



H3C SecPath F100 ライセンス登録から初期設定まで



00 装置のGUIへアクセスする

01 装置ファイル(.did)のダウンロード

02 ライセンスリニューアル

03 ライセンスのインストール

04 シグネチャーの更新

05 各種ログの環境整備

06 攻撃検証環境の整備

07 検証結果

08 トラブルシュート

装置のGUIへアクセスする

ログの保存用

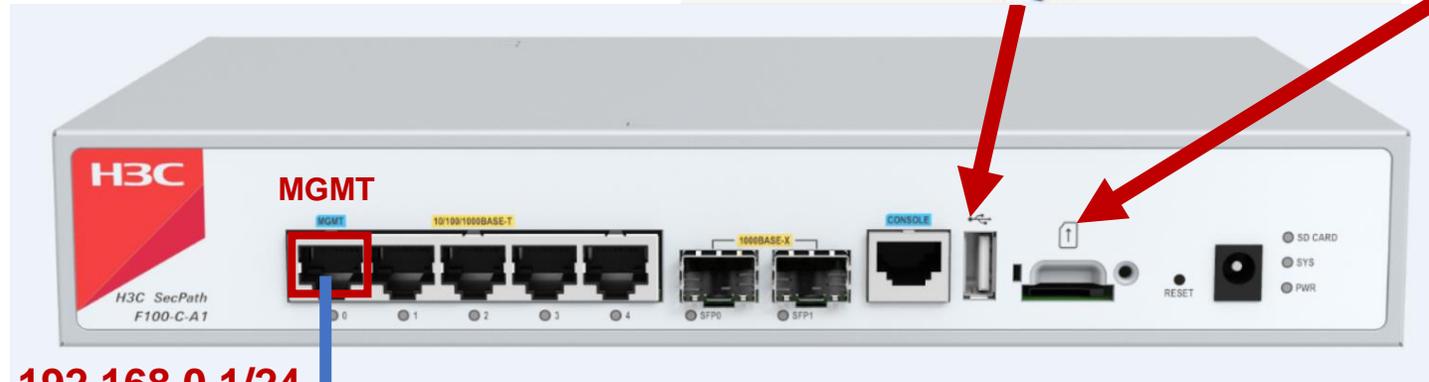
usb0:



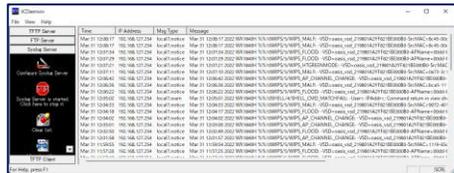
ログの保存用



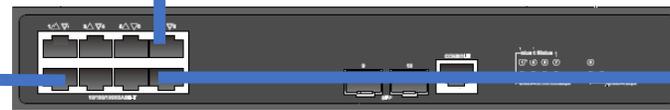
sda0:



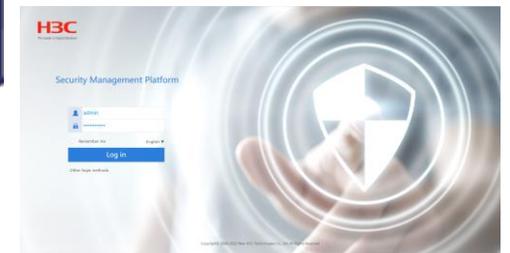
192.168.0.1/24



Syslogサーバー



<https://192.168.0.1/>



<https://192.168.0.1/>

H3C
The Leader in Digital Solutions

Security Management Platform

admin

.....

Remember me English ▾

Log in

Other login methods

デフォルトのログイン情報
ユーザー名: admin
パスワード: admin

Copyright © 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

初期パスワードを変更します

The screenshot shows the H3C Security Management Platform login interface. In the top left, the H3C logo is displayed with the tagline 'The Leader in Digital Solutions'. The main heading is 'Security Management Platform'. The login form includes a username field with 'admin' entered, a password field with masked characters, a 'Remember me' checkbox, and a language dropdown set to 'English'. A prominent blue 'Log in' button is present, along with a link for 'Other login methods'. A modal dialog box titled 'Change Password' is overlaid on the right side. It contains a warning message: 'The default password is not secure. A qualified password must meet the following requirements: It must contain a minimum of 10 characters. It must contain a minimum of 2 types, and a minimum of 1 characters for each type. It can't contain the username or the reversed letters of the username.' Below the message are three input fields: 'Old Password' (masked with 5 dots), 'New Password' (masked with 10 dots), and 'Confirm Password' (masked with 10 dots). At the bottom of the dialog are 'Apply' and 'Cancel' buttons. The background of the entire page features a stylized shield icon and a hand holding a glowing orb.

H3C
The Leader in Digital Solutions

Security Management Platform

admin

.....

Remember me English ▼

Log in

[Other login methods](#)

Change Password

The default password is not secure. A qualified password must meet the following requirements: It must contain a minimum of 10 characters. It must contain a minimum of 2 types, and a minimum of 1 characters for each type. It can't contain the username or the reversed letters of the username.

Old Password:

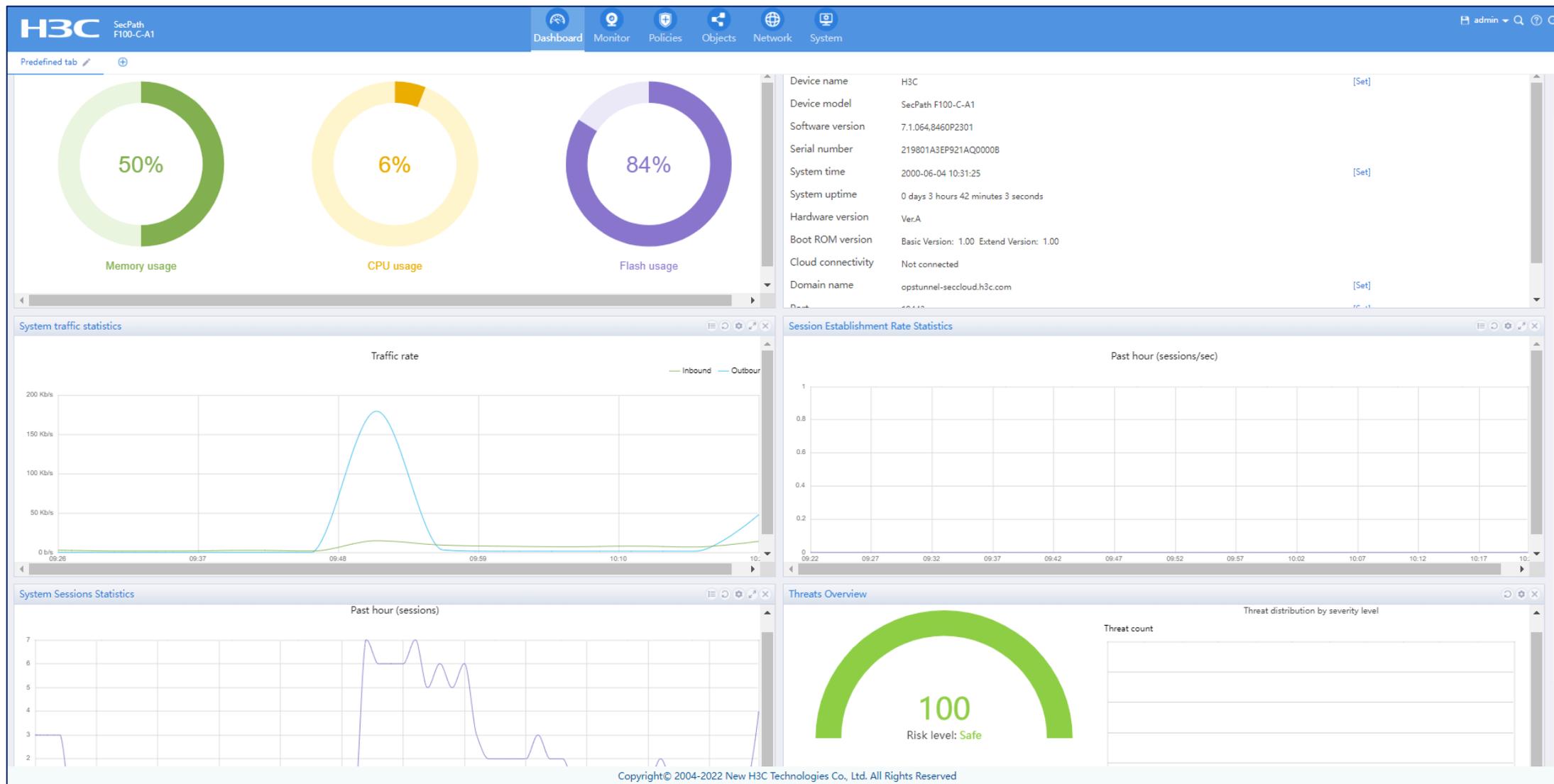
New Password:

Confirm Password:

Apply **Cancel**

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

ダッシュボードが表示されます





00 装置のGUIへアクセスする

01 装置ファイル(.did)のダウンロード

02 ライセンスリニューアル

03 ライセンスのインストール

04 シグネチャーの更新

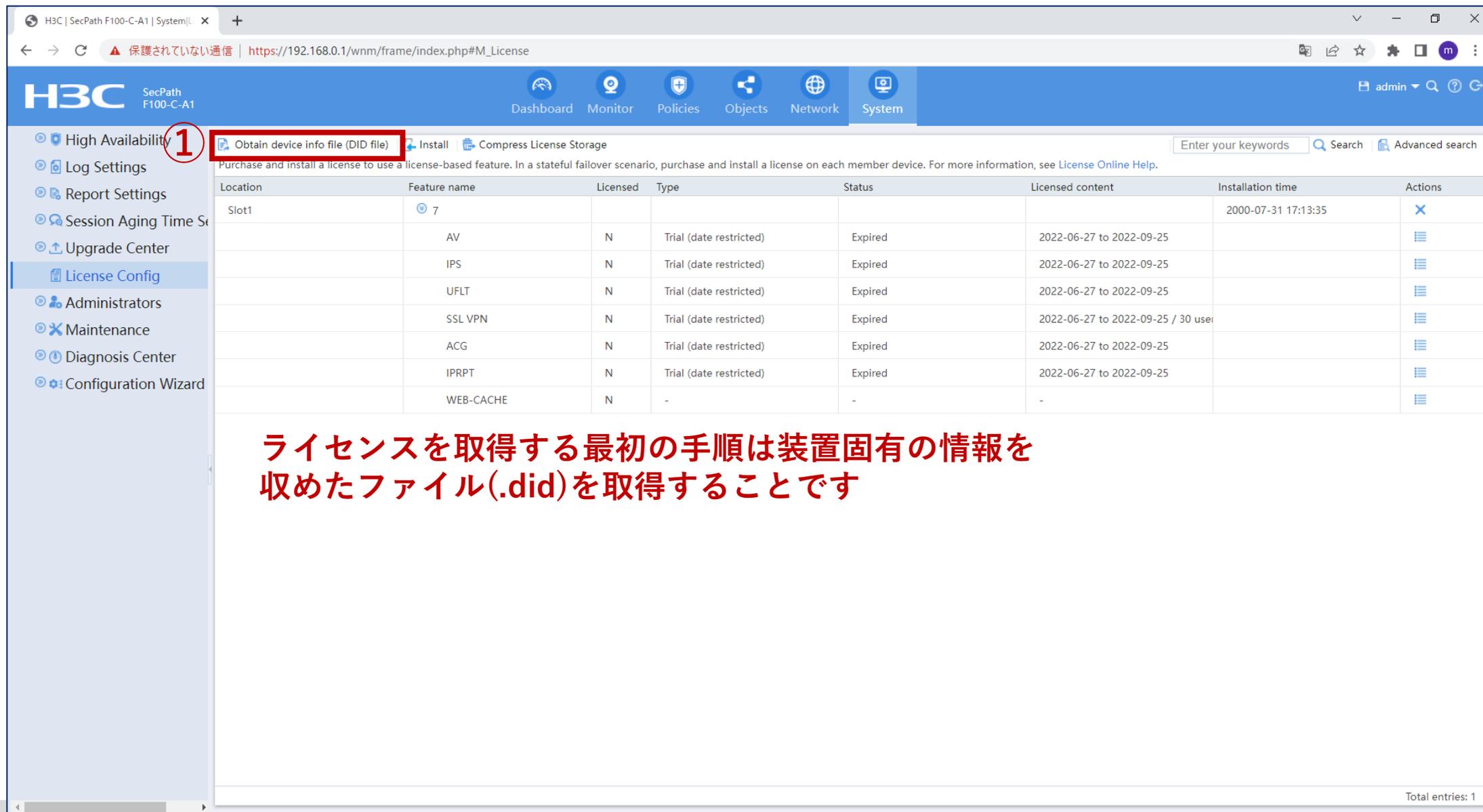
05 各種ログの環境整備

06 攻撃検証環境の整備

07 検証結果

08 トラブルシュート

ライセンスのインストーラーを取得するために装置固有の情報を取得する



The screenshot shows the H3C SecPath F100-C-A1 System Management interface. The left sidebar contains navigation options, with 'License Config' selected. The main content area shows the 'Obtain device info file (DID file)' button, which is highlighted with a red box and a circled '1'. Below this button is a table of license information for Slot1.

