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

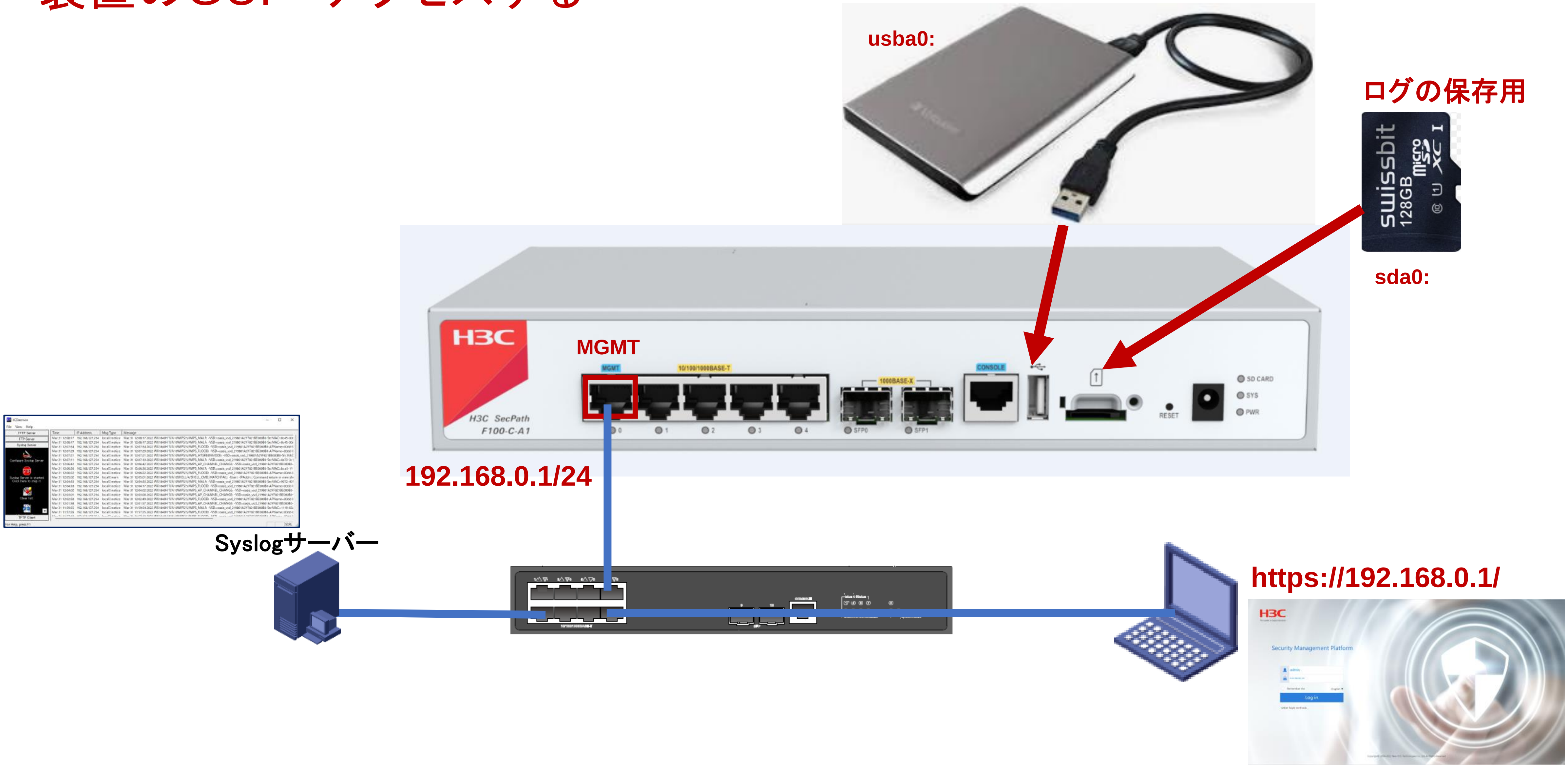
05 各種ログの環境整備

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

usba0:

ログの保存用

sda0:

