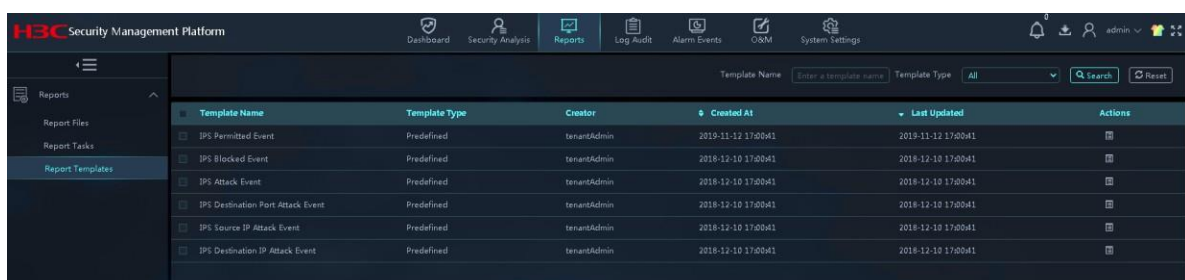


The screenshot shows the 'Log Audit' section of the H3C Security Management Platform. It features a sidebar with navigation options like 'Security Logs', 'Vulnerability Attack Log', 'Virus Attack Log', 'Security Policy Log', 'Traffic Logs', and 'Application Audit Logs'. The main area displays a table of security events with columns: Time, Source Sec..., Destination..., Security Poli..., Rule Number, Protocol Type, Source IP, Destination IP, Source Port, Destination..., Security Acti..., and Actions. The table contains multiple rows of log entries, and a footer indicates 'Showing 1 to 15 of 1329 rows'.

Time	Source Sec...	Destination...	Security Poli...	Rule Number	Protocol Type	Source IP	Destination IP	Source Port	Destination...	Security Acti...	Actions
2021-01-29 16:46:04	Local	Management	securitytest	0	TCP	21.0.0.108	10.72.66.37	40171	53	Permit	[icon]
2021-01-29 16:46:04	Local	Management	securitytest	0	TCP	21.0.0.108	10.72.66.37	40170	53	Permit	[icon]
2021-01-29 16:46:03	Local	Management	securitytest	0	TCP	21.0.0.108	10.72.66.36	40169	53	Permit	[icon]
2021-01-29 16:46:03	Local	Management	securitytest	0	TCP	21.0.0.108	10.72.66.36	40168	53	Permit	[icon]
2021-01-29 16:46:02	Local	Management	securitytest	0	UDP	21.0.0.108	10.72.66.37	30673	53	Permit	[icon]
2021-01-29 16:46:02	Local	Management	securitytest	0	UDP	21.0.0.108	10.72.66.37	30672	53	Permit	[icon]
2021-01-29 16:46:01	Management	Local	securitytest	0	TCP	100.0.1.101	21.0.0.108	40434	80	Permit	[icon]
2021-01-29 16:46:01	Local	Management	securitytest	0	UDP	21.0.0.108	10.72.66.36	30670	53	Permit	[icon]
2021-01-29 16:46:01	Local	Management	securitytest	0	UDP	21.0.0.108	10.72.66.36	30671	53	Permit	[icon]
2021-01-29 16:46:00	Local	Management	securitytest	0	UDP	21.0.0.108	10.72.66.37	30668	53	Permit	[icon]
2021-01-29 16:46:00	Local	Management	securitytest	0	UDP	21.0.0.108	10.72.66.37	30669	53	Permit	[icon]
2021-01-29 16:46:00	Management	Local	securitytest	0	TCP	100.0.1.105	21.0.0.108	44292	80	Permit	[icon]
2021-01-29 16:46:07	Local	Management	securitytest	0	UDP	21.0.0.108	10.72.66.36	30666	53	Permit	[icon]
2021-01-29 16:46:07	Local	Management	securitytest	0	UDP	21.0.0.108	10.72.66.36	30667	53	Permit	[icon]
2021-01-29 16:46:07	Management	Local	securitytest	0	TCP	100.0.1.105	21.0.0.108	44216	80	Permit	[icon]

Report management

- Predefined report templates.
- Customized report tasks. You can define the report task type and execution time.
- SMP has predefined five report templates. They are IPS block event, IPS attack event, IPS attack destination port, IPS attack source IP, and IPS attack destination IP. SMP supports you to customize reports based on the time, report template, and objects.