Location	Feature name	Licensed	Type	Status	Licensed content	Installation time	Actions
Slot1	7					2000-07-31 17:13:35	✕
	AV	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25		☰
	IPS	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25		☰
	UFLT	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25		☰
	SSL VPN	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25 / 30 use		☰
	ACG	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25		☰
	IPRPT	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25		☰
	WEB-CACHE	N	-	-	-		☰

ライセンスを取得する最初の手順は装置固有の情報を収めたファイル(.did)を取得することです

.didファイルのある場所を指定します

The screenshot shows the H3C SecPath F100-C-A1 System Management interface. The left sidebar contains navigation options: High Availability, Log Settings, Report Settings, Session Aging Time Settings, Upgrade Center, License Config (selected), Administrators, Maintenance, Diagnosis Center, and Configuration Wizard. The main content area displays the 'Obtain device info file (DID file)' section with a table of licenses. A dialog box titled 'Obtain Device Info File (DID File)' is open, showing the 'Location' dropdown set to 'Slot1' (marked with a red circle and '1'), 'Device SN' as '219801A3EP921AQ0000B', and 'DID file' as 'flash:/license/219801A3EP921AQ0000B.did'. The 'OK' button is highlighted with a red circle and '2'.

Location	Feature name	Licensed	Type	Status	Licensed content	Installation time	Actions
Slot1	7					2000-07-31 17:13:35	✕
	AV	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25		☰
	IPS	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25		☰
	UFLT	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25		☰
	SSL VPN	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25 / 30 users		☰
	ACG	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25		☰
	IPRPT				2022-06-27 to 2022-09-25		☰
	WEB-CACHE						☰

Obtain Device Info File (DID File)

Location **1** Slot1

Device SN 219801A3EP921AQ0000B

DID file **2** flash:/license/219801A3EP921AQ0000B.did

OK Cancel



00 装置のGUIへアクセスする

01 装置ファイル(.did)のダウンロード

02 ライセンスリニューアル

03 ライセンスのインストール

04 シグネチャーの更新

05 各種ログの環境整備

06 攻撃検証環境の整備

07 検証結果

08 トラブルシュート

事前にライセンスを購入しておきます。



ライセンスを購入するとライセンスキーが送付されてまいります。

https://www.h3c.com/en/Support/Online_Help/License_Service/Register_the_First_Time/

The screenshot shows the H3C website's 'Register Upgrade Licenses' page. The browser's address bar is highlighted with a red box and a circled '1'. The page content includes a navigation menu, a header, and a main section with instructions: 'Registers licenses for a device that has never been activated.' Below this, there is a breadcrumb trail: 'Home > Support > Online Help > License Service > Register Upgrade Licenses'. A grey box contains the text: 'To register add-ons, add-on features, or time extensions, please select a product category that has not previously been activated, please select First-Time Registration in the menu on the left.' The 'Select product category' section has a dropdown menu with 'Security_NG Firewall' selected, highlighted with a red box and a circled '2'. The 'Device information' section has a 'Device information file' field with a 'ファイルを選択' button highlighted by a red box and a circled '3'. An 'Upload' button is visible next to it. Overlaid on the right is a Windows File Explorer window showing the 'Downloads' folder. It contains a file named 'license_219801A3EP921AQ0000B.did' with a date of '2022/07/05 10:45'. The file name is highlighted with a red box and a circled '4'. The File Explorer's file name field at the bottom also contains the same file name and is highlighted with a red box.

ライセンス登録サイトにアクセスして.didファイルをアップロードします。

ライセンスファイル(excel形式)をアップロードします

License information

Upload license keys from ②

excel file [Download the template](#) ①

Input license keys or

select by sales contract

Product code

Description

ライセンスキーをExcelに以下のように記載

	A
1	31 30A4 D7-XpP@eWE\$-Nke kcxplo ENV-cM%aYjqa
2	31 30A4 E9-ivmE@GHYJM-MmWU5:\$k+r\$W%98
3	31 30A4 EA-7!ar#3 kKMhu8 qrcDV-Ujc855%A
4	31 30A4 EG-@4V*9djch6s+JLpCn-LX#JD+4#
5	31 30A4 EM-S7XBFshchfv#WKYDh+k\$invR6
6	31 30A4 EN-nqT FD&'(jhUSE@TE%-D@:UAT88
7	
8	
9	

必須項目を入力します

https://192.168.0.1/web/frame/en/... Support - Register Upgrade License

h3c.com/en/Support/Online_Help/License_Service/Register_Upgrade_Licenses/

H3C Products & Technology Solutions **Support** Training & Certification Partners About Us

Continue adding license key

Contact Information

Customer H3CTS
company/organization

Company/Organization h3c

First name h3c

Last name

Phone number 123

Email address gw.koshiromasahiro@h3c.com

Zip code

Address

Project name

Verify code 2164 2164

accept all terms of H3C Legal Statement *

Get activation key or file Cancel

① ② ③ ④

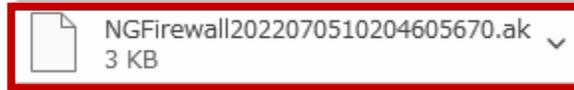
必須項目を入力して
Get activation key of file
をクリックすると入力した
Email address宛にインストレ
ーションファイル(.ak)ファイル
が添付されて送られてきます

インストールファイルがメールで送られてきます。

Your request for H3C device activation is approved.

license_master@h3c.com

宛先 test@gmail.com



H3CTS:

Thank you for using H3C products.

Your request for H3C device activation is approved.

Please see the attached file for the activation key for your product.

The following is your device and license key information.

Failover type: single

License key:

License key	Generated at	Product
-------------	--------------	---------

3130A4D7-/UiqLent-5C8%WR\$5-%FBkhD\$2		
---------------------------------------	--	--

2022/6/24 18:53:59	
--------------------	--

LIS-F100-BAS-TI-1Y

Device information file: license_219801A3EP921AQ0000B.did

Please do not reply to this email.

For comments or questions, please contact us through http://www.h3c.com/portal/About_H3C/Contact_Us.

H3C License Center

2022/7/5 10:20:46



00 装置のGUIへアクセスする

01 装置ファイル(.did)のダウンロード

02 ライセンスリニューアル

03 ライセンスのインストール

04 シグネチャーの更新

05 各種ログの環境整備

06 攻撃検証環境の整備

07 検証結果

08 トラブルシュート

ライセンスファイル(.ak)をインストールします。

The screenshot displays the H3C web management interface for a SecPath F100-C-A1 device. The 'License Config' section is active, showing a table of features and their license status. A red box highlights the 'Install' button, and a circled '1' is next to it. An 'Install License' dialog box is open, with a red box around the 'OK' button and a circled '3' next to it. A file explorer window is also open, showing the selection of the license file 'NGFirewall2022070510204605670.ak', with a red box around the filename and a circled '2' next to it.

Location	Feature name	Licensed	Type	Status	Licensed content	Installation time	Actions
Slot1	7						
	AV	N	Trial (date restricte				
	IPS	N	Trial (date restricte				
	UFLT	N	Trial (date restricte				
	SSL VPN	N	Trial (date restricte				
	ACG	N	Trial (date restricte				
	IPRPT	N	Trial (date restricte				
	WEB-CACHE						

購入したライセンスが有効になりました

The screenshot displays the H3C SecPath F100-C-A1 management interface. The left sidebar contains navigation options such as High Availability, Log Settings, Report Settings, Session Aging Time Settings, Upgrade Center, License Config (highlighted), Administrators, Maintenance, Diagnosis Center, and Configuration Wizard. The main content area shows a table of installed licenses with columns for Location, Feature name, Licensed, Type, Status, Licensed content, Installation time, and Actions. A red box highlights the 'Licensed' column, which contains 'Y' for AV, IPS, UFLT, and SSL VPN, and 'N' for IPRPT and WEB-CACHE. The table also shows two trial licenses for feature '7' installed on Slot1.

Location	Feature name	Licensed	Type	Status	Licensed content	Installation time	Actions
Slot1	7					2022-07-05 11:32:00	✕
Slot1	7					2022-07-07 09:30:18	✕
	AV	Y	Trial (date restricted)	In use	2022-07-07 to 2022-10-05		☰
	IPS	Y	Trial (date restricted)	In use	2022-07-07 to 2022-10-05		☰
	UFLT	Y	Trial (date restricted)	In use	2022-07-07 to 2022-10-05		☰
	SSL VPN	Y	Trial (date restricted)	In use	2022-07-07 to 2022-10-05 / 30 use		☰
	ACG	Y	Trial (date restricted)	In use	2022-07-07 to 2022-10-05		☰
	IPRPT	N	-	-	-		☰
	WEB-CACHE	N	-	-	-		☰

Total entries: 2

Copyright © 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved



00 装置のGUIへアクセスする

01 装置ファイル(.did)のダウンロード

02 ライセンスリニューアル

03 ライセンスのインストール

04 シグネチャーの更新

05 各種ログの環境整備

06 攻撃検証環境の整備

07 検証結果

08 トラブルシュート

シグネチャーデータベースへのアクセス確認

The screenshot shows the H3C SecPath F100-C-A1 management interface. The top navigation bar includes Dashboard, Monitor, Policies, Objects, Network, and System. The left sidebar lists various settings like High Availability, Log Settings, Report Settings, Session Aging Time Settings, Upgrade Center, License Config, Administrators, Maintenance, Diagnosis Center, and Configuration Wizard. The main content area displays a table of signature libraries with columns for Signature library, Current version, Release date, Auto update, Scheduled update time, and Actions. A red box highlights the 'Test signature library server connectivity' button, labeled with a circled '1'. Below the table, an 'Information' dialog box is open, containing the message 'The signature library server is correctly connected.' and a 'Close' button, labeled with a circled '2'.

Signature library	Current version	Release date	Auto update	Scheduled update time	Actions
IPS signature library	1.0.189	2022-07-04	<input type="checkbox"/>	-	Online update Manual update Roll back
Anti-virus signature library	1.0.158	2022-07-04	<input type="checkbox"/>	-	Online update Manual update Roll back
APR signature library	1.0.139	2022-06-21	<input type="checkbox"/>	-	Online update Manual update Roll back
URL filtering signature library	1.0.66	2022-05-26	<input type="checkbox"/>	-	Online update Manual update Roll back
URL reputation signature library	1.0.89	2022-07-04	<input type="checkbox"/>	-	Online update Manual update Roll back
Domain reputation signature library	1.0.189	2022-07-04	<input type="checkbox"/>	-	Online update Manual update Roll back
IP reputation signature library	1.0.189	2022-07-04	<input type="checkbox"/>	-	Online update Manual update Roll back

Information

The signature library server is correctly connected.

Close

Page 1 of 1 | Entries per page 25 | Displaying 1 - 7 of 7

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

シグネチャーを更新するためにSecPathがシグネチャーデータベースへアクセスできるかを確認する

シグネチャーの更新タイミングの設定

Refresh | Configure proxy server | Test signature library server connectivity

Signature library	Current version	Release date	Auto update	Scheduled update time	Actions
IPS signature library	1.0.189	2022-07-04	<input type="checkbox"/>	-	Online update Manual update Roll back
Anti-virus signature library	1.0.158	2022-07-04	<input type="checkbox"/>	-	Online update Manual update Roll back
APR signature library	1.0.139	2022-06-21	<input type="checkbox"/>	-	Online update Manual update Roll back
URL filtering signature library	1.0.66	2022-05-26	<input type="checkbox"/>	-	Online update Manual update Roll back
URL reputation signature library	1.0.89	2022-07-04	<input type="checkbox"/>	-	Online update Manual update Roll back
Domain reputation signature library	1.0.189	2022-07-04	<input type="checkbox"/>	-	Online update Manual update Roll back
IP reputation signature library	1.0.83	2022-06-30	<input type="checkbox"/>	-	Online update Manual update Roll back

Configure Scheduled Update For IPS Signature Library

Scheduled update time: 2 0 0 (hh/mm/ss)

シグネチャーの更新方法

手動

- オンラインで即実行
- H3Cのサイトからダウンロードしたシグネチャーファイルを読み込んで更新
- 1世代前のシグネチャーに戻す

自動

更新する日(毎日、毎月曜日、毎火曜日、毎水曜日、毎木曜日、毎金曜日、毎土曜日、毎日曜日)、時間を指定して自動的に実行

Page 1 of 1 | Entries per page 25 | Displaying 1 - 7 of 7

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

https://www.h3c.com/en/Support/Resource_Center/Software_Download/Security/

Home > Support > Resource Center > Software Download > Security

H3C SecPath F5000 Firewall Series

F5000
[Learn More →](#)

H3C SecPath F1000-AI Firewall Series

F1000-AI
[Learn More →](#)

H3C SecPath F1000 Firewall Series

F1000
[Learn More →](#)

Signature Database Services

Signature Database Services
[Learn More →](#)

シグネチャーを手動で更新するためのシグネチャーがダウンロードできるサイトにアクセスする

シグネチャーファイルのダウンロード

Signature Database Services			
	Title	Date	Downloads
→ IPS Signature V7-IPS-1.0.189	必要なシグネチャーファイルを ダウンロードする	04-07-2022	↓
→ IPS Signature V7-IPS-1.0.188		02-07-2022	↓
→ Anti-Virus Signature V7-AV-1.0.157		01-07-2022	↓
→ Anti-Virus Signature V7-AV-H-1.0.157		01-07-2022	↓
→ WAF Signature V7-WAF-1.0.18		30-06-2022	↓
→ Anti-Virus Signature V7-AV-1.0.156		29-06-2022	↓
→ Anti-Virus Signature V7-AV-H-1.0.156		29-06-2022	↓
→ Application Signature V7-APR-1.0.139		28-06-2022	↓
→ IPS Signature V7-IPS-1.0.187		26-06-2022	↓
→ Anti-Virus Signature V7-AV-1.0.155		24-06-2022	↓
→ Anti-Virus Signature V7-AV-H-1.0.155		23-06-2022	↓
→ Anti-Virus Signature V7-AV-1.0.154		22-06-2022	↓
→ Anti-Virus Signature V7-AV-H-1.0.154		22-06-2022	↓