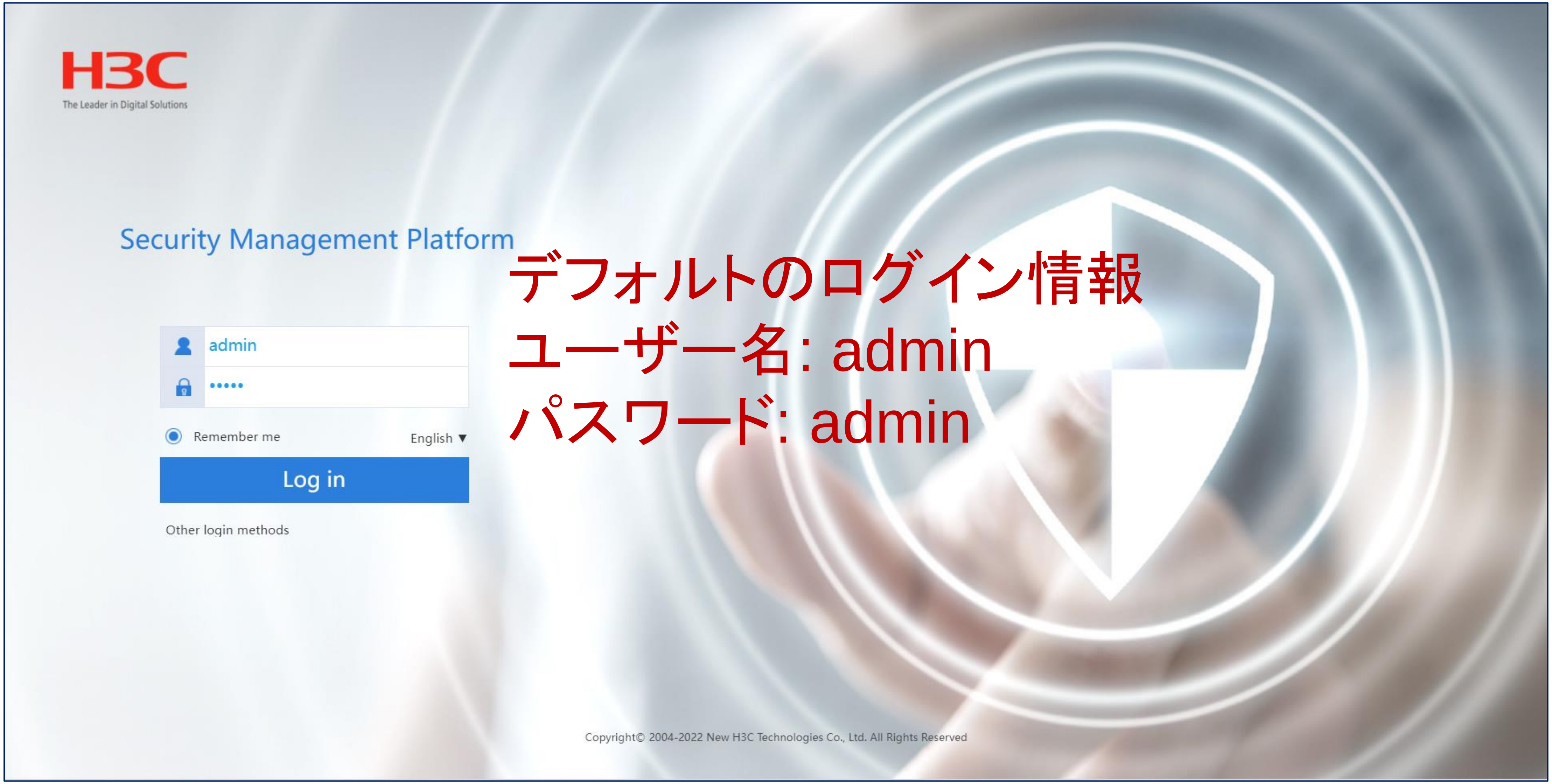
MGMT

192.168.0.1/24

Syslogサーバー

https://192.168.0.1/

https://192.168.0.1/



Security Management Platform

admin

•••••

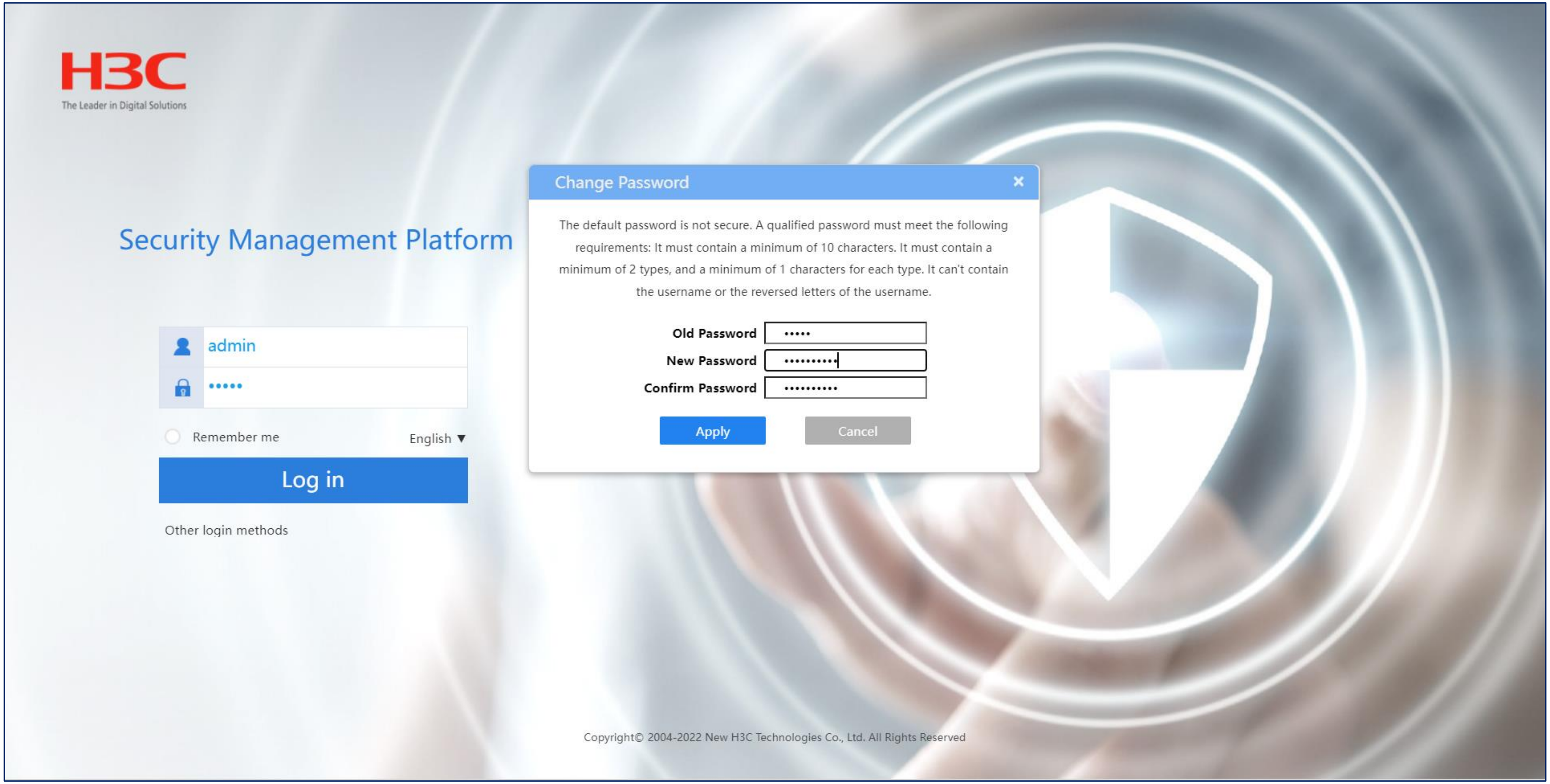
● Remember me

English ▼

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

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

初期パスワードを変更します



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.

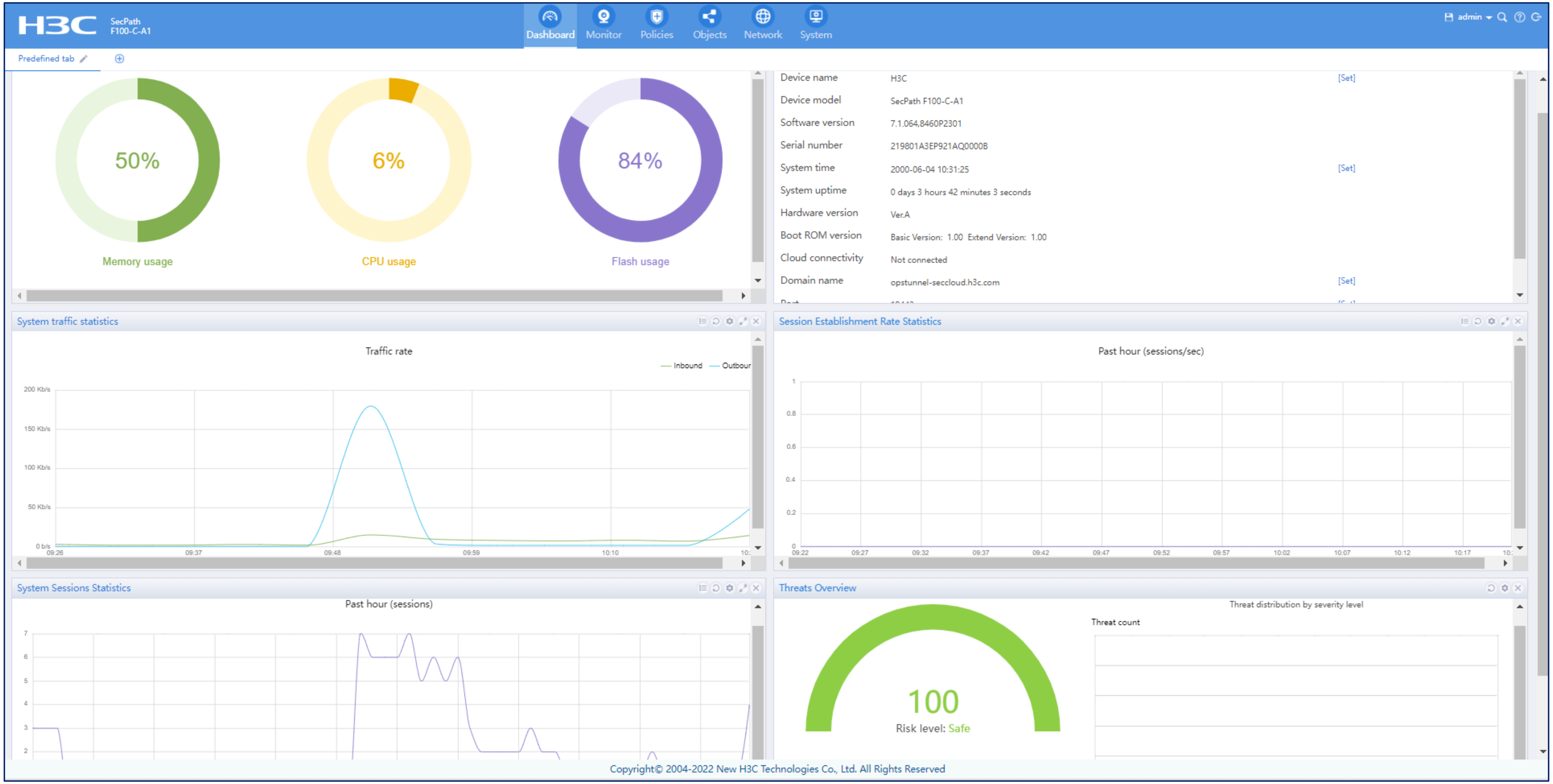
Old Password •••••

New Password ••••••••••

Confirm Password ••••••••••

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



Device name	H3C	[Set]
Device model	SecPath F100-C-A1	
Software version	7.1.064,8460P2301	
Serial number	219801A3EP921AQ0000B	
System time	2000-06-04 10:31:25	[Set]
System uptime	0 days 3 hours 42 minutes 3 seconds	
Hardware version	Ver.A	
Boot ROM version	Basic Version: 1.00 Extend Version: 1.00	
Cloud connectivity	Not connected	
Domain name	opstunnel-seccloud.h3c.com	[Set]

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

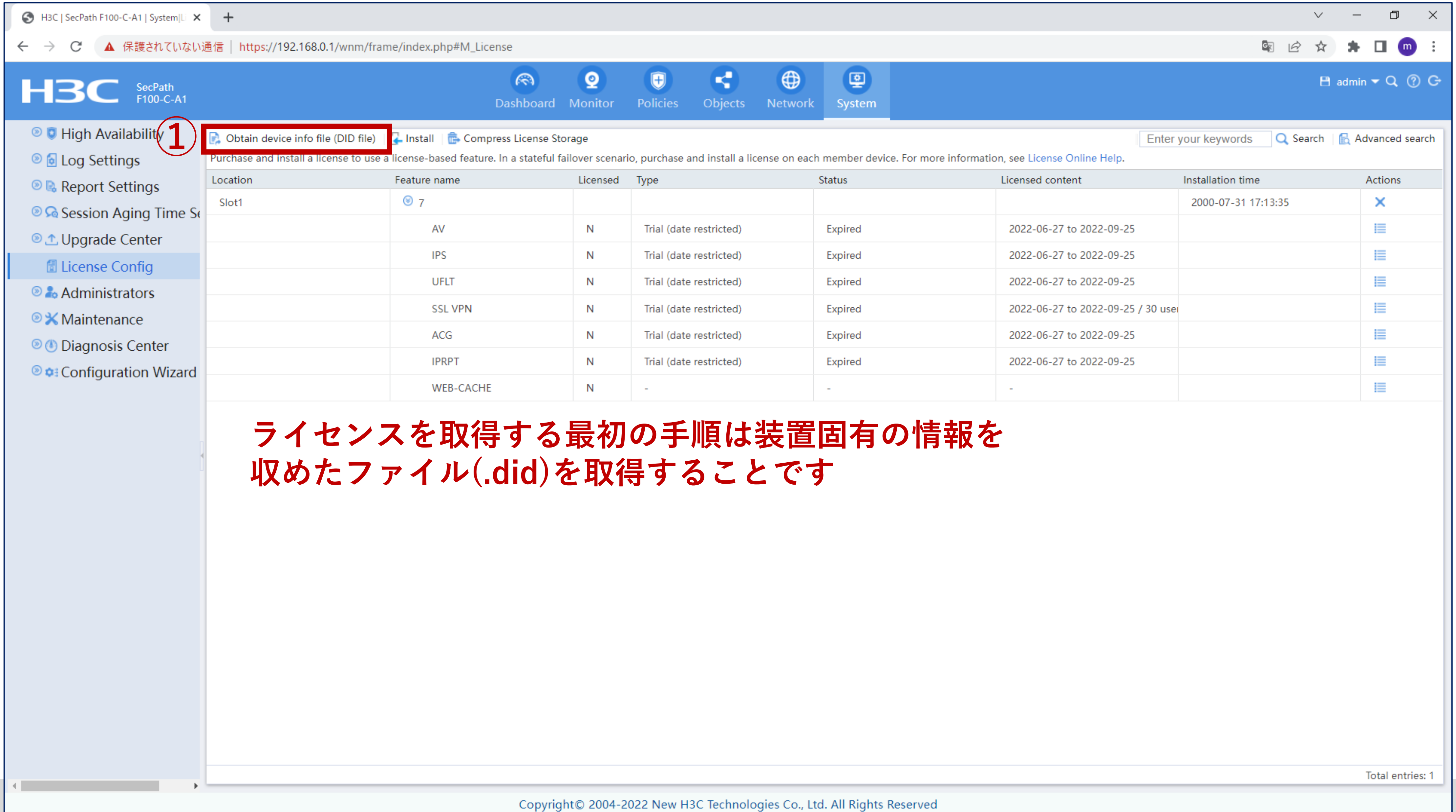
05 各種ログの環境整備

06 攻撃検証環境の整備

07 検証結果

08 トラブルシュート

ライセンスのインストラーを取得するために装置固有の情報を取得する



Purchase and install a license to use a license-based feature. In a stateful failover scenario, purchase and install a license on each member device. For more information, see License Online Help.