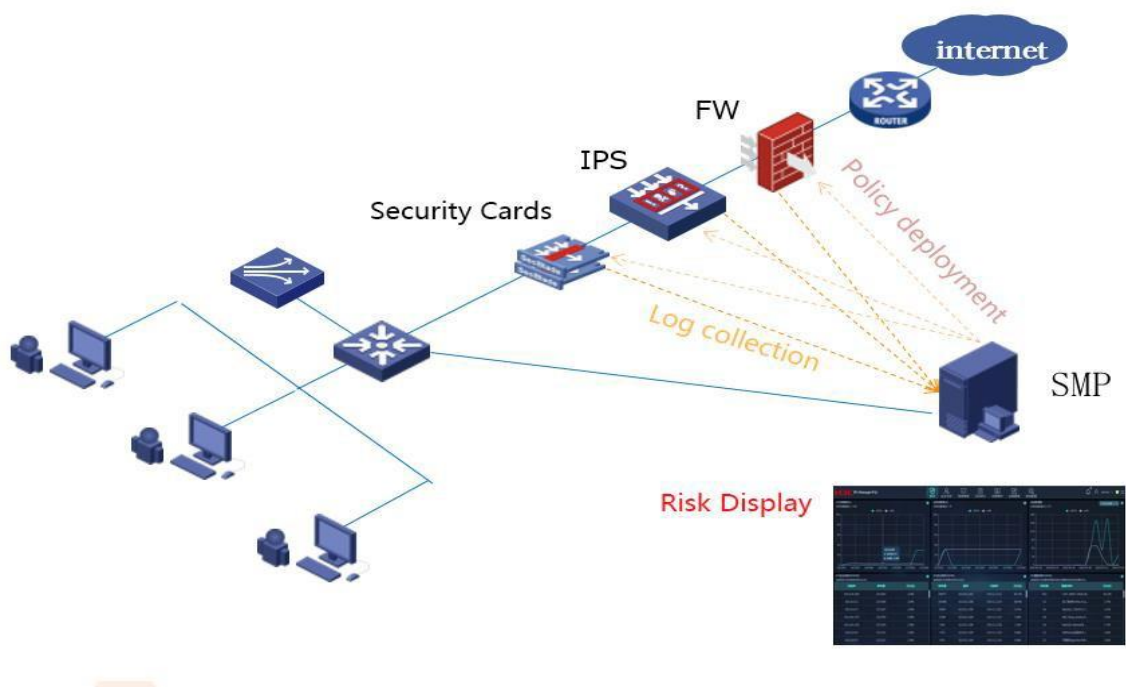
The screenshot shows the 'Reports' section of the H3C Security Management Platform. It features a sidebar with navigation options like 'Report Files', 'Report Tasks', and 'Report Templates'. The main area displays a table of predefined report templates with columns: Template Name, Template Type, Creator, Created At, Last Updated, and Actions. The table contains five rows of report templates, and a footer indicates 'Showing 1 to 5 of 5 rows'.

Template Name	Template Type	Creator	Created At	Last Updated	Actions
IPS Permitted Event	Predefined	tenantAdmin	2019-11-12 17:00:41	2019-11-12 17:00:41	[icon]
IPS Blocked Event	Predefined	tenantAdmin	2019-12-10 17:00:41	2019-12-10 17:00:41	[icon]
IPS Attack Event	Predefined	tenantAdmin	2019-12-10 17:00:41	2019-12-10 17:00:41	[icon]
IPS Destination Port Attack Event	Predefined	tenantAdmin	2019-12-10 17:00:41	2019-12-10 17:00:41	[icon]
IPS Source IP Attack Event	Predefined	tenantAdmin	2019-12-10 17:00:41	2019-12-10 17:00:41	[icon]
IPS Destination IP Attack Event	Predefined	tenantAdmin	2019-12-10 17:00:41	2019-12-10 17:00:41	[icon]

Technical specifications

Item	Description
Dashboard	Displays device performances and security events; Displays Top items in different time spans.
Log Audit	Collects and classifies IPS/FW threat logs; supports log searching by multiple conditions; displays log details; supports log exporting.
Alarm Events	Generates alarm events according to the alarm rules; supports popup display for an alarm event; supports acknowledging and bulk acknowledging alarm events.
O&M	Supports management of areas, assets, security policies, and signature libraries and configuration management.
System Settings	Provides system management features, including data cleaning, system parameter configuration, roles and privileges management, and logo customization.

Application scenarios



Ordering information

Item	Description
H3C SecCenter SMP	Required.
H3C SecCenter SMP Hierarchy Authorization	Optional. Required for hierarchical management.
H3C SecCenter SMP IPS Authorization	Optional. By default, FW management is available and IPS management requires authorization.

H3C SecCenter SMP-1 License	Optional. For management of one device.
H3C SecCenter SMP-5 License	Optional. For management of one device.
H3C SecCenter SMP-20 License	Optional. For management of twenty devices.
H3C SecCenter SMP-50 License	Optional. For management of fifty devices.
H3C SecCenter SMP-200 License	Optional. For management of two hundred devices.



The Leader in Digital Solutions

New H3C Technologies Co., Limited
Beijing Headquarters
Tower 1, LSH Center, 8 Guangshun South Street,
Chaoyang
District, Beijing, China
Zip: 100102
Hangzhou Headquarters
No.466 Changhe Road, Binjiang District, Hangzhou,
Zhejiang,
China Zip: 310052
Tel: +86-571-86760000
Fax: +86-571-86760001

Copyright ©2025 New H3C Technologies Co., Limited
Reserves all rights Disclaimer: Though H3C strives to
provide accurate information in this document, we
cannot guarantee that details do not contain any
technical error or printing error. Therefore, H3C cannot
accept responsibility for any inaccuracy in this
document. H3C reserves the right for the modification of
the contents herein without prior notification.

<http://www.h3c.com>