00 装置のGUIへアクセスする

01 装置ファイル(.did)のダウンロード

02 ライセンスリニューアル

03 ライセンスのインストール

04 シグネチャーの更新

05 各種ログの環境整備

06 攻撃検証環境の整備

07 検証結果

08 トラブルシュート

ログの種類と適用のシナリオ

ログの種類	簡単な紹介	出力方法	適用のシナリオ
System log	システムログ (Syslog) は各サービスモジュールによって生成されたイベントまたは統計を記録します	システムログは、インフォメーションセンターモジュールを介してASCII形式で端末、コンソール、およびその他の宛先を監視するために出力されます。	デバイスの日常のメンテナンスと監視が必要なシナリオに適用できます。
Flow log	フローログ (User log) は、フローに基づいてセッション情報を記録します。フローログエントリには、セッションパケットの5つの情報とトラフィック統計が含まれます	フローログはログホストに出力されるか、インフォメーションセンターに送信され、フローログモジュールを介してより効果的なバイナリ形式でさらに処理されます。	多数のセッションの統計分析とパケットトレサビリティが必要なシナリオに適用できます。
Fast log	高速ログ (FastlogまたはCustomlog) は、ほとんどのセキュリティサービスモジュールによって生成された統計またはイベントを記録します。	高速ログは、高速ログ出力モジュールを介してASCII形式でインフォメーションセンターではなくログホストに出力されます。出力効率が高い。	セキュリティサービスモジュールの処理結果を監査、監視、および分析する必要があるシナリオに適用できます
Data analysis center log	データ分析センターのログは、デバイスによって生成されたイベントまたは統計をインテリジェントに分析し、分析結果を視覚的に表示します。	ログは、データ分析センターモジュールを介してさまざまなチャートや表でWebインターフェイスに表示されます。	ログ分析を視覚的に表示するシナリオに適用可能デバイスのWebインターフェイスでの結果が必要です。

syslogサーバーのアドレス設定

The screenshot displays the H3C SecPath F100-C-A1 web management interface. The top navigation bar includes icons for Dashboard, Monitor, Policies, Objects, Network, and System. The left sidebar shows a tree view with 'Log Settings' selected. The main content area is titled 'Syslog' and contains several configuration options and a table.

Numbered callouts indicate the following steps:

1. Click the 'System' icon in the top navigation bar.
2. Click 'Log Settings' in the left sidebar.
3. Click the 'Syslog' tab in the main content area.
4. Check the 'Output to log buffer' checkbox.
5. Click the 'Create' button to add a new log host entry.

The 'Log buffer size' is set to 512 entries (0-1024, Default: 512). Below the 'Apply' button, there is a table for log host addresses:

Log host address	Port number	VRF	Edit
<input type="checkbox"/> 192.168.0.254	514	Public network	

ログに書き出す検知情報の指定

① System

② Log Settings

③ Fast Log Output

Syslog Flow Log **Fast Log Output** Storage Space Settings

Log timestamp Greenwich Mean Time (GMT) Local time

Source IP for log packets

Log character encoding

Apply

+ Create X Delete

<input type="checkbox"/>	Log ...	Port...	VRF	Sess...	Atta...	Rep...	AFT...	URL...	App...	Net...	Tele...	Tele...	CM...	CM...	Uni...	Uni...	Sec...
<input type="checkbox"/>	19...	514	P...	✓	✓	✓	✓	✓	✓	✓	⊖	⊖	⊖	⊖	✓	✓	✓

ログに書き出す検知情報の指定(続き)

Edit Log Host

Log host address *(1-253 chars)

Port number (1-65535. Default: 514.)

VRF

Session logs

NAT logs

Log format

NAT session logs

NAT444 user logs

AFT logs

Application audit logs

URL filtering logs

Attack defense logs

Reputation Logs

Netshare logs

OK Cancel

①

②

Edit Log Host

Security policy configuration logs

Heartbeat logs

IPS logs

Bandwidth management logs

Sandbox logs

LB logs

SLB logs

Inbound link LB logs

Outbound LB logs

Transparent DNS Proxy logs

Terminal identification logging

Anti-virus logs

External authentication logs

Notification logs

OK Cancel

③

④

ログに書き出す検知情報の指定(続き)

The screenshot displays the configuration interface for H3C SecPath F100-C-A1. The left sidebar shows a navigation menu with 'Log Settings' expanded to 'Threat Log Settings'. The main content area is divided into two sections: 'IPS logs' and 'Anti-virus logs'. In both sections, the 'Log type' is set to 'System log', which is highlighted with a red box and a circled number (1 for IPS, 2 for Anti-virus). Below each section, there are checkboxes for 'Output through email' and 'Output logs in Chinese'. A red warning message is present below each 'Log type' selection, stating: 'Opening the system log may affect the performance of the device. It is recommended to enable the quick log.' An 'Apply' button is located at the bottom of the Anti-virus logs section.

H3C SecPath F100-C-A1

Dashboard Monitor Policies Objects Network System

High Availability

Log Settings

- Basic Settings
- Email Server
- Session Log Settings
- NAT Log Settings
- AFT Log Settings
- SandBox Log Settings
- Threat Log Settings
- Application Audit Log
- URL Filtering Log Settings
- Attack Defense Log Settings
- Reputation Log Settings
- Bandwidth Alarm Settings
- Configuration Logs Settings

IPS logs

Log type System log **1** Fast log

Opening the system log may affect the performance of the device. It is recommended to enable the quick log.

Output through email

Output logs in Chinese ?

Anti-virus logs

Log type System log **2** Fast log

Opening the system log may affect the performance of the device. It is recommended to enable the quick log.

Output through email

Apply

ログに書き出す検知情報の指定(続き)

The screenshot displays the configuration interface for H3C SecPath F100-C-A1. The left sidebar shows the navigation menu with 'Log Settings' expanded and 'Attack Defense Log Settings' selected. The main content area is divided into three sections: 'Log type', 'Blacklist log settings', and 'Attack defense log settings'. In the 'Log type' section, 'System log' is selected and circled with a red box and the number '1'. Below it, a red warning message states: 'Opening the system log may affect the performance of the device. It is recommended to enable the quick log.' In the 'Blacklist log settings' section, two checkboxes are checked and circled with a red box and the number '2': 'Log aggregation for single-packet attack' and 'Enable blacklist logging'. Below these checkboxes is an 'Apply' button. The 'Attack defense log settings' section contains three input fields: 'Log buffer size' (512), 'Log file size' (1), and 'Log file usage alarm threshold' (80), each with a corresponding unit and range. An 'Apply' button is located below these fields.

H3C SecPath F100-C-A1

Dashboard Monitor Policies Objects Network System

High Availability

Log Settings

- Basic Settings
- Email Server
- Session Log Settings
- NAT Log Settings
- AFT Log Settings
- SandBox Log Settings
- Threat Log Settings
- Application Audit Log
- URL Filtering Log Settings
- Attack Defense Log Settings
- Reputation Log Settings
- Bandwidth Alarm Settings
- Configuration Logs Settings
- Security Policy Log Settings
- Heartbeat Log Settings
- IP Access Log
- MAC Access Log
- LB Log
- Bandwidth Management
- Trusted Access Control

Log type System log Fast log

Opening the system log may affect the performance of the device. It is recommended to enable the quick log.

Log aggregation for single-packet attack

Enable blacklist logging

Apply

Blacklist log settings

Log buffer size *entries (0-1024)

Log file size *MB (1-10)

Log file usage alarm threshold *% (0-100)

Apply

Attack defense log settings

Log buffer size *entries (0-1024)

Log file size *MB (1-10)

Log file usage alarm threshold *% (0-100)

Apply

usba0:/のディスク使用状況

H3C SecPath F100-C-A1

Dashboard Monitor Policies Objects Network System

Syslog Flow Log Fast Log Output **Storage Space Settings**

Storage space usage

Total storage space:28.89GB
Used space:65.98MB
Available space:28.83GB

- threat
- url_filter
- traffic_log
- file_filter
- terminal
- Server farm member trend statistics
- Server farm member stability trend statistics
- HTTP delay trend statistics
- Link application traffic statistics
- IPCAR TopN statistics
- Others
- Available space

Before unplugging the storage device, you must click **Unload** to avoid file system corruption.

Service	Max storage days (1-65535)	Max storage space (%)	Action	Used space (%)	Enable	Edit
dpi threat	365	20	Delete	0.0	<input checked="" type="checkbox"/>	
dpi url_filter	365	20	Delete	0.0	<input checked="" type="checkbox"/>	
device-log traffic_log	365	20	Delete	0.0	<input checked="" type="checkbox"/>	
dpi file_filter	365	20	Delete	0.0	<input type="checkbox"/>	
dpi terminal	365	20	Delete	0.0	<input type="checkbox"/>	
Loadbalance log information Server far...	365	20	Delete	0.0	<input type="checkbox"/>	
Loadbalance log information Server far...	365	20	Delete	0.0	<input type="checkbox"/>	

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

ログファイル: flash:/

<H3C>dir

Directory of flash: (VFAT)

```
0 drw-      - Oct 05 2022 23:58:38  WEB
1 drw-      - Jul 13 2022 01:18:06  diagfile
2 drw-      - Jul 08 2022 00:08:18  dpi
3 -rw-      677 Oct 07 2022 20:01:10  ifindex.dat
4 -rw-      1808 Mar 02 2021 01:54:00  licbackup
5 drw-      - Mar 02 2021 01:54:00  license
6 -rw-      1808 Mar 02 2021 01:54:00  licnormal
7 drw-      - Sep 29 2022 19:50:50  logfile
8 drw-      - Mar 02 2021 01:54:06  pki
9 drw-      - Mar 02 2021 01:54:00  seclog
10 -rw-      0 Mar 02 2021 01:54:00  sim_f1000_fw-cmw710-boot-a6401.bin
11 -rw-      0 Mar 02 2021 01:54:00  sim_f1000_fw-cmw710-system-a6401.bin
12 -rw-      11114 Oct 07 2022 20:01:10  startup.cfg
13 -rw-      275050 Oct 07 2022 20:01:10  startup.mdb
14 drw-      - Oct 12 2022 13:49:12  webtmp
```

1046512 KB total (869820 KB free)

<H3C>

ログファイル: flash:/dpi

<H3C>**dir dpi**

Directory of flash:/dpi

```
0 drw-      - Jul 08 2022 00:08:18  apr
1 drw-      - Jul 08 2022 00:08:18  audit
2 drw-      - Jul 08 2022 00:08:18  av
3 drw-      - Jul 08 2022 00:08:18  dnsreputation
4 -rw-     30 Dec 10 2022 07:50:42  dpi_sigpack.log
5 drw-      - Jul 08 2022 00:08:18  filereg
6 drw-      - Jul 08 2022 00:08:18  ipreputation
7 drw-      - Jul 08 2022 00:08:18  ips
8 drw-      - Jul 08 2022 00:08:18  netshare
9 drw-      - Jul 08 2022 00:08:18  uflt
10 drw-     - Jul 08 2022 00:08:18  urlreputation
11 drw-     - Jul 08 2022 00:08:18  waf
```

1046512 KB total (869820 KB free)

<H3C>**dir dpi/ips**

Directory of flash:/dpi/ips

```
0 drw-      - Jul 08 2022 00:08:18  pcap
1 drw-      - Oct 01 2022 06:57:02  predefined
2 drw-      - Jul 08 2022 00:08:18  snort
```

1046512 KB total (869820 KB free)

<H3C>

ログファイル: flash:/logfile

<H3C>**dir logfile/**

Directory of flash:/logfile

```
0 -rw-      917 Sep 29 2022 19:50:50  atk_scan.log
1 -rw-     10860 Oct 01 2022 08:30:28  atk_single.log
2 -rw-     14074 Oct 01 2022 08:30:28  cfglog.log
3 -rw-     48806 Oct 01 2022 08:30:28  logfile.log
```

1046512 KB total (869820 KB free)

<H3C>**more logfile/atk_scan.log**

%@1%Sep 29 10:48:07:540 2022 H3C ATK/3/ATK_IP4_**PORTSCAN**_SZ: SubModule(1127)=SCAN;

SrcZoneName(1025)=Management; Protocol(1001)=TCP; SrcIPAddr(1003)=192.168.56.254;

SndDSLiteTunnelPeer(1041)=--; RcvVPNInstance(1042)=; DstIPAddr(1007)=192.168.56.1; Action(1053)=logging,drop;

BeginTime_c(1011)=20220929104807.

%@2%Sep 29 10:48:19:079 2022 H3C ATK/3/ATK_IP4_PORTSCAN_SZ: SubModule(1127)=SCAN;

SrcZoneName(1025)=Local; Protocol(1001)=TCP; SrcIPAddr(1003)=192.168.56.254; SndDSLiteTunnelPeer(1041)=--;

RcvVPNInstance(1042)=; DstIPAddr(1007)=192.168.56.1; Action(1053)=logging,drop;

BeginTime_c(1011)=20220929104819.