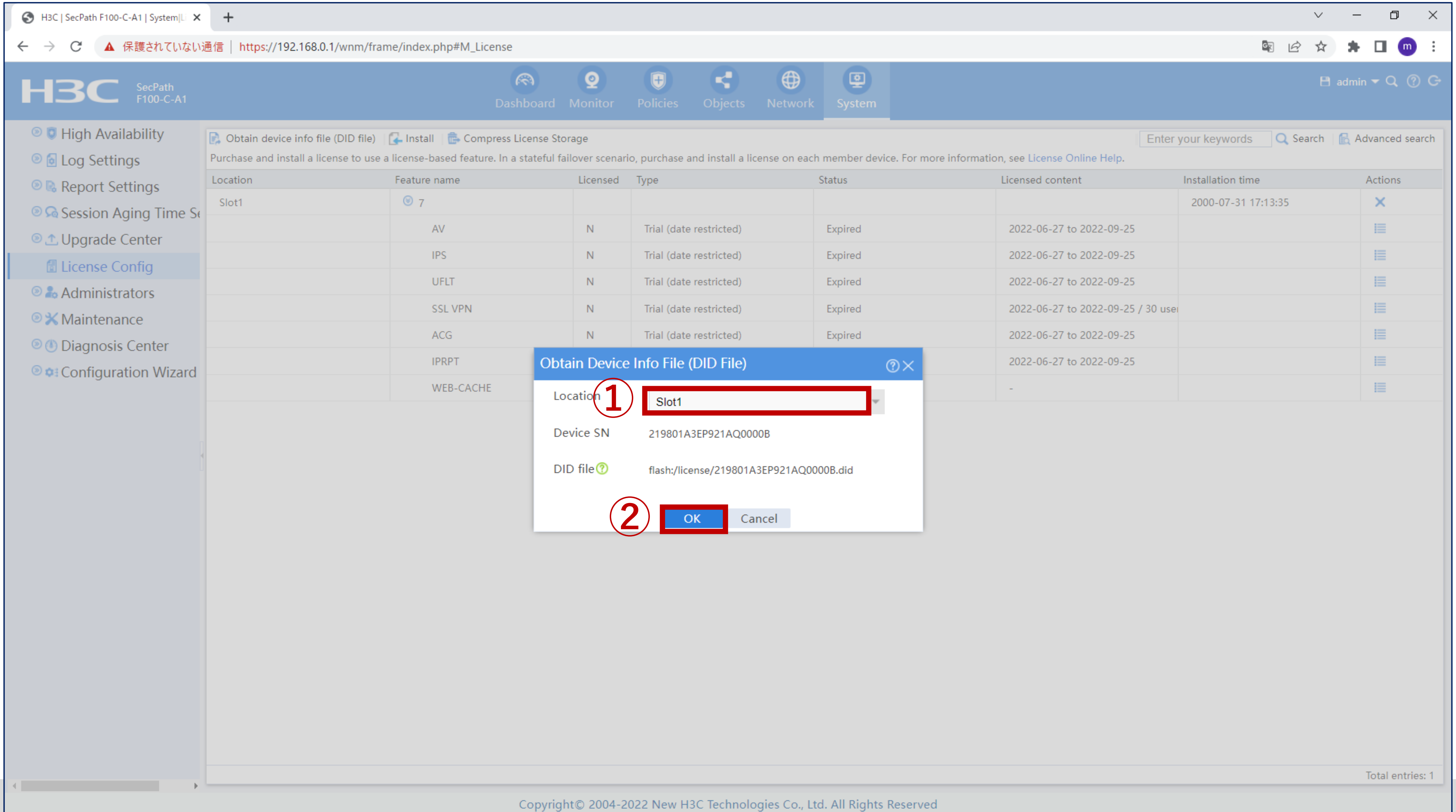
Location	Feature name	Licensed	Type	Status	Licensed content	Installation time	Actions
Slot1	7					2000-07-31 17:13:35	✕
	AV	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25		☰
	IPS	N	Trial (date restricted)	Expired	2022-06-27 to 2022-09-25		☰
	UFLT	N	Trial (date restricted)	Expired	2022-06-27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

Total entries: 1

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

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



Purchase and install a license to use a license-based feature. In a stateful failover scenario, purchase and install a license on each member device. For more information, see License Online Help.

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				2022-06-27 to 2022-09-25		☰
	WEB-CACHE				-		☰

Total entries: 1

Obtain Device Info File (DID File)