ログファイル: sda0:/



```
<H3C>dir sda0:/  
Directory of sda0: (VFAT)  
 0 drw-      - Jul 04 2022 09:57:22  System Volume Information  
 1 drw-      - Jul 06 2022 10:04:16  seclog
```

```
<H3C>dir sda0:/seclog  
Directory of sda0:/seclog  
 0 -rw-      838 Jul 07 2022 12:09:38  anti-vir.log  
 1 -rw-     42868 Jul 07 2022 12:09:38  atk_flood.log  
 2 -rw-     95856 Jul 07 2022 12:09:38  cfglog.log  
 3 -rw-      639 Jul 07 2022 12:09:38  ips.log  
 4 -rw-     33971 Jul 07 2022 12:09:38  logfile.log  
 5 -rw-      339 Jul 07 2022 12:09:38  uflt.log
```

```
31184896 KB total (31184608 KB free)
```

ログファイル: usba0:/



```
<H3C>dir usba0:/
Directory of usba0: (VFAT)
 0 drw-      - Jul 05 2022 21:39:16  System Volume Information
 1 drw-      - Jul 07 2022 10:14:18  ntop_database
 2 drw-      - Jul 05 2022 21:39:28  seclog
```

```
<H3C>dir usba0:/ntop_database/
Directory of usba0:/ntop_database
 0 -rw-      20480 Jul 07 2022 10:14:18  Analysis.event
 1 -rw-      4096 Jul 07 2022 10:14:14  app.db
 2 -rw-     32768 Jun 04 2000 06:51:05  app.db-shm
 3 -rw-    832272 Jun 04 2000 06:51:05  app.db-wal
 4 drw-      - Jul 07 2022 10:14:04  attack-defense-blacklist
 5 drw-      - Jul 07 2022 10:13:40  attack-defense-flood
 6 drw-      - Jul 07 2022 10:13:52  attack-defense-ipcar_alarm
 7 drw-      - Jul 07 2022 10:13:40  attack-defense-ipcar_statistics
 8 drw-      - Jul 07 2022 10:13:42  attack-defense-scan
 9 drw-      - Jul 07 2022 10:14:06  attack-defense-signature
10 drw-      - Jul 07 2022 10:13:40  audit
11 drw-      - Jul 07 2022 10:13:46  botnet-detect-botnetinfo
12 drw-      - Jul 07 2022 10:14:14  botnet-detect-exception
13 drw-      - Jul 07 2022 10:14:14  botnet-detect-globalinfo
14 drw-      - Jul 07 2022 10:14:14  botnet-detect-riskscore
15 drw-      - Jul 07 2022 10:13:54  botnet-detect-threatost
16 drw-      - Jul 07 2022 10:14:06  dpi-reputation
17 drw-      - Jul 07 2022 10:13:42  dpi-terminal
18 -rw-    28672 Jul 07 2022 10:14:16  event_analysis.pool
19 drw-      - Jul 07 2022 10:14:14  file-filter
20 drw-      - Jul 07 2022 10:14:08  lb-SSL
21 drw-      - Jul 07 2022 10:13:42  lb-cache
22 drw-      - Jul 07 2022 10:13:40  lb-dnsproxy
23 drw-      - Jul 07 2022 10:14:04  lb-dnsresponse
24 drw-      - Jul 07 2022 10:13:42  lb-domain
25 drw-      - Jul 07 2022 10:13:44  lb-http
26 drw-      - Jul 07 2022 10:13:42  lb-link
27 drw-      - Jul 07 2022 10:13:40  lb-linkapp
28 drw-      - Jul 07 2022 10:13:56  lb-linkinfo
29 drw-      - Jul 07 2022 10:13:42  lb-linkmatchclass
30 drw-      - Jul 07 2022 10:13:42  lb-linkstatus
31 drw-      - Jul 07 2022 10:13:54  lb-linkwarning
32 drw-      - Jul 07 2022 10:13:42  lb-member
33 drw-      - Jul 07 2022 10:13:48  lb-memberstatus
34 drw-      - Jul 07 2022 10:13:42  lb-nodewarning
35 drw-      - Jul 07 2022 10:13:42  lb-outbound
36 drw-      - Jul 07 2022 10:13:58  lb-overviewdomain
37 drw-      - Jul 07 2022 10:13:42  lb-overviewlink
38 drw-      - Jul 07 2022 10:13:42  lb-overviewmember
39 drw-      - Jul 07 2022 10:13:42  lb-overviews
40 drw-      - Jul 07 2022 10:13:42  lb-overviewsf
41 drw-      - Jul 07 2022 10:13:40  lb-overviewws
42 drw-      - Jul 07 2022 10:13:42  lb-protectattack
43 drw-      - Jul 07 2022 10:13:40  lb-protectwarning
44 drw-      - Jul 07 2022 10:14:12  lb-realserver
45 drw-      - Jul 07 2022 10:13:42  lb-rsstatus
46 drw-      - Jul 07 2022 10:13:42  lb-serverfarm
47 drw-      - Jul 07 2022 10:13:42  lb-serverfarmstatus
48 drw-      - Jul 07 2022 10:13:40  lb-virtualserver
49 drw-      - Jul 07 2022 10:13:42  lb-virtualserverstatus
50 drw-      - Jul 07 2022 10:14:14  maintenance
51 drw-      - Jul 07 2022 10:13:52  nat-flow_log
52 drw-      - Jul 07 2022 10:13:42  packet-filter-
security_policy
53 drw-      - Jul 07 2022 10:14:04  sandbox-detail
54 drw-      - Jul 07 2022 10:13:42  sandbox-log
55 drw-      - Jul 07 2022 10:14:00  security-policy-counting
56 drw-      - Jul 07 2022 10:13:40  syslog-cfglog
57 drw-      - Jul 07 2022 10:13:42  syslog-syslog
58 drw-      - Jul 07 2022 10:14:14  threat
59 drw-      - Jul 07 2022 10:14:14  traffic
60 drw-      - Jul 07 2022 10:14:14  url-filter
30294000 KB total (30226768 KB free)
```

```
Jul 05 16:09:00 192.168.0.1 Jul 5 16:07:38 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705160738.
Jul 05 16:10:58 192.168.0.1 Jul 5 16:09:36 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705160936.
Jul 05 16:20:04 192.168.0.1 Jul 6 01:18:42 2022 H3C %%10NTP/5/NTP_LEAP_CHANGE: System Leap Indicator changed from 3 to 0 after clock update.
Jul 05 16:20:04 192.168.0.1 Jul 6 01:18:42 2022 H3C %%10NTP/5/NTP_STRATUM_CHANGE: System stratum changed from 16 to 8 after clock update.
Jul 05 16:20:33 192.168.0.1 Jul 6 01:19:12 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220706011912.
Jul 05 16:21:43 192.168.0.1 Jul 5 16:20:21 2022 H3C %%10NTP/5/NTP_LEAP_CHANGE: System Leap Indicator changed from 3 to 0 after clock update.
Jul 05 16:21:43 192.168.0.1 Jul 5 16:20:21 2022 H3C %%10NTP/5/NTP_STRATUM_CHANGE: System stratum changed from 16 to 8 after clock update.
Jul 05 16:22:32 192.168.0.1 Jul 5 16:21:10 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705162110.
Jul 05 16:32:07 192.168.0.1 Jul 5 16:30:45 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705163045.
Jul 05 16:34:05 192.168.0.1 Jul 5 16:32:43 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705163243.
Jul 05 16:43:40 192.168.0.1 Jul 5 16:42:19 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705164219.
Jul 05 16:45:39 192.168.0.1 Jul 5 16:44:17 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705164417.
Jul 05 16:55:14 192.168.0.1 Jul 5 16:53:52 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705165352.
Jul 05 16:57:12 192.168.0.1 Jul 5 16:55:51 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705165551.
Jul 05 17:06:47 192.168.0.1 Jul 5 17:05:26 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705170526.
Jul 05 17:08:46 192.168.0.1 Jul 5 17:07:24 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705170724.
Jul 05 17:18:21 192.168.0.1 Jul 5 17:16:59 2022 H3C %%10ATK/3/ATK_ICMP_FLOOD_SZ: AtkDirection(1134)=Destination; SrcZoneName(1025)=Management; SrcIPAddr(1003)=; DstIPAddr(1007)=224.0.0.2; RcvVPNInstance(1042)=; UpperLimit(1049)=1; Action(1053)=logging,drop; BeginTime_c(1011)=20220705171659.
```



00 装置のGUIへアクセスする

01 装置ファイル(.did)のダウンロード

02 ライセンスリニューアル

03 ライセンスのインストール

04 シグネチャーの更新

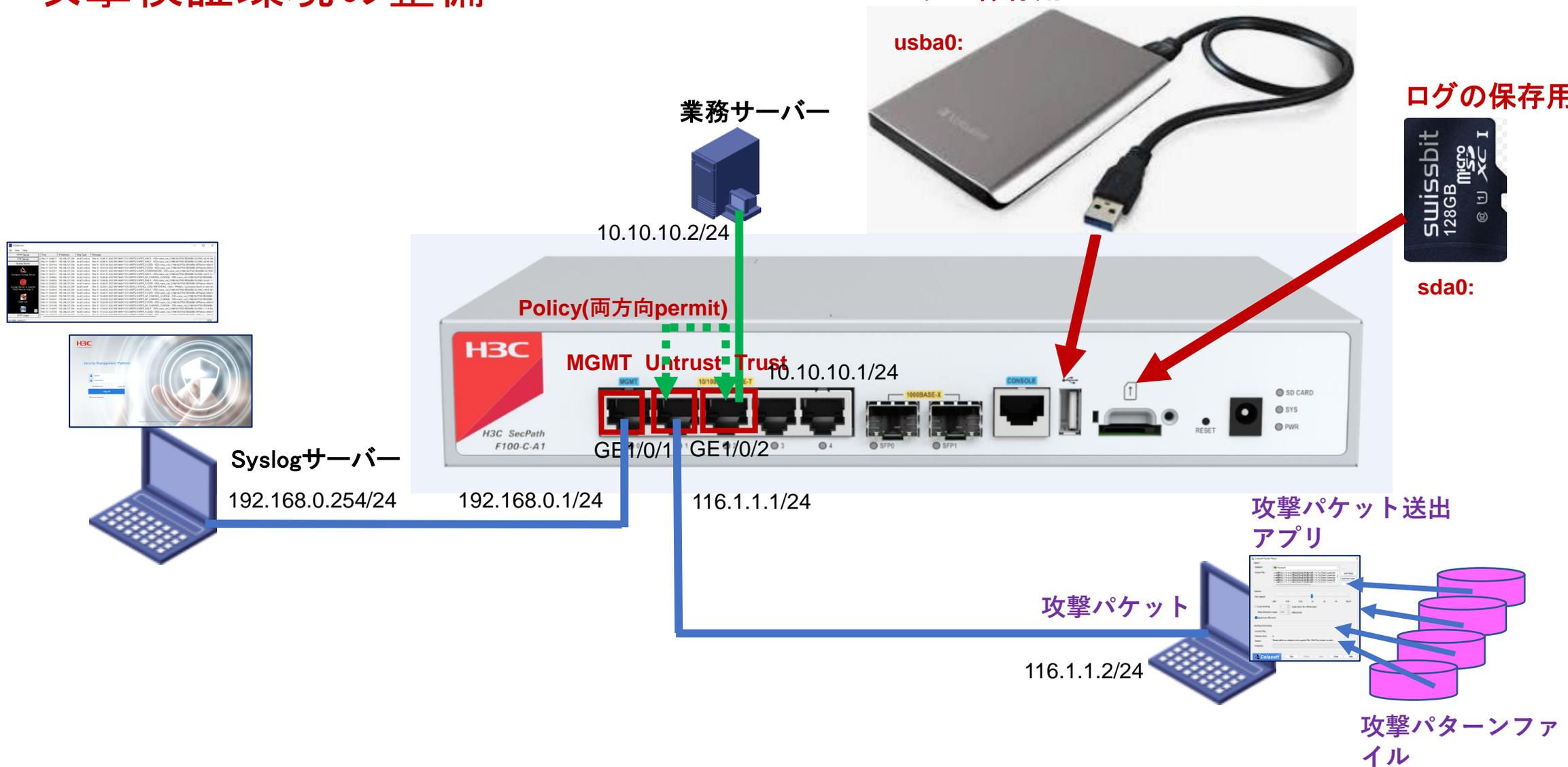
05 各種ログの環境整備

06 攻撃検証環境の整備

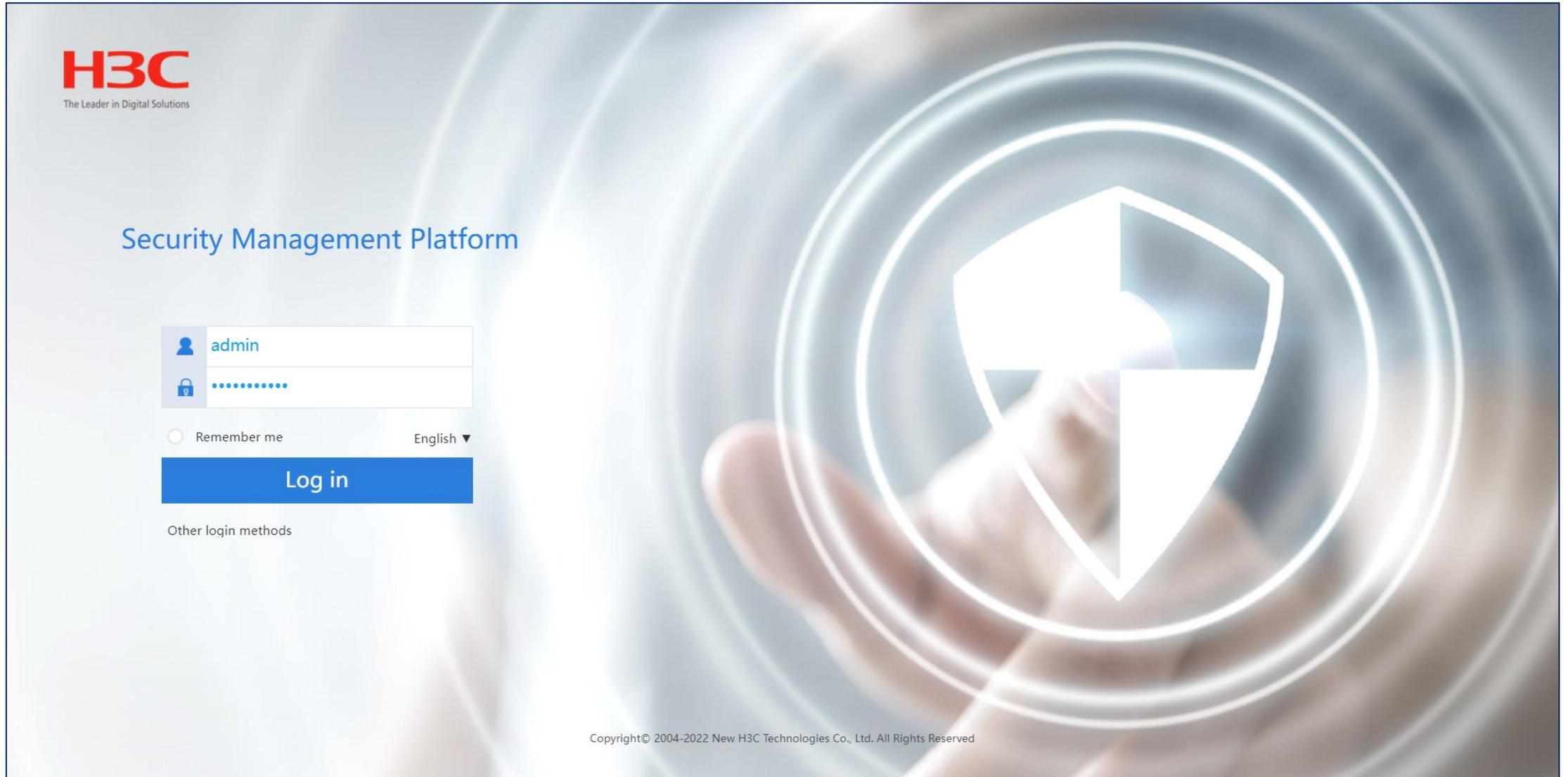
07 検証結果

08 トラブルシュート

攻撃検証環境の整備



https://192.168.0.1/でGUIにアクセス



初期パスワードの変更

The screenshot shows the H3C Security Management Platform login interface. The H3C logo is in the top left, with the tagline 'The Leader in Digital Solutions'. The main heading is 'Security Management Platform'. The login form includes a username field with 'admin', a password field with masked characters, a 'Remember me' checkbox, and a language dropdown set to 'English'. A blue 'Log in' button is present, along with a link for 'Other login methods'. A 'Change Password' dialog box is open in the center, displaying password requirements and three input fields for 'Old Password', 'New Password', and 'Confirm Password'. The dialog has 'Apply' and 'Cancel' buttons.

H3C
The Leader in Digital Solutions

Security Management Platform

admin

.....

Remember me English ▼

Log in

[Other login methods](#)

Change Password

The default password is not secure. A qualified password must meet the following requirements: It must contain a minimum of 10 characters. It must contain a minimum of 2 types, and a minimum of 1 characters for each type. It can't contain the username or the reversed letters of the username.

Old Password:

New Password:

Confirm Password:

Apply **Cancel**

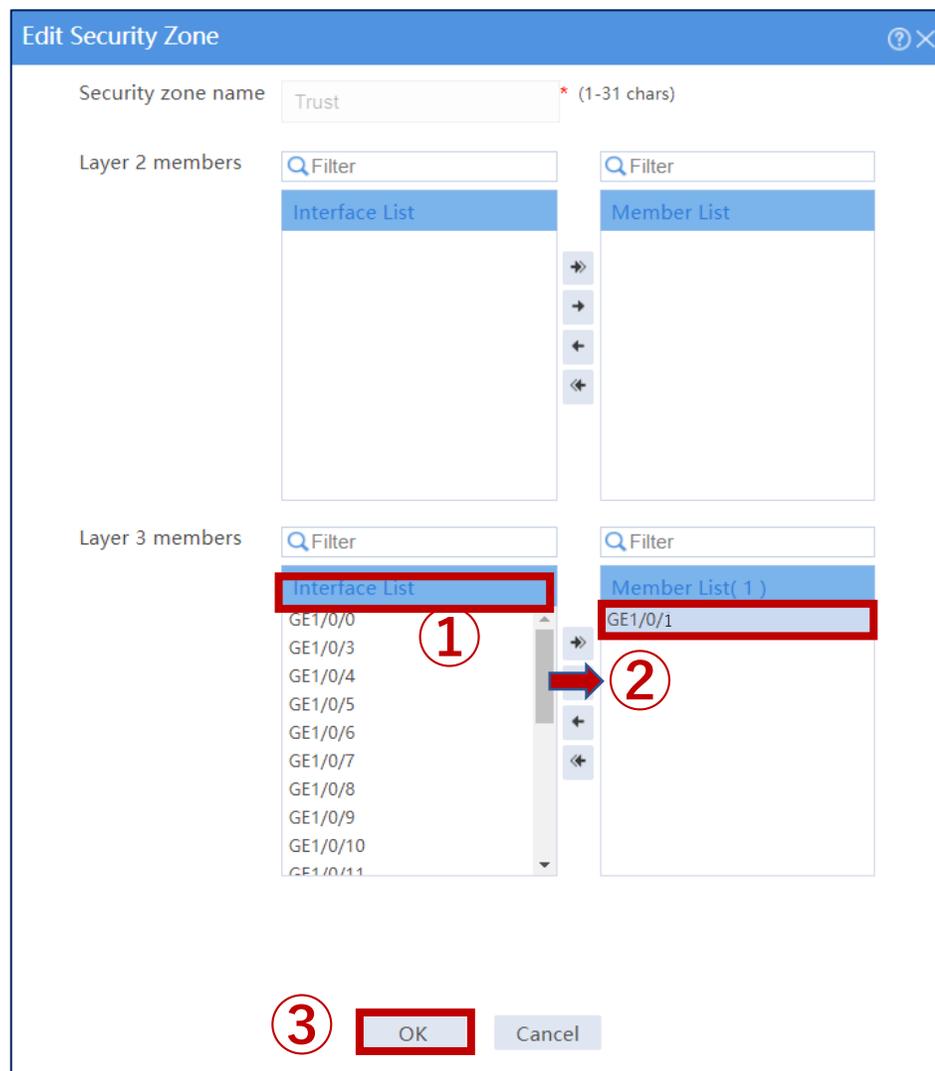
Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

GE1/0/1をUntrustゾーンに割り当ててIPアドレスを割り当てます

The screenshot displays the H3C Network Configuration interface. The 'Network' menu item is highlighted with a red box and a circled '1'. In the left sidebar, 'Interface Configuration' is highlighted with a red box and a circled '2', and 'Security Zones' is selected. The main content area shows a table of security zones. The 'unturst' zone is highlighted with a red box, and its 'Edit' icon is also highlighted with a red box and a circled '3'.

Security zone	Number of members	Members	Edit
<input type="checkbox"/> Local	--		
<input type="checkbox"/> Trust	0		
<input type="checkbox"/> DMZ	0		
<input type="checkbox"/> Untrust	0		
<input type="checkbox"/> Management	0		
<input type="checkbox"/> unturst	0		

GE1/0/1をUntrustゾーンに割り当ててIPアドレスを割り当てます



GE1/0/1をUntrustゾーンに割り当ててIPアドレスを割り当てます

The screenshot displays the H3C Network Configuration interface. The 'Network' tab is selected, and the 'Interface Configuration' section is active. The 'Interfaces' sub-section is highlighted. A table lists various interfaces, with GE1/0/1 highlighted in red. The 'Security zone' for GE1/0/1 is 'Untrust'. The 'Status' is 'Up'. The 'IP address' is empty. The 'Edit' icon for GE1/0/1 is also highlighted in red. The interface includes a search bar and various navigation icons.

①

②

③

Interface	Security zone	Status	IP address	Speed(kbps)	Link mode	Duplex ...	Loopbac...	Protocol exceptions		Description	Edit
								Received	Originated		
<input type="checkbox"/> GE1/0/0		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/0 Interface	
<input type="checkbox"/> GE1/0/1	Untrust	Up	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/1 Interface	
<input type="checkbox"/> GE1/0/2	Trust	Up	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/2 Interface	
<input type="checkbox"/> GE1/0/3		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/3 Interface	
<input type="checkbox"/> GE1/0/4		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/4 Interface	
<input type="checkbox"/> GE1/0/5		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/5 Interface	
<input type="checkbox"/> GE1/0/6		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/6 Interface	
<input type="checkbox"/> GE1/0/7		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/7 Interface	
<input type="checkbox"/> GE1/0/8		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/8 Interface	
<input type="checkbox"/> GE1/0/9		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/9 Interface	
<input type="checkbox"/> GE1/0/10		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/10 Interface	
<input type="checkbox"/> GE1/0/11		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/11 Interface	
<input type="checkbox"/> GE1/0/12		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/12 Interface	
<input type="checkbox"/> GE1/0/13		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/13 Interface	
<input type="checkbox"/> GE1/0/14		Down	--	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/14 Interface	

GE1/0/1をUntrustゾーンに割り当ててIPアドレスを割り当てます

Modify Interface Settings

Name: GE1/0/1

Link status: Up Shut down

Description: GigabitEthernet1/0/1Interface

Link mode: Layer 3 mode

Security zone: **1** Untrust

Protocol exceptions

Received: Telnet Ping SSH HTTP HTTPS SNMP
 NETCONF over HTTP NETCONF over HTTPS NETCONF over SSH

Originated: Telnet Ping SSH HTTP HTTPS

Basic Configuration: **2** IPv4 Address IPv6 Address Physical Interface Configuration

IP address: Manual assignment DHCP PPPoE

IP address/mask length: **3** 116.1.1.1 / 255.255.255.0

Gateway:

<input type="checkbox"/>	Secondary IP address	Mask length	Edit
--------------------------	----------------------	-------------	------

4

GE1/0/2をTrustゾーンに割り当ててIPアドレスを割り当てます

The screenshot shows the H3C Network Management System interface. The top navigation bar includes Dashboard, Monitor, Policies, Objects, Network (selected), and System. The left sidebar shows various configuration options, with 'Security Zones' selected. The main content area displays a table of security zones.

Security zone	Number of members	Members	Edit
<input type="checkbox"/> Local	--		
<input type="checkbox"/> Trust	0		
<input type="checkbox"/> DMZ	0		
<input type="checkbox"/> Untrust	1	GE1/0/1	
<input type="checkbox"/> Management	0		
<input type="checkbox"/> unturst	0		

GE1/0/2をTrustゾーンに割り当ててIPアドレスを割り当てます

The screenshot shows the 'Edit Security Zone' configuration window. The 'Security zone name' is set to 'Trust'. The 'Layer 2 members' section is empty. The 'Layer 3 members' section has an 'Interface List' on the left and a 'Member List (1)' on the right. The 'Interface List' contains a scrollable list of interfaces from GE1/0/0 to GE1/0/11. The 'Member List (1)' contains the interface GE1/0/2. A red box highlights the 'Interface List' header with a circled '1'. A red box highlights the 'GE1/0/2' entry in the 'Member List' with a circled '2'. A red arrow points from the 'GE1/0/2' entry in the 'Member List' to the 'OK' button at the bottom, which is also circled with a '3'.

Security zone name: Trust * (1-31 chars)

Layer 2 members

Layer 3 members

Interface List

Member List (1)

GE1/0/0

GE1/0/3

GE1/0/4

GE1/0/5

GE1/0/6

GE1/0/7

GE1/0/8

GE1/0/9

GE1/0/10

GE1/0/11

GE1/0/2

OK Cancel

GE1/0/2をTrustゾーンに割り当ててIPアドレスを割り当てます

The screenshot displays the H3C Network Configuration interface. The 'Network' menu is selected in the top navigation bar. The left sidebar shows the 'Interface Configuration' menu, with 'Interfaces' highlighted. The main table lists network interfaces. The row for GE1/0/2 is highlighted, showing it is assigned to the 'Trust' security zone and has the IP address 116.1.1.1/255.255.255.0. The 'Edit' button for this interface is circled in red.