Location ① Slot1

Device SN 219801A3EP921AQ0000B

DID file flash:/license/219801A3EP921AQ0000B.did

② OK Cancel

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

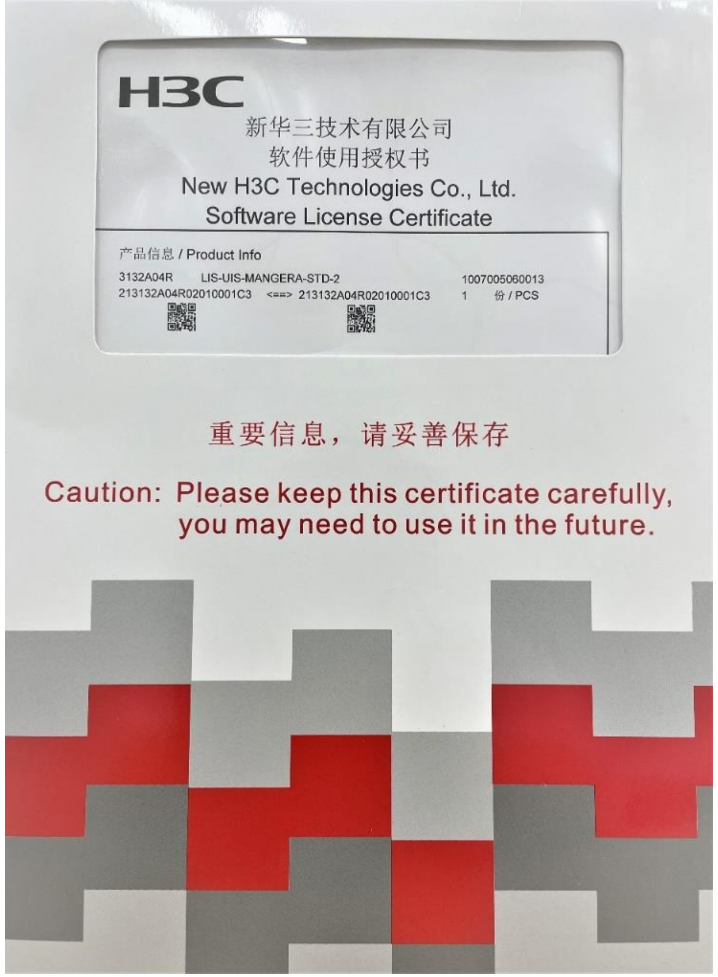
05 各種ログの環境整備

06 攻撃検証環境の整備

07 検証結果

08 トラブルシュート

事前にライセンスを購入しておきます。



H3C

新华三技术有限公司
软件使用授权书
New H3C Technologies Co., Ltd.
Software License Certificate

产品信息 / Product Info

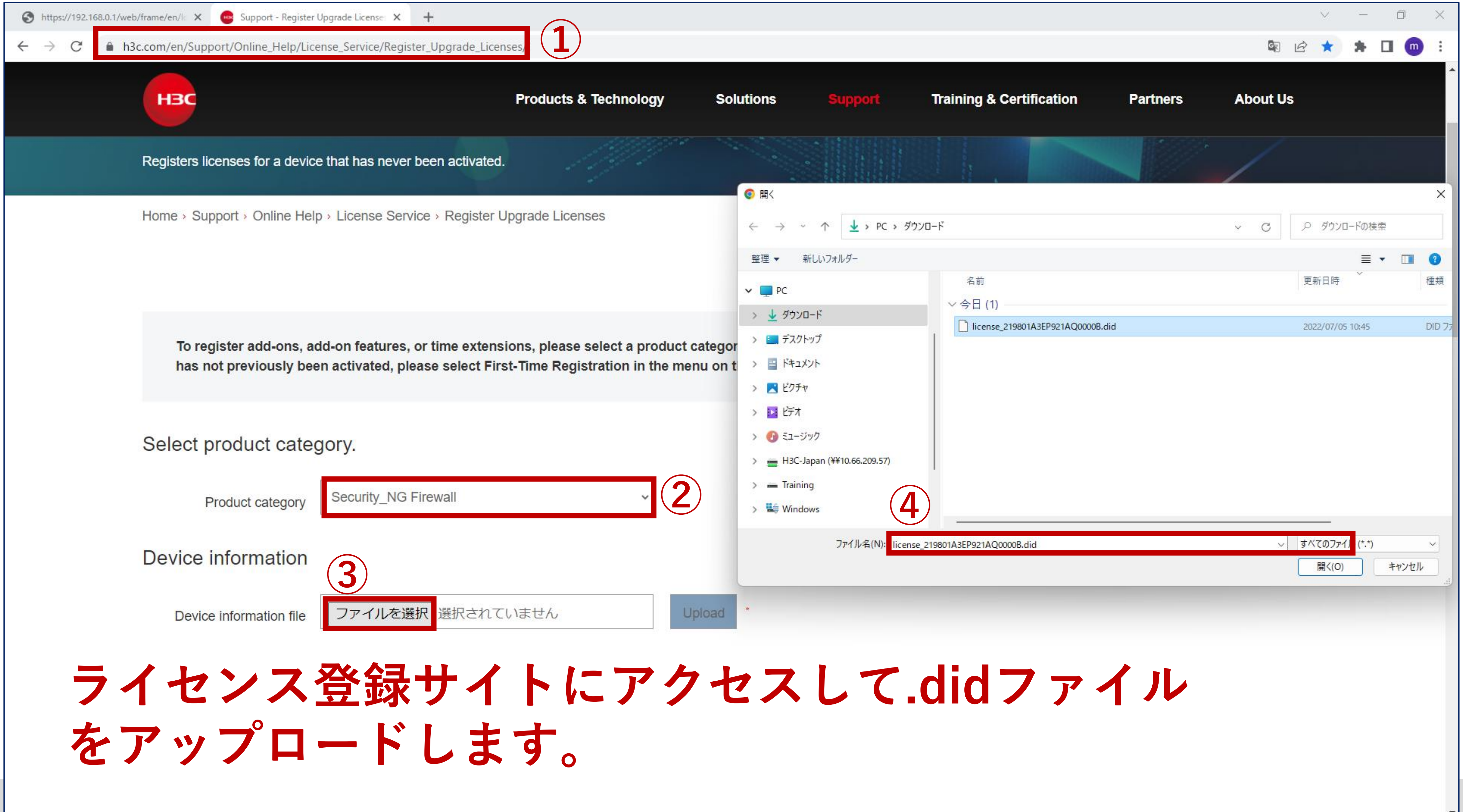
```
3132A04R              LIS-UIS-MANGERA-STD-2                      1007005060013
213132A04R02010001C3  <==>  213132A04R02010001C3                 1      份 / PCS
```

重要信息，请妥善保存

Caution: Please keep this certificate carefully,
you may need to use it in the future.

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/



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

Registers licenses for a device that has never been activated.

Home › Support › Online Help › License Service › Register Upgrade Licenses

To register add-ons, add-on features, or time extensions, please select a product categor
has not previously been activated, please select First-Time Registration in the menu on t

Select product category.

Product category: Security_NG Firewall

Device information

Device information file: ファイルを選択 選択されていません Upload *

開く

PC › ダウンロード

license_219801A3EP921AQ0000B.did 2022/07/05 10:45 DID ファ

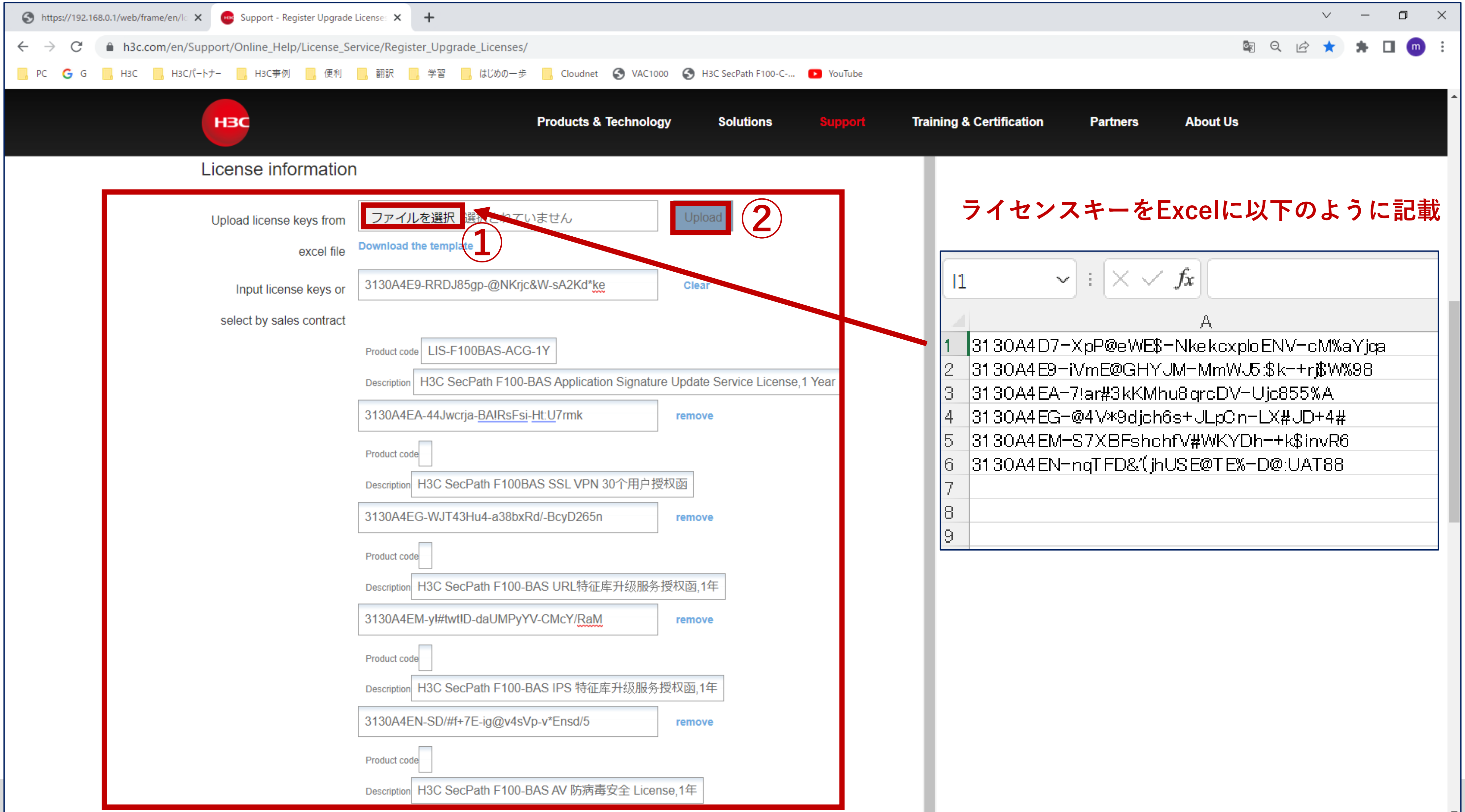
ファイル名(N): license_219801A3EP921AQ0000B.did

すべてのファイル (*.*)

開く(O) キャンセル

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 excel file: ファイルを選択 選択されていません [Upload]

Download the template

Input license keys or select by sales contract: 3130A4E9-RRDJ85gp-@NKrjc&W-sA2Kd*ke — Clear

Product code: LIS-F100BAS-ACG-1Y

Description: H3C SecPath F100-BAS Application Signature Update Service License,1 Year

3130A4EA-44Jwcrja-BA!RsFsi-Ht:U7rmk — remove

Product code:

Description: H3C SecPath F100BAS SSL VPN 30个用户授权函

3130A4EG-WJT43Hu4-a38bxRd/-BcyD265n — remove

Product code:

Description: H3C SecPath F100-BAS URL特征库升级服务授权函,1年

3130A4EM-y!#twt!D-daUMPyYV-CMcY/RaM — remove

Product code:

Description: H3C SecPath F100-BAS IPS 特征库升级服务授权函,1年

3130A4EN-SD/#f+7E-ig@v4sVp-v*Ensd/5 — remove

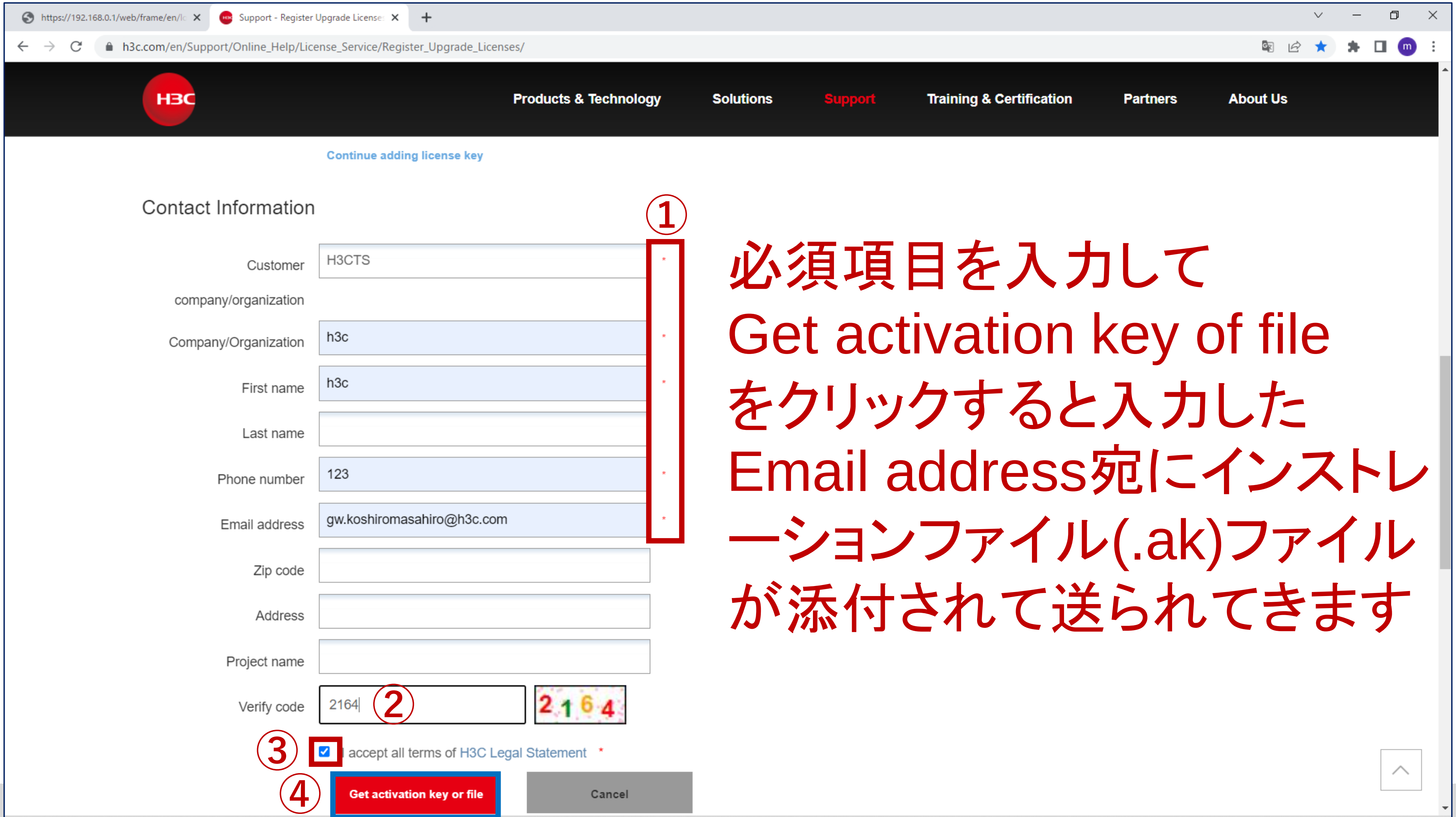
Product code:

Description: H3C SecPath F100-BAS AV 防病毒安全 License,1年

ライセンスキーをExcelに以下のように記載

	A
1	3130A4D7-XpP@eWE$-NkekcxploENV-cM%aYjqa
2	3130A4E9-iVmE@GHYJM-MmWJ5:$k-+rj$W%98
3	3130A4EA-7!ar#3kKMhu8qrcDV-Ujc855%A
4	3130A4EG-@4V*9djch6s+JLpCn-LX#JD+4#
5	3130A4EM-S7XBFshchfV#WKYDh-+k$invR6
6	3130A4EN-nqTFD&'(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/lc
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 company/organization	H3CTS
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

①

② 2164

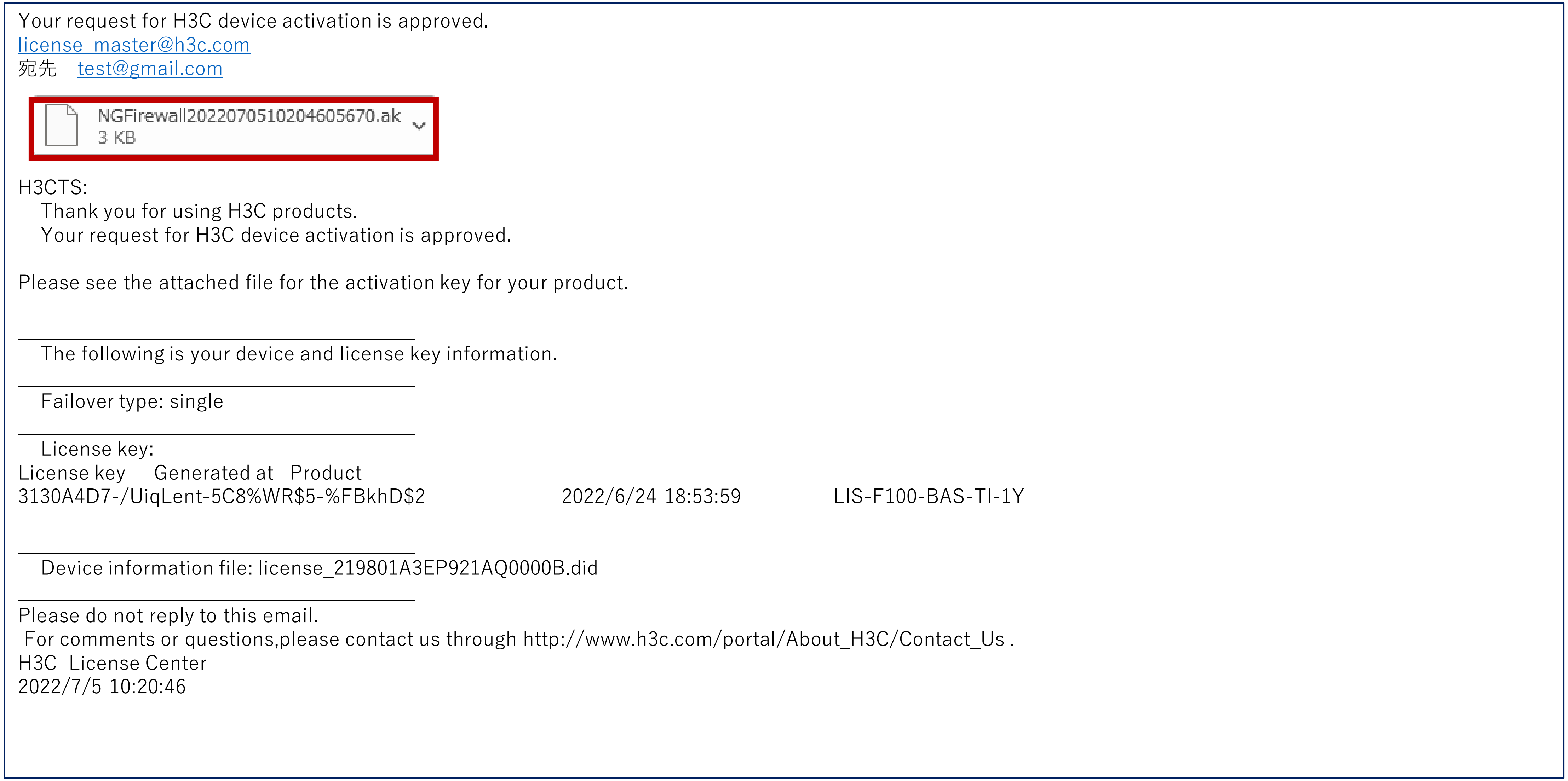
③ ☑ I accept all terms of H3C Legal Statement *

④ Get activation key or file

Cancel

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

インストレーション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

NGFirewall2022070510204605670.ak
3 KB

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

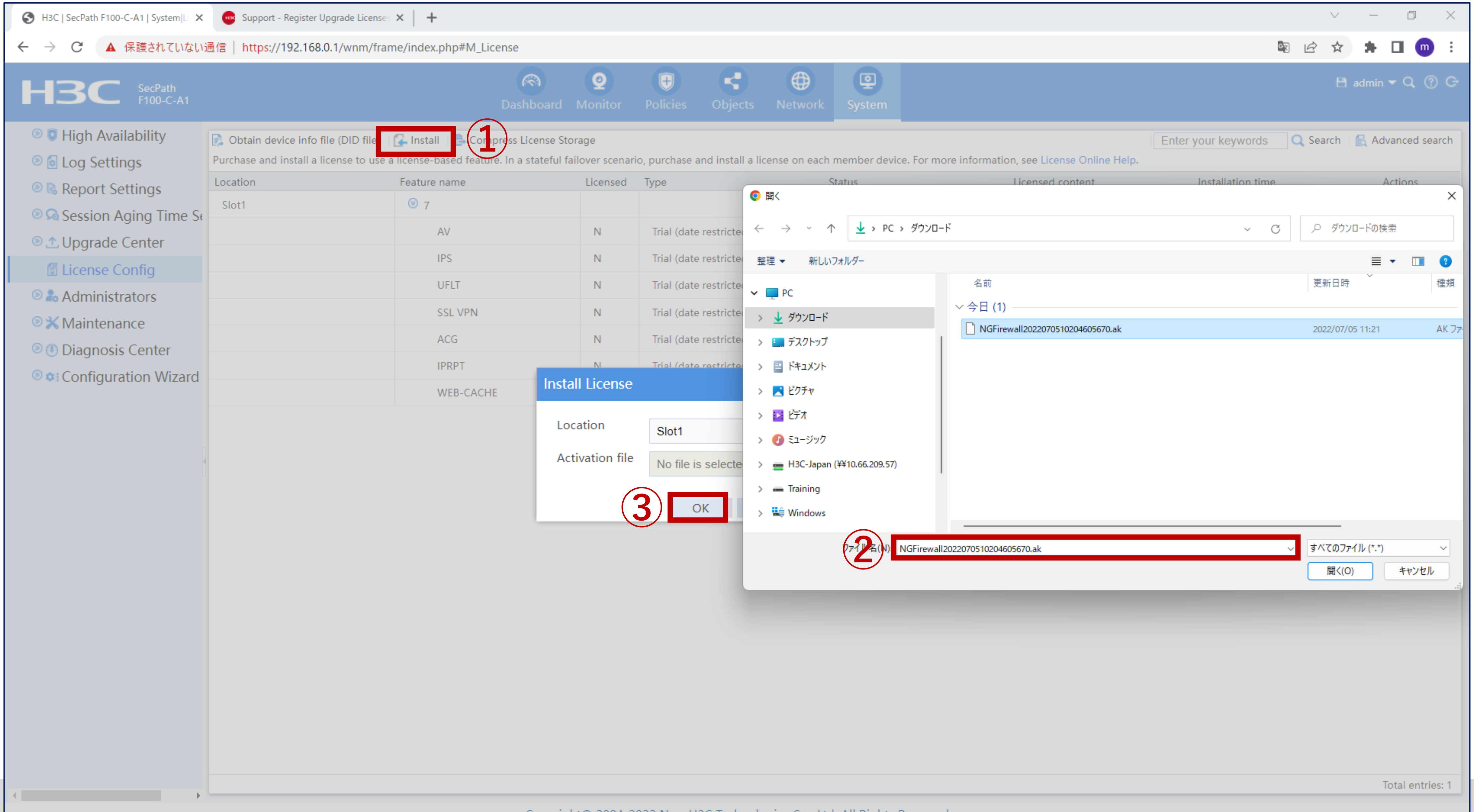
05 各種ログの環境整備

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。



① Install

Purchase and install a license to use a license-based feature. In a stateful failover scenario, purchase and install a license on each member device. For more information, see License Online Help.