①

②

③

Interface	Security zone	Status	IP address	Speed(kbps)	Link mode	Duplex ...	Loopbac...	Protocol exceptions		Description	Edit
								Received	Originated		
<input type="checkbox"/> GE1/0/0		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/0 Interface	
<input type="checkbox"/> GE1/0/1	Untrust	Up	116.1.1.1/255.255.255.0	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/1 Interface	
<input type="checkbox"/> GE1/0/2	Trust	Up	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/2 Interface	
<input type="checkbox"/> GE1/0/3		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/3 Interface	
<input type="checkbox"/> GE1/0/4		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/4 Interface	
<input type="checkbox"/> GE1/0/5		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/5 Interface	
<input type="checkbox"/> GE1/0/6		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/6 Interface	
<input type="checkbox"/> GE1/0/7		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/7 Interface	
<input type="checkbox"/> GE1/0/8		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/8 Interface	
<input type="checkbox"/> GE1/0/9		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/9 Interface	
<input type="checkbox"/> GE1/0/10		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/10 Interface	
<input type="checkbox"/> GE1/0/11		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/11 Interface	
<input type="checkbox"/> GE1/0/12		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/12 Interface	
<input type="checkbox"/> GE1/0/13		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/13 Interface	
<input type="checkbox"/> GE1/0/14		Down	---	1000000	Layer 3...	Full du...	Disabled			GigabitEthernet1/0/14 Interface	

GE1/0/2をTrustゾーンに割り当ててIPアドレスを割り当てます

Modify Interface Settings

Name: GE1/0/2

Link status: Up Shut down

Description: GigabitEthernet1/0/2 Interface

Link mode: Layer 3 mode

Security zone: **1** Trust

Protocol exceptions

Received: Telnet Ping SSH HTTP HTTPS SNMP
 NETCONF over HTTP NETCONF over HTTPS NETCONF over SSH

Originated: Telnet Ping SSH HTTP HTTPS

Basic Configuration **2** IPv4 Address IPv6 Address Physical Interface Configuration

IP address: **3** Manual assignment DHCP PPPoE

IP address/mask length: 10.10.10.1 / 255.255.255.0

Gateway:

Assign secondary IP Delete secondary IP

<input type="checkbox"/>	Secondary IP address	Mask length	Edit
--------------------------	----------------------	-------------	------

4 Apply OK Cancel

UntrustゾーンからTrustゾーンへのパケットをセキュリティチェックに合格したら通過させます

The screenshot displays the H3C SecPath F100-C-A1 interface with the 'Create Security Policy' dialog box open. The dialog is configured as follows:

- Name:** to-intra
- Type:** IPv4 (selected)
- Source zone:** Untrust
- Destination zone:** Trust

Red boxes and numbers 1-4 highlight the following elements:

1. The IPv4 radio button in the Type section.
2. The Untrust dropdown menu in the Source zone section.
3. The Trust dropdown menu in the Destination zone section.
4. The OK button at the bottom of the dialog.

The background interface shows the 'Policies' tab selected, with a table of existing policies. The table has columns for 'rule name', 'Search', 'Advanced search', 'Validity state indicator', 'Table s...', 'Left coll...', 'Enable', 'View Se...', and 'Edit'. A single policy is listed with '1' in the 'Table s...' column, '1' in the 'Enable' column, and 'View' in the 'View Se...' column.

Page 1 of 1 | Entries per page 25 | Displaying 1 - 1 of 1

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

UntrustゾーンからTrustゾーンへのパケットをセキュリティチェックに合格したら通過させます 51

The screenshot displays the H3C SecPath F100-C-A1 management interface. The main window is titled 'Create Security Policy' and is divided into several sections: General Config, Source, Destination, Service, Apps and Users, and Operation. A 'Select Service' dialog box is open in the foreground, showing two lists: 'Available' and 'Selected (104)'. The 'Available' list is highlighted with a red box and a circled '1'. The 'Selected' list is also highlighted with a red box and a circled '2'. A red arrow points from the 'Available' list to the 'Selected' list. The 'OK' button in the dialog is highlighted with a red box and a circled '3'. The background interface shows various configuration options and a table of security policies.

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

UntrustゾーンからTrustゾーンへのパケットをセキュリティチェックに合格したら通過させます 52

The screenshot shows the 'Edit Security Policy' configuration window in the H3C SecPath F100-C-A1 interface. The window is divided into several sections:

- General Config**: Application, User, Time range, VRF.
- Source**: Application, User.
- Destination**: User.
- Service**: (Empty)
- Apps and Users**: A list of applications with 'Any' selected. This section is highlighted with a red box and a circled '1'.
- Operation**: Action (Permit selected, Deny unselected), IPS profile, Data filtering profile, File filtering profile, Anti-virus profile, URL filtering profile, APT defense profile. This section is highlighted with a red box and a circled '2'.
- Logging**: Policy hit counting, Session aging.

At the bottom of the window, the 'OK' button is highlighted with a red box and a circled '3'.

TrustゾーンからUntrustゾーンへのパケットをセキュリティチェックに合格したら通過させます 53

The screenshot shows the H3C SecPath F100-C-A1 web interface. The main menu includes Dashboard, Monitor, Policies, Objects, Network, and System. The left sidebar shows Security Policies, Attack Defense, Threat Intelligence, and other security features. The 'Create Security Policy' dialog box is open, showing the following configuration:

- Name:** to-internet
- Type:** IPv4 (selected)
- Source zone:** Trust
- Destination zone:** Untrust

Red circles and boxes highlight the following elements:

1. The 'Type' field, specifically the 'IPv4' radio button.
2. The 'Source zone' dropdown menu, which is set to 'Trust'.
3. The 'Destination zone' dropdown menu, which is set to 'Untrust'.
4. The 'OK' button at the bottom of the dialog.

At the bottom of the page, there is a footer: Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved.

TrustゾーンからUntrustゾーンへのパケットをセキュリティチェックに合格したら 54 ら通過させます

The screenshot displays the H3C SecPath F100-C-A1 web management interface. The main window is titled "Create Security Policy" and is currently on the "Destination" tab. A "Select Service" dialog box is open in the foreground, showing a list of services to be selected for the policy. The dialog has a search filter (1), a list of available services (2) with a red box around it, and a list of selected services (104). A red arrow points from the available services list to the selected services list. The "OK" button (3) is highlighted at the bottom of the dialog. The background shows the "Destination" configuration fields, including "Destination zone" set to "Untrust", "Address object group", and "Service" (partially visible).

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

TrustゾーンからUntrustゾーンへのパケットをセキュリティチェックに合格したら 55 ら通過させます

The screenshot shows the 'Edit Security Policy' configuration window in the H3C SecPath F100-C-A1 interface. The window is divided into several sections:

- General Config:** Includes fields for User, Time range, VRF, Destination, Service, and Action.
- Apps and Users:** Includes fields for IPS profile, Data filtering profile, File filtering profile, Anti-virus profile, URL filtering profile, and APT defense profile.
- Operation:** Includes radio buttons for Permit (selected) and Deny.
- Logging:** Includes checkboxes for Enable/Disable for Logging, Policy hit counting, Session aging, Persistent session aging, Policy status, and Redundancy analysis.

Three red boxes with numbers 1, 2, and 3 highlight specific settings:

- 1:** Source configuration: Any, Any, Public network.
- 2:** Operation configuration: Permit (selected).
- 3:** OK button.

The interface also shows a sidebar with 'Security Policies' and 'Attack Defense' sections, and a main area with a table of security policies. The footer contains the copyright information: Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved.

完成したコンフィグの一部

```
#
version 7.1.064, Alpha 7164
#
sysname F1060
#
clock timezone Tokyo add 09:00:00
#.....
vlan 1
#
interface NULL0
#
interface GigabitEthernet1/0/0
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/1
port link-mode route
combo enable copper
ip address 192.168.56.254 255.255.255.0
session log enable ipv4 inbound
session log enable ipv4 outbound
#
interface GigabitEthernet1/0/2
port link-mode route
combo enable copper
ip address 10.10.10.1 255.255.255.0
session log enable ipv4 inbound
session log enable ipv4 outbound
#
interface GigabitEthernet1/0/3
port link-mode route
combo enable copper
ip address 192.168.1.1 255.255.255.0
session log enable ipv4 inbound
session log enable ipv4 outbound
#.....
```

```
#.....
security-zone name Local
attack-defense apply policy Attack_defence2
#
security-zone name Trust
import interface GigabitEthernet1/0/2
import interface GigabitEthernet1/0/3
attack-defense apply policy Attack_defence2
#
security-zone name DMZ
#
security-zone name Untrust
attack-defense apply policy Attack_defence2
#
security-zone name Management
import interface GigabitEthernet1/0/1
attack-defense apply policy Attack_defence2
#.....
customlog format security-policy sgcc
customlog format keepalive sgcc
customlog format dpi reputation
#.....
userlog flow export host 192.168.1.2 port 9002
userlog flow export host 192.168.137.1 port
9002
#
ntp-service enable
#.....
```

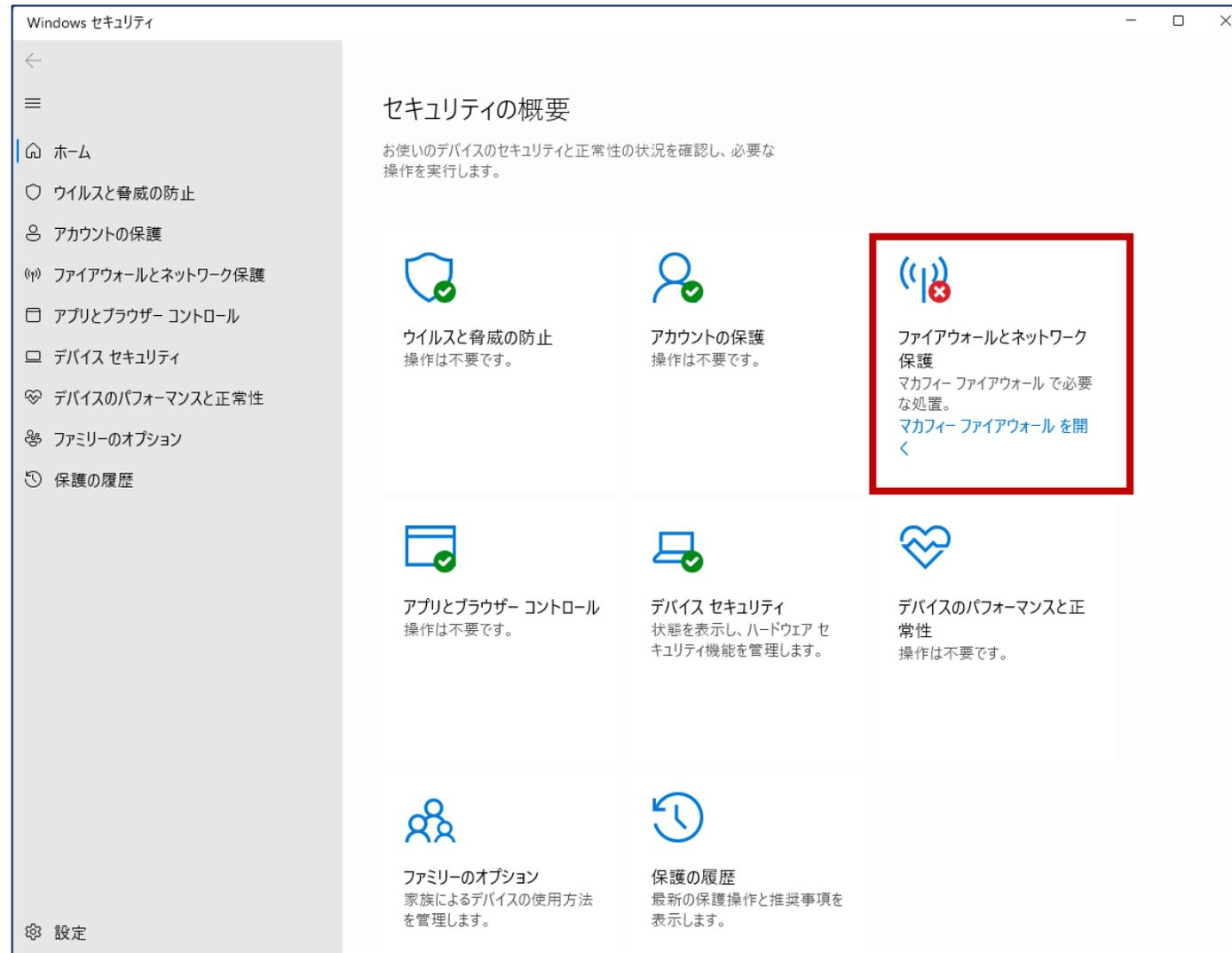
```
#
blacklist global enable
#.....
attack-defense policy Attack_defence2
scan detect level high action drop logging
syn-flood detect non-specific
syn-flood action logging
rst-flood detect non-specific
rst-flood action logging
#.....
signature detect large-icmp action drop logging
signature detect large-icmpv6 action drop logging
signature detect tcp-invalid-flags action drop
logging
signature detect tcp-null-flag action drop logging
http-slow-attack action logging
#
app-profile 0_IPv4
ips apply policy default mode protect
data-filter apply policy default
url-filter apply policy default
file-filter apply policy default
anti-virus apply policy default mode protect
waf apply policy default mode protect
apt apply policy default
#....
inspect redirect parameter-profile
waf_redirect_default_parameter
#
inspect email parameter-profile
mailsetting_default_parameter
undo authentication enable
```

```
#
security-policy ip
rule 0 name attack_defence
action pass
logging enable
profile 0_IPv4
#
ips logging parameter-profile
ips_logging_default_parameter
#
anti-virus logging parameter-profile
av_logging_default_parameter
#
return
```

テストする際にWindowsファイアウォールを無効にする



テストする際にWindowsファイアウォールを無効にする



SecPathからhostへの疎通OK

```
secpath_attack
NGFW x GW x
n/avg/max/std-dev = 0.000/0.000/0.000/0.000 ms.
<H3C>ping 116.1.1.2
Ping 116.1.1.2 (116.1.1.2): 56 data bytes, press CTRL+C to break
56 bytes from 116.1.1.2: icmp_seq=0 ttl=128 time=1.000 ms
56 bytes from 116.1.1.2: icmp_seq=1 ttl=128 time=1.000 ms
56 bytes from 116.1.1.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 116.1.1.2: icmp_seq=3 ttl=128 time=0.000 ms
56 bytes from 116.1.1.2: icmp_seq=4 ttl=128 time=0.000 ms
--- Ping statistics for 116.1.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
<H3C>%Jul 23 06:47:07:927 2022 H3C PING/6/PING_STATISTICS: -
Context=1; Ping statistics for 116.1.1.2: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip mi
```