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						

Install License

Location: Slot1

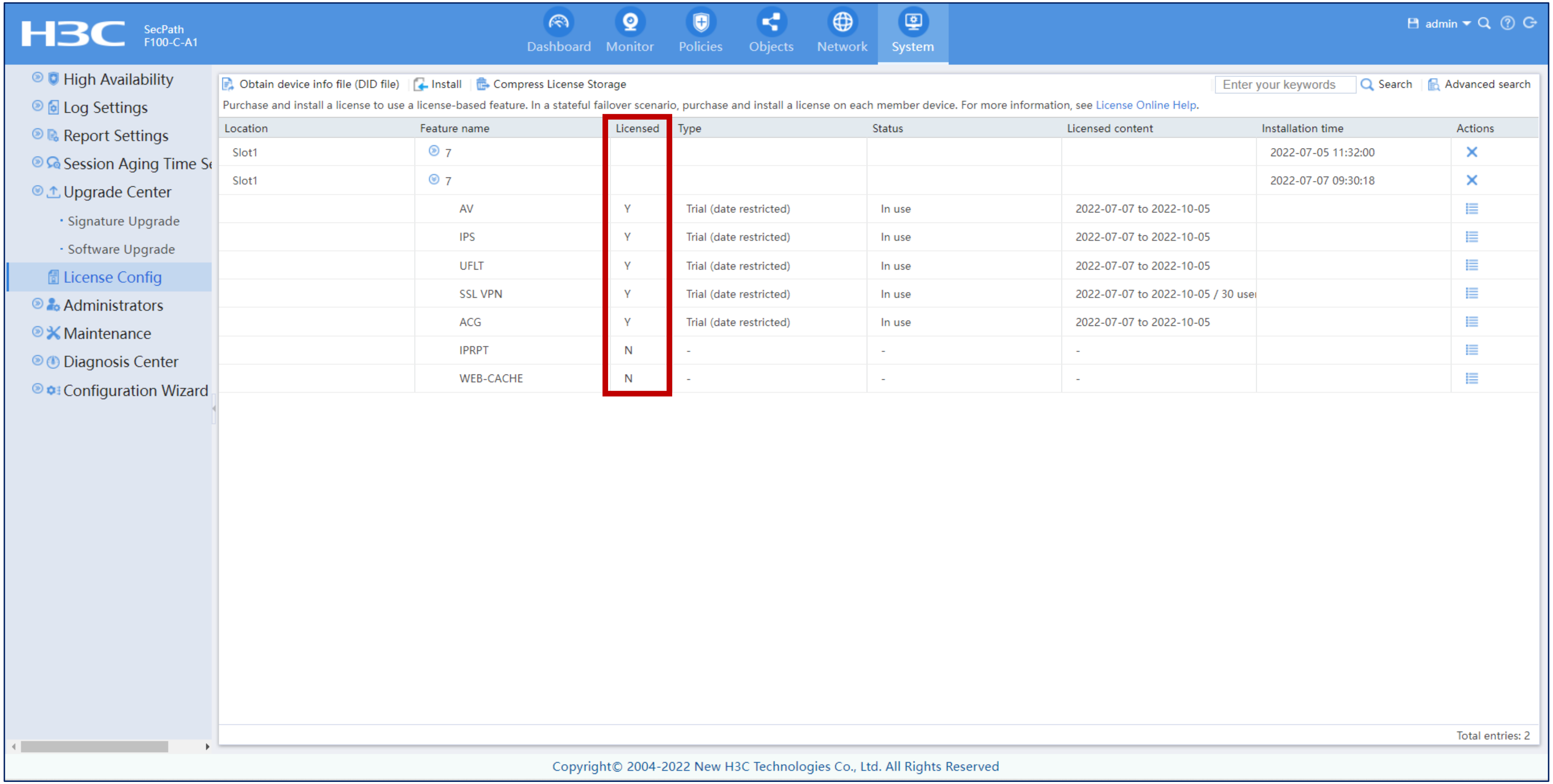
Activation file: No file is selecte

③ OK

名前	更新日時	種類
今日 (1)		
NGFirewall20220705102046 05670.ak	2022/07/05 11:21	AK ファ

② ファイル名(N): NGFirewall2022070510204605670.ak

購入したライセンスが有効になりました



Purchase and install a license to use a license-based feature. In a stateful failover scenario, purchase and install a license on each member device. For more information, see License Online Help.

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

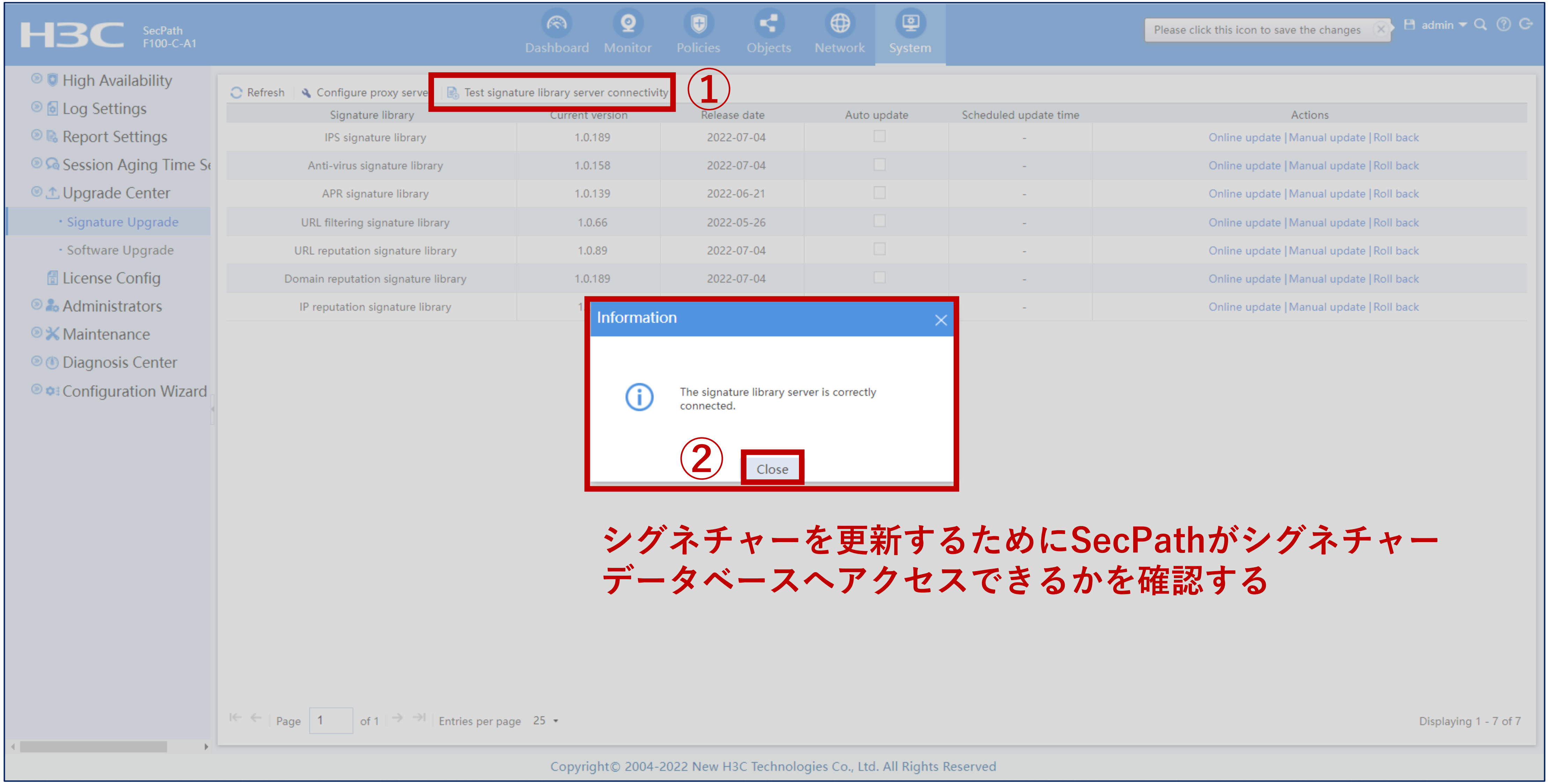
05 各種ログの環境整備

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



Signature library	Current version	Release date	Auto update	Scheduled update time	Actions
IPS signature library	1.0.189	2022-07-04	□	-	Online update | Manual update | Roll back
Anti-virus signature library	1.0.158	2022-07-04	□	-	Online update | Manual update | Roll back
APR signature library	1.0.139	2022-06-21	□	-	Online update | Manual update | Roll back
URL filtering signature library	1.0.66	2022-05-26	□	-	Online update | Manual update | Roll back
URL reputation signature library	1.0.89	2022-07-04	□	-	Online update | Manual update | Roll back
Domain reputation signature library	1.0.189	2022-07-04	□	-	Online update | Manual update | Roll back
IP reputation signature library	1			-	Online update | Manual update | Roll back

Information

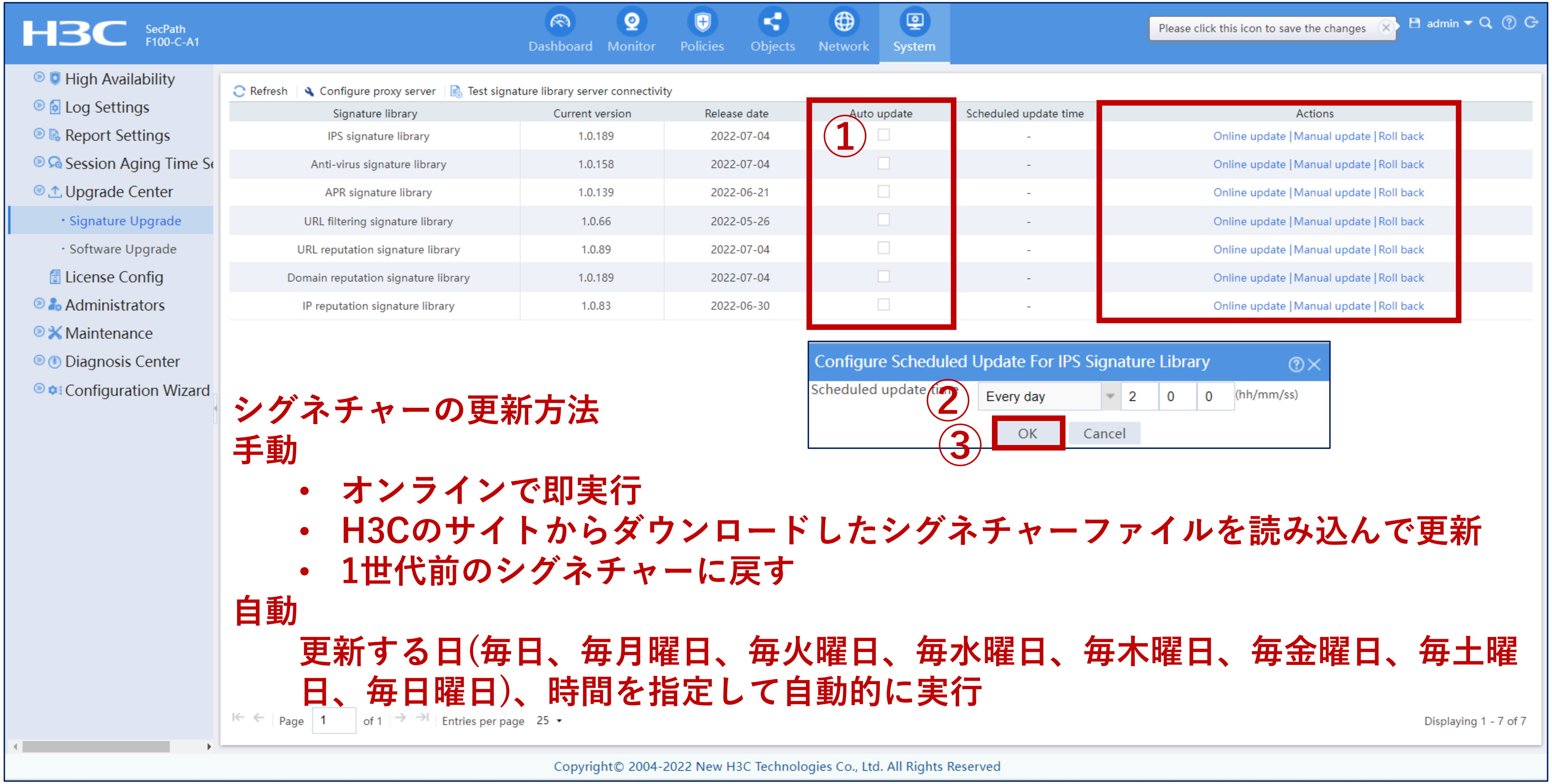
The signature library server is correctly connected.