業務サーバーからhostへの疎通OK

```
secpath_attack
NGFW x GW x
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
<H3C>%Jul 23 06:55:16:435 2022 H3C PING/6/PING_STATISTICS: Ping statistics for 116.1.1.2: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms.

<H3C>ping 116.1.1.2
Ping 116.1.1.2 (116.1.1.2): 56 data bytes, press CTRL+C to break
56 bytes from 116.1.1.2: icmp_seq=0 ttl=127 time=1.000 ms
56 bytes from 116.1.1.2: icmp_seq=1 ttl=127 time=1.000 ms
56 bytes from 116.1.1.2: icmp_seq=2 ttl=127 time=1.000 ms
56 bytes from 116.1.1.2: icmp_seq=3 ttl=127 time=2.000 ms
56 bytes from 116.1.1.2: icmp_seq=4 ttl=127 time=1.000 ms

--- Ping statistics for 116.1.1.2 ---
```



00 装置のGUIへアクセスする

01 装置ファイル(.did)のダウンロード

02 ライセンスリニューアル

03 ライセンスのインストール

04 シグネチャーの更新

05 各種ログの環境整備

06 攻撃検証環境の整備

07 検証結果

08 トラブルシュート

Application Usage ログ

② Application Analysis Center

① Monitor

Application Analysis Center

Context: All Refresh Time range: Past hour 2022-07-23 07:09:18 - 2022-07-23 08:09:17 Select module

Global filters: +Filters

Application Usage

Bytes Sessions Threats URLs Files WAF

User Activity

KB

Upstream traffic Downstream traffic

Application	Ris	Bytes	Sessions	Threats	URLs	Files	Attack co...
https_other	4	187.33KB	1	0	0	0	0
syslog	2	22.92KB	5	0	0	0	0
https	1	15.98KB	11	0	0	0	0

Username	Bytes	Sessions	Threats	URLs	Files	Attack cou...
116.1.1.2	203.31KB	12	0	0	0	0
116.1.1.1	22.92KB	5	0	0	0	0

https://116.1.1.1/wnm/frame/index.php#M_CDAS Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

User Activityログ

② Application Analysis Center

① Monitor

Application Analysis Center

Context: All Refresh Time range: Past hour 2022-07-23 06:58:41 - 2022-07-23 07:58:40 Select module

Global filters: +Filters

Application Usage

Bytes Sessions Threats URLs Files WAF

Other_Service

ICMP

Application	Ris...	Bytes	Sessions	Threats	URLs	Files	Attack co...
ICMP	1	1.64KB	2	0	0	0	0

User Activity

Bytes Sessions Threats URLs Files WAF

KB

2

1.5

1

0.5

0

06:58 07:03 07:08 07:13 07:18 07:23 07:28 07:33 07:38 07:43 07:48 07:53 07:58

Upstream traffic Downstream traffic

Username	Bytes	Sessions	Threats	URLs	Files	Attack cou...
10.10.10.2	1.64KB	2	0	0	0	0

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

Single-Packet Attack攻撃ログ

Dashboard Monitor Policies Objects Network System

admin vSystem: Admin

Application Analysis

- Security Logs
 - Blacklist Logs
 - Single-Packet Attack Logs
 - Scanning Attack Logs
 - Flood Attack Logs
 - Threat Logs
 - Reputation Logs
 - URL Filtering Logs
 - File Filtering Logs
 - Security Policy Logs
 - Sandbox Logs
 - Terminal Logs
- Application Audit Logs
- Device Logs
 - System Logs
 - Operation Logs
 - Traffic Logs
- Statistics
 - TopN Traffic
 - Users
 - Apps
 - Source IPs
 - Destination IPs

Refresh Clear all filters Import Export Clear Search results: 2022-10-12 00:00:00-13:39:59 9 matching logs. Advanced search

Time	Severity level	Type	Action	VPN name	Source security zon...	Destination IP address	Source IP address
2022-10-12 13:37:23	error	Impossible	logging,drop		Local	127.0.0.1	127.0.0.1
2022-10-12 13:32:23	error	Impossible	logging,drop		Local	127.0.0.1	127.0.0.1
2022-10-12 13:27:23	error	Impossible	logging,drop		Local	127.0.0.1	127.0.0.1
2022-10-12 13:22:23	error	Impossible	logging,drop		Local	127.0.0.1	127.0.0.1
2022-10-12 13:17:23	error	Impossible	logging,drop		Local	127.0.0.1	127.0.0.1
2022-10-12 13:12:23	error	Impossible	logging,drop		Local	127.0.0.1	127.0.0.1
2022-10-12 13:07:23	error	Impossible	logging,drop		Local	127.0.0.1	127.0.0.1
2022-10-12 13:02:23	error	Impossible	logging,drop		Local	127.0.0.1	127.0.0.1
2022-10-12 12:57:23	error	Impossible	logging,drop		Local	127.0.0.1	127.0.0.1

Page 1 of 1 Entries per page 25

Displaying 1 - 9 of 9

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

Scanning Attack攻撃ログ

Application Analysis C

Security Logs

- Blacklist Logs
- Single-Packet Attack Log
- Scanning Attack Logs**
- Flood Attack Logs
- Threat Logs
- Reputation Logs
- URL Filtering Logs
- File Filtering Logs
- Security Policy Logs
- Sandbox Logs
- Terminal Logs

Application Audit Log

Device Logs

Statistics

Trends

Botnet Analysis

Asset Security

Threat Case Manager

Reports

Sessions

LB Session Information

User Info Center

DNS Cache

Terminal Info

Dashboard Monitor Policies Objects Network System

admin vSystem: Admin

Refresh Clear all filters Import Export Clear Search results: 2023-04-27 00:00:00-15:15:09 7 matching logs. Advanced search

Time	Severity level	Type	Action	VPN name	Destination IP address	Attack start time
2023-04-27 13:32:38	error	Port scan	logging,drop		192.168.56.254	2023-04-27 13:32:38
2023-04-27 13:32:16	error	Port scan	logging,drop		192.168.56.254	2023-04-27 13:32:16
2023-04-27 13:31:55	error	Port scan	logging,drop		192.168.56.254	2023-04-27 13:31:55
2023-04-27 13:31:44	error	Port scan	logging,drop		192.168.56.254	2023-04-27 13:31:44
2023-04-27 13:25:23	error	Port scan	logging,drop		192.168.56.254	2023-04-27 13:25:23
2023-04-27 13:24:52	error	Port scan	logging,drop		192.168.56.254	2023-04-27 13:24:52
2023-04-27 13:24:41	error	Port scan	logging,drop		192.168.56.254	2023-04-27 13:24:41

Page 1 of 1 Entries per page 25

Displaying 1 - 7 of 7

Copyright © 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved.

IPS攻撃ログ

The screenshot displays the H3C Monitor interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Policies', 'Objects', 'Network', and 'System'. The 'Monitor' menu item is circled in red and labeled with a '1'. On the left sidebar, 'Threat Logs' is highlighted with a red box and labeled with a '2'. The main content area shows a table of logs with the following data:

Details	Time	Threat type	Threat ID	Threat name	Severity...	Source secu...	Destination...	Source IP add...	Destination l...	Application	Protocol	File name	Content sec...	Ad
<input type="checkbox"/>	2022-10-16 21:27:34	IPS	45651	CVE-2021-44228_A...	Critical	Local	Trust	192.168.1.1	192.168.1.2	syslog	UDP		default	

At the bottom of the interface, it shows 'Page 1 of 1' and 'Entries per page 25'. The footer contains the copyright notice: 'Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved'.

Security policy攻撃ログ

Dashboard Monitor Policies Objects Network System

Please click this icon to save the changes

admin vSystem: Admin

Refresh Import Export Clear Search results: 2022-07-23 00:00:00-08:02:57 100 matching logs. Advanced search

Time	Source s...	Destinati...	Security policy	Rule ID	Protocol	Application	Source IP address	Source p...	Destination IP address	Destinati...	Number of rule...	Action
2022-07-23 08:00:58	Trust	Local	permitall	0	IGMP		116.1.1.2	0	239.255.255.250	0	1	Permit
2022-07-23 08:00:45	Trust	Local	permitall	0	TCP	https_other	116.1.1.2	16564	116.1.1.1	443	1213	Permit
2022-07-23 08:00:45	Trust	Local	permitall	0	TCP	https_other	116.1.1.2	16565	116.1.1.1	443	598	Permit
2022-07-23 08:00:45	Trust	Local	permitall	0	TCP	https_other	116.1.1.2	16563	116.1.1.1	443	266	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	UDP	general_udp	116.1.1.2	64877	116.1.1.255	22936	3	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https	116.1.1.2	16565	116.1.1.1	443	4	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https	116.1.1.2	16564	116.1.1.1	443	5	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https	116.1.1.2	16563	116.1.1.1	443	5	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https_other	116.1.1.2	16559	116.1.1.1	443	1157	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https	116.1.1.2	16562	116.1.1.1	443	5	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https	116.1.1.2	16561	116.1.1.1	443	5	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https	116.1.1.2	16560	116.1.1.1	443	5	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https_other	116.1.1.2	16558	116.1.1.1	443	89	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https	116.1.1.2	16559	116.1.1.1	443	5	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https	116.1.1.2	16558	116.1.1.1	443	4	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https	116.1.1.2	16557	116.1.1.1	443	5	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https	116.1.1.2	16556	116.1.1.1	443	5	Permit
2022-07-23 08:00:44	Trust	Local	permitall	0	TCP	https	116.1.1.2	16555	116.1.1.1	443	5	Permit

Page 1 of 4 Entries per page 25

Displaying 1 - 25 of 100

https://116.1.1.1/wnm/frame/index.php#M_ZonePairLog

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

Traffic ログ

Refresh Import Export Clear Clear all filters Log aggregation settings Search results: 2022-07-23 00:00:00-14:23:35 11 matching logs. Advanced search

To display log data, first enable [session statistics collection](#) and [log collection](#) of the traffic service.

Details	Time	Source security z...	Destination secur...	Source address	Destination addr...	Application	Protocol	Total traffic	Ingress interface	Egress interface
	2022-07-23 13:31:28	Trust	Local	116.1.1.2	116.1.1.1	https_other	TCP	123.61KB	GigabitEthernet1/0/1	InLoopBack0
	2022-07-23 13:31:27	Trust	Local	116.1.1.2	116.1.1.1	https	TCP	1.14KB	GigabitEthernet1/0/1	InLoopBack0
	2022-07-23 13:31:27	Trust	Local	116.1.1.2	116.1.1.1	https	TCP	1.14KB	GigabitEthernet1/0/1	InLoopBack0
	2022-07-23 13:31:27	Trust	Local	116.1.1.2	116.1.1.1	https	TCP	1.14KB	GigabitEthernet1/0/1	InLoopBack0
	2022-07-23 13:31:27	Trust	Local	116.1.1.2	116.1.1.1	https	TCP	1.14KB	GigabitEthernet1/0/1	InLoopBack0
	2022-07-23 13:31:27	Trust	Local	116.1.1.2	116.1.1.1	https	TCP	1.14KB	GigabitEthernet1/0/1	InLoopBack0
	2022-07-23 13:31:26	Trust	Local	116.1.1.2	116.1.1.1	https	TCP	1.80KB	GigabitEthernet1/0/1	InLoopBack0
	2022-07-23 13:31:26	Trust	Local	116.1.1.2	116.1.1.1	https	TCP	1.80KB	GigabitEthernet1/0/1	InLoopBack0
	2022-07-23 13:31:26	Trust	Local	116.1.1.2	116.1.1.1	https	TCP	3.31KB	GigabitEthernet1/0/1	InLoopBack0
	2022-07-23 13:31:26	Trust	Local	116.1.1.2	116.1.1.1	https	TCP	1.14KB	GigabitEthernet1/0/1	InLoopBack0
	2022-07-23 13:31:26	Trust	Local	116.1.1.2	116.1.1.1	https	TCP	1.14KB	GigabitEthernet1/0/1	InLoopBack0

Page 1 of 1 Entries per page 25

Displaying 1 - 11 of 11

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

Destination IP ログ

The screenshot displays the H3C Monitor interface. The 'Monitor' menu item is highlighted with a red box and a circled '1'. In the left sidebar, the 'Destination IPs' menu item is highlighted with a red box and a circled '2'. The main content area shows a donut chart and a table of traffic statistics for three destination IP addresses.

Time used: 0.5 seconds
Time range: 2022-10-12 00:00:00 - 2022-10-12 23:59:59
Traffic direction: Bidirectional
Application: All
Application category: All
Show: Top 10
Bar chart: Show top 10
Pie chart: Show top 10

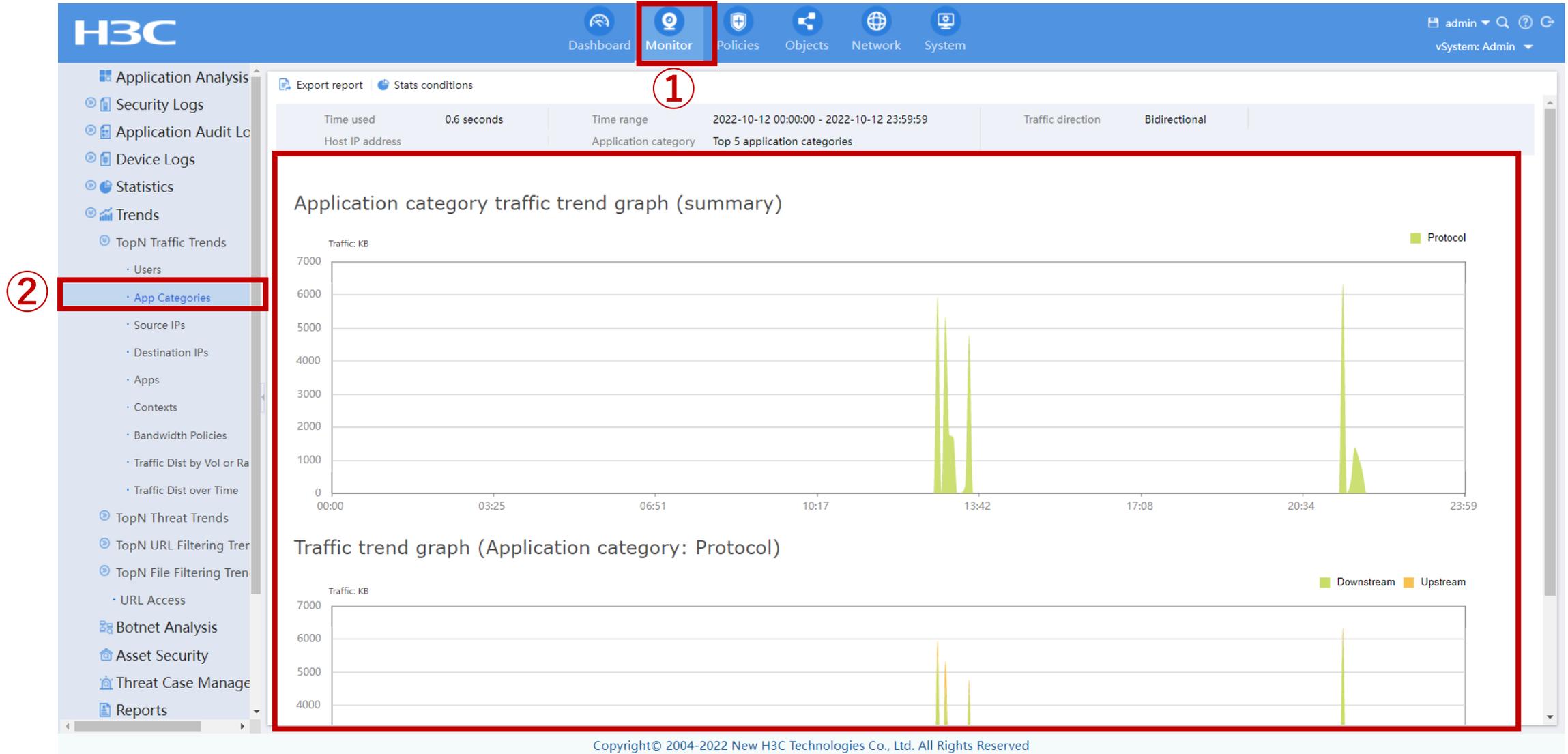
Bar Chart | Pie Chart

Rank	Destination address	Upstream	Downstream	Bidirectional	Traffic percentage	Session	Session percentage
1	192.168.56.254	3.42MB	25.46MB	28.89MB	99.921%	310	89.595%
2	192.168.1.2	22.89KB	0.00B	22.89KB	0.077%	35	10.116%
3	192.168.56.1	396.00B	0.00B	396.00B	0.001%	1	0.289%

Legend:
192.168.56.254
192.168.1.2
192.168.56.1

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

攻撃Application category ログ

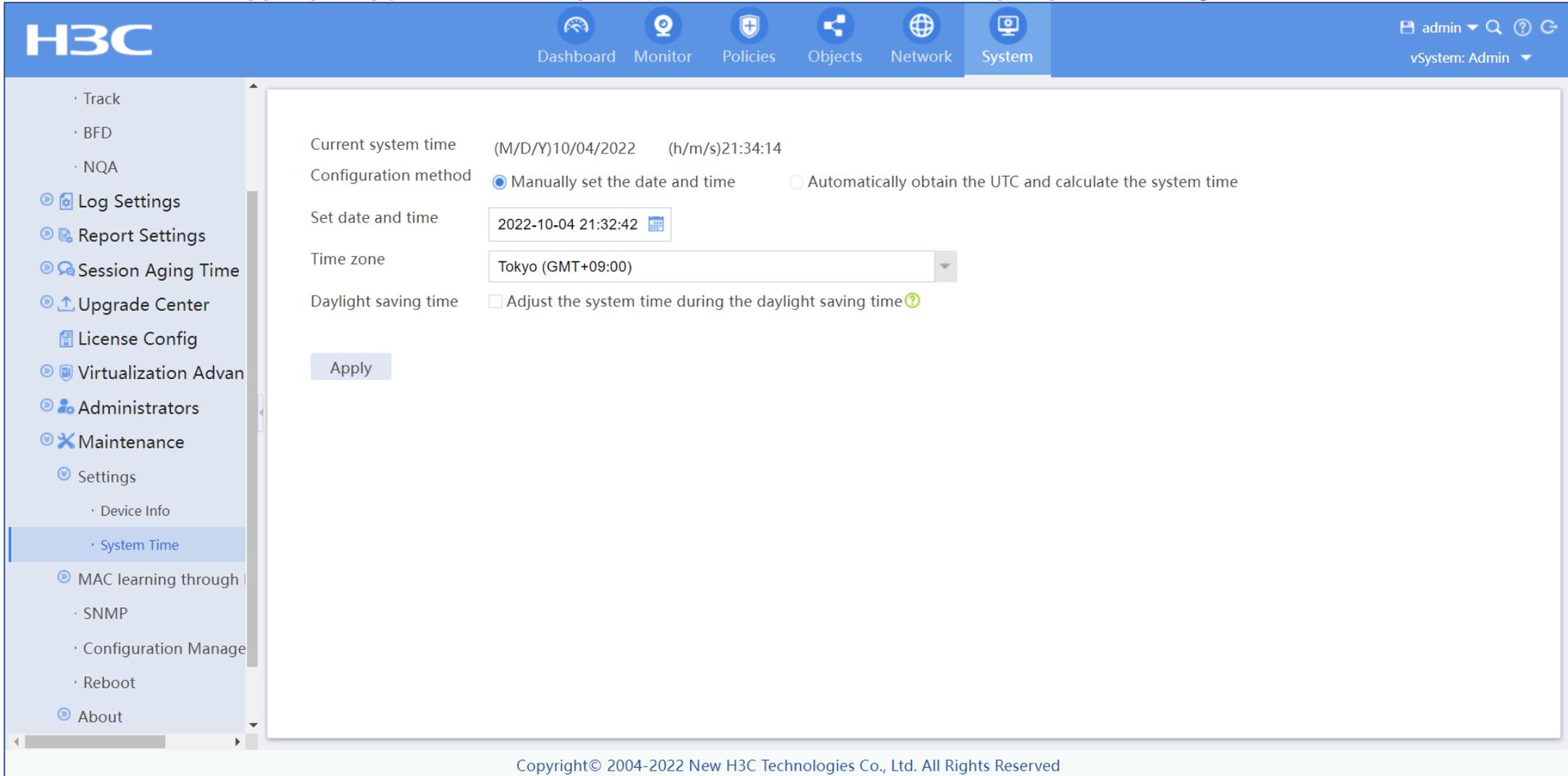


Sessions ログ

Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

注意事項：System time

System timeが正しく設定されていないとMonitorに何も表示されません。表示期間と発生したログの時間帯が合わないため何も表示するものがないと判断されます。



The screenshot displays the H3C System Time configuration interface. The top navigation bar includes Dashboard, Monitor, Policies, Objects, Network, and System. The left sidebar lists various system settings, with System Time selected. The main content area shows the following configuration details:

- Current system time: (M/D/Y)10/04/2022 (h/m/s)21:34:14
- Configuration method: Manually set the date and time, Automatically obtain the UTC and calculate the system time
- Set date and time: 2022-10-04 21:32:42
- Time zone: Tokyo (GMT+09:00)
- Daylight saving time: Adjust the system time during the daylight saving time

An 'Apply' button is located at the bottom of the configuration area.

Copyright © 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

注意事項：System time

System timeが正しく設定されていないとMonitorに何も表示されません。表示期間と発生したログの時間帯が合わないため何も表示するものがないと判断されます。

Application Analysis Center

Context All Refresh Time range Past hour 2022-10-05 14:41:48 - 2022-10-05 15:41:47

Global filters: +Filters

Application Usage

Bytes Sessions Threats URLs Files WAF

Other_Service

User Act

Bytes

MB

28.6

PCの時間から表示するログの時間を割り出す

PCの時間

15:41
2022/10/05

ntpから時間を得ていないとNGFWの内部時間とブラウザの時間が異なります

Current system time (M/D/Y)10/05/2022 (h/m/s)09:10:28

Configuration method Manually set the date and time Automatically obtain

Set date and time 2022-10-05 09:10:23

Time zone Tokyo (GMT+09:00)

Daylight saving time Adjust the system time during the daylight saving time

注意事項：Signatureは常に最新に保つ

ウイルスの特徴を保存している最新のsignatureは毎日更新されます。新しいものが見つからなければ、内容は前日と同じ場合もありますが、自動的にサーバーにアクセスする設定にしてください。

The screenshot shows the H3C management interface with the 'Signature Upgrade' section selected in the left navigation menu. The main content area displays a table of signature libraries with the following data:

Signature library	Current version	Release date	Auto update	Scheduled update...	Actions
IPS signature library	1.0.212	2022-09-19	<input type="checkbox"/>	-	Online update Manual update
Anti-virus signature library	1.0.0	2018-12-28	<input type="checkbox"/>	-	Online update Manual update
APR signature library	1.0.0	2022-03-22	<input type="checkbox"/>	-	Online update Manual update
URL filtering signature library	1.0.69	2022-09-08	<input type="checkbox"/>	-	Online update Manual update
URL reputation signature library	-	-	<input type="checkbox"/>	-	Online update Manual update
Domain reputation signature library	-	-	<input type="checkbox"/>	-	Online update Manual update
IP reputation signature library	-	-	<input type="checkbox"/>	-	Online update Manual update
WAF signature library	1.0.18	2022-06-24	<input type="checkbox"/>	-	Online update Manual update

At the bottom of the page, there is a footer: Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved.



00 装置のGUIへアクセスする

01 装置ファイル(.did)のダウンロード

02 ライセンスリニューアル

03 ライセンスのインストール

04 シグネチャーの更新

05 各種ログの環境整備

06 攻撃検証環境の整備

07 検証結果

08 **トラブルシュート**

診断ログの採取

障害の原因が解明できない場合、H3Cのテクニカルサポートへ**診断ログ**や装置の**シリアル番号**など必要な情報を明記してメールにて送信してください。

① Systemメニューをクリック

② Diagnostic Centerをクリック

③ Diagnostic Infoをクリック

④ Collectをクリック

Enter File Name

File name OK

Info

Finished collecting diagnostic information.
diag_20221206-142906.tar.gz
 Download diagnostic information file
OK

- ⑤保存される診断情報のファイル名が表示され、これで良ければOKをクリック
- ⑥情報が取得されたのでDownload…をチェックしてOKをクリックするとファイルがダウンロードされます。

コンフィグファイルの採取

コンフィグファイルは本体に保存されているコンフィグが壊れてしまった場合のバックアップとしてコンフィグファイルとして保存しておきましょう。

The screenshot displays the H3C web management interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Policies', 'Objects', 'Network', and 'System'. The 'System' menu is highlighted with a red box and a circled '1'. The left sidebar contains various settings, with 'Maintenance' (2) and 'Configuration Manager' (3) highlighted with red boxes. The main content area shows a configuration list with columns for line numbers and configuration commands. The 'Export running configuration' button is highlighted with a red box and a circled '4'. A 'Please Wait' dialog box is overlaid on the configuration list, indicating the export process. The dialog box contains a loading spinner and the text 'Exporting the running configuration...'. At the bottom left, the 'startup.cfg' file is visible, highlighted with a red box and a circled '5'.

Line	Configuration
1	#
2	version 7.1.064, Alpha 7164
3	#
4	sysname F1060
5	#
6	clock timezone Toky
7	clock protocol none
8	#
9	context Admin id 1
10	#
11	telnet server enable
12	#
13	irf mac-address persistent timer
14	irf auto-update enable
15	undo irf link-delay

テクニカルサポートへ解析依頼

ダウンロードされたファイルを以下のように障害の内容を記載して以下のテクニカルサポート宛に送付ください。

【送付先】

TO: h3cts@h3c.com

CC: &TS-INTL-JPN@h3c.com

【H3C カスタマーサービスE-mail テンプレート】

会社名 & 担当者名:

プロジェクト名 (オプション): *office Network Reconstruction
Project**

問題説明: S5130S Switch interface fails to go up

**※オペレーションログ: Record the process of the operation, or
the process log of the failure.**

※Diag診断ログ: diagnostic information in failure time

※ログファイル: log information in failure time

※ネットワークトポロジー: ***

※製品モデル: S5130S-28P-EI

※シリアル番号: 219801A1N59186Q0XXXX

※ソフトウェアバージョン: Version 7.1.064, Release 5223

※緊急性:

H3C

www.h3c.com