Close

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



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

Configure Scheduled Update For IPS Signature Library

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

OK Cancel

シグネチャーの更新方法

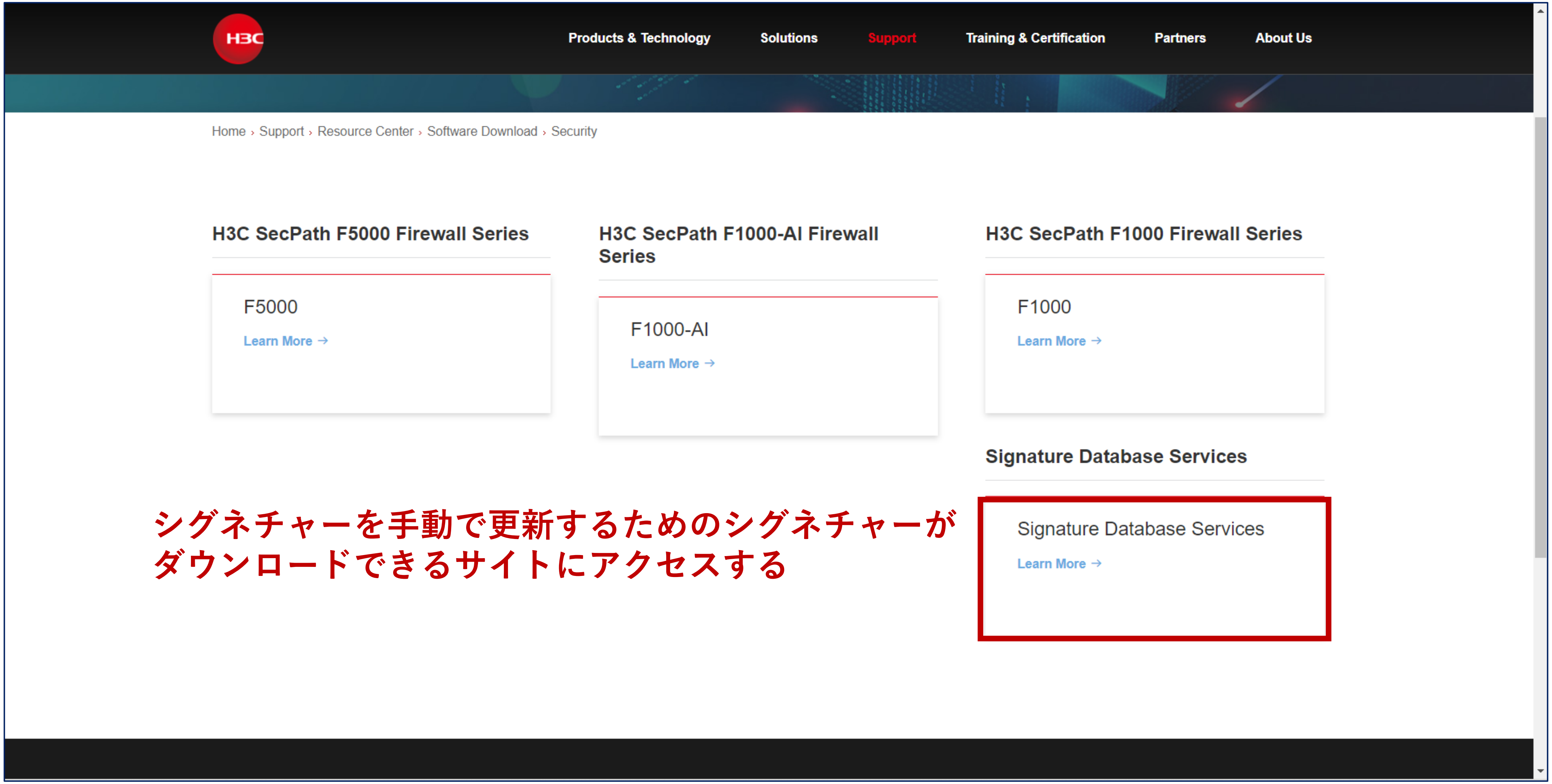
手動

- 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

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 →

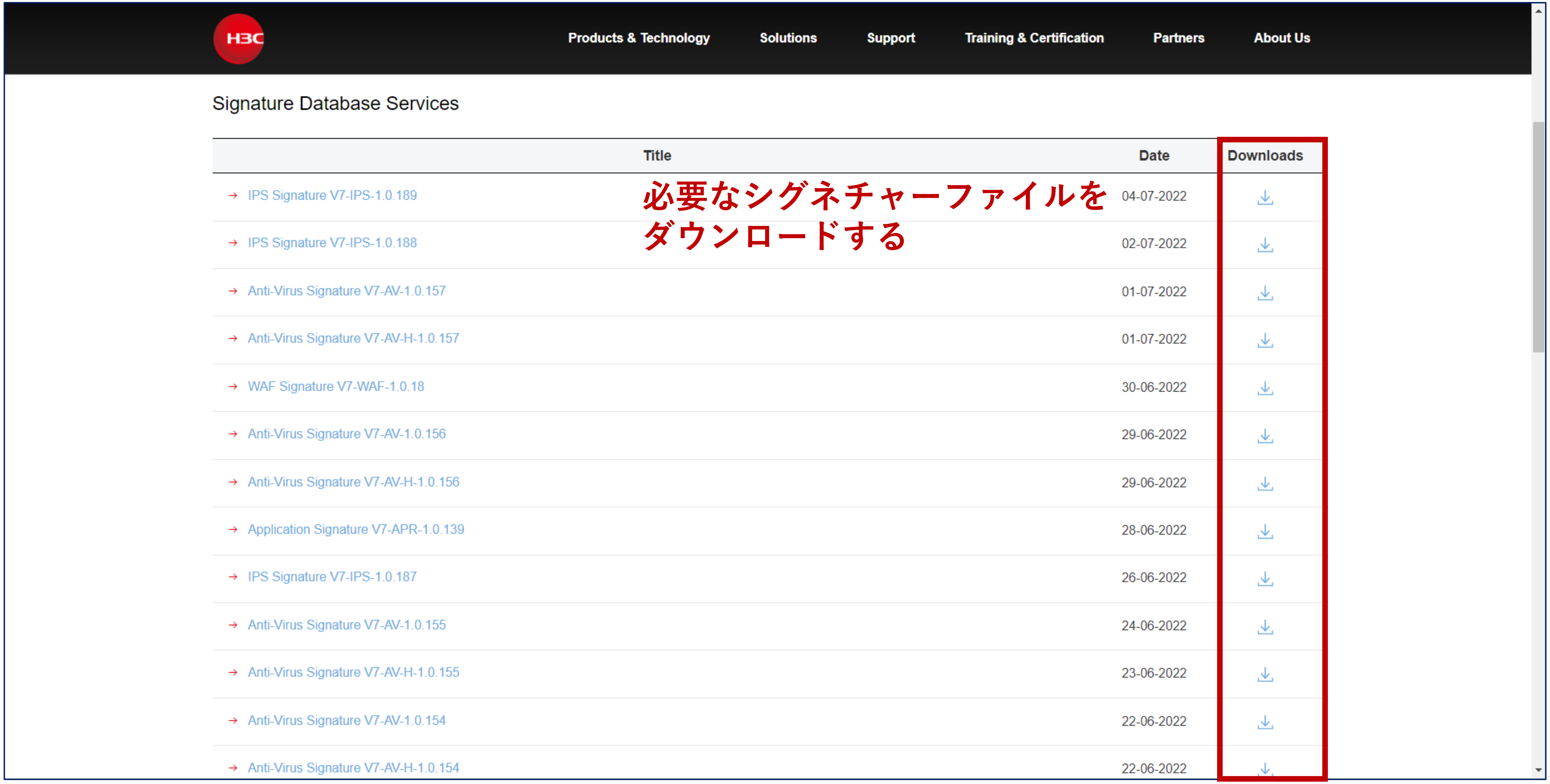
Signature Database Services

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	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	⤓

必要なシグネチャーファイルを
ダウンロードする

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

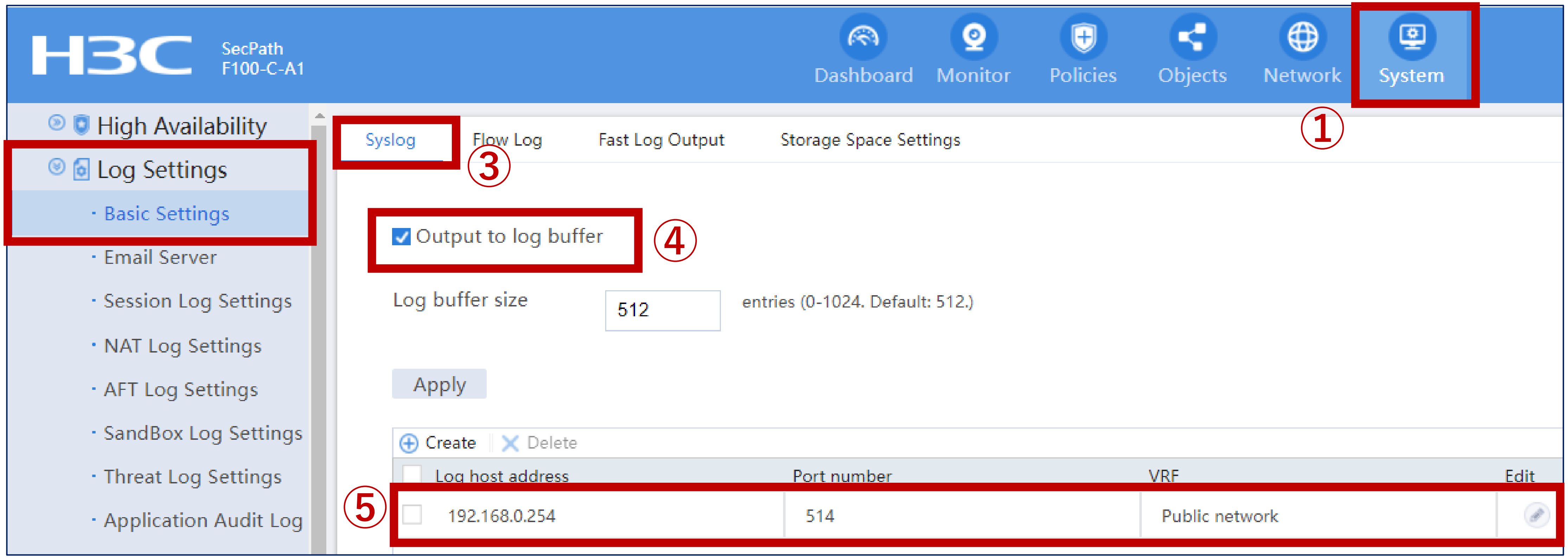
07 検証結果

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ーサ 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

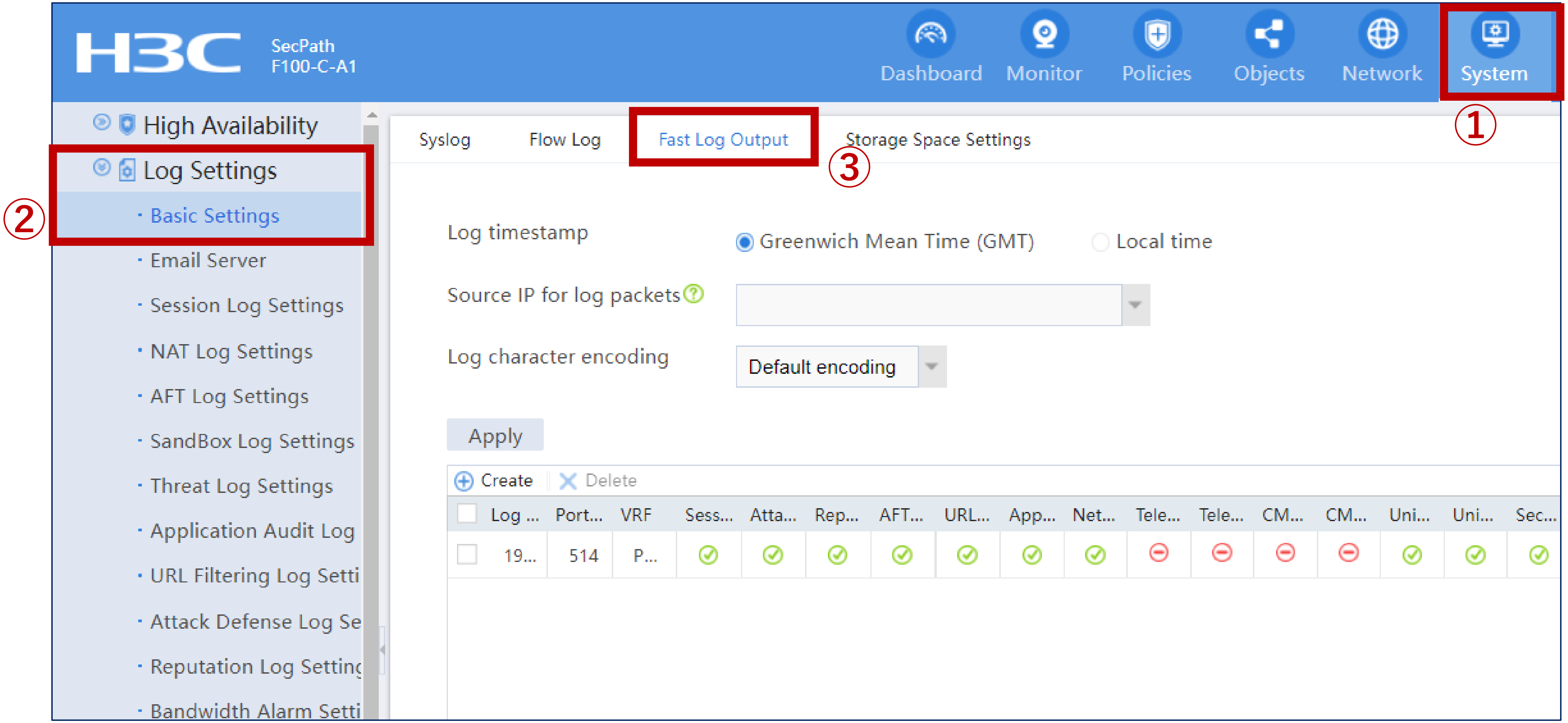


☑ Output to log buffer

Log buffer size: 512 entries (0-1024. Default: 512.)

□	Log host address	Port number	VRF	Edit
□	192.168.0.254	514	Public network	

ログに書き出す検知情報の指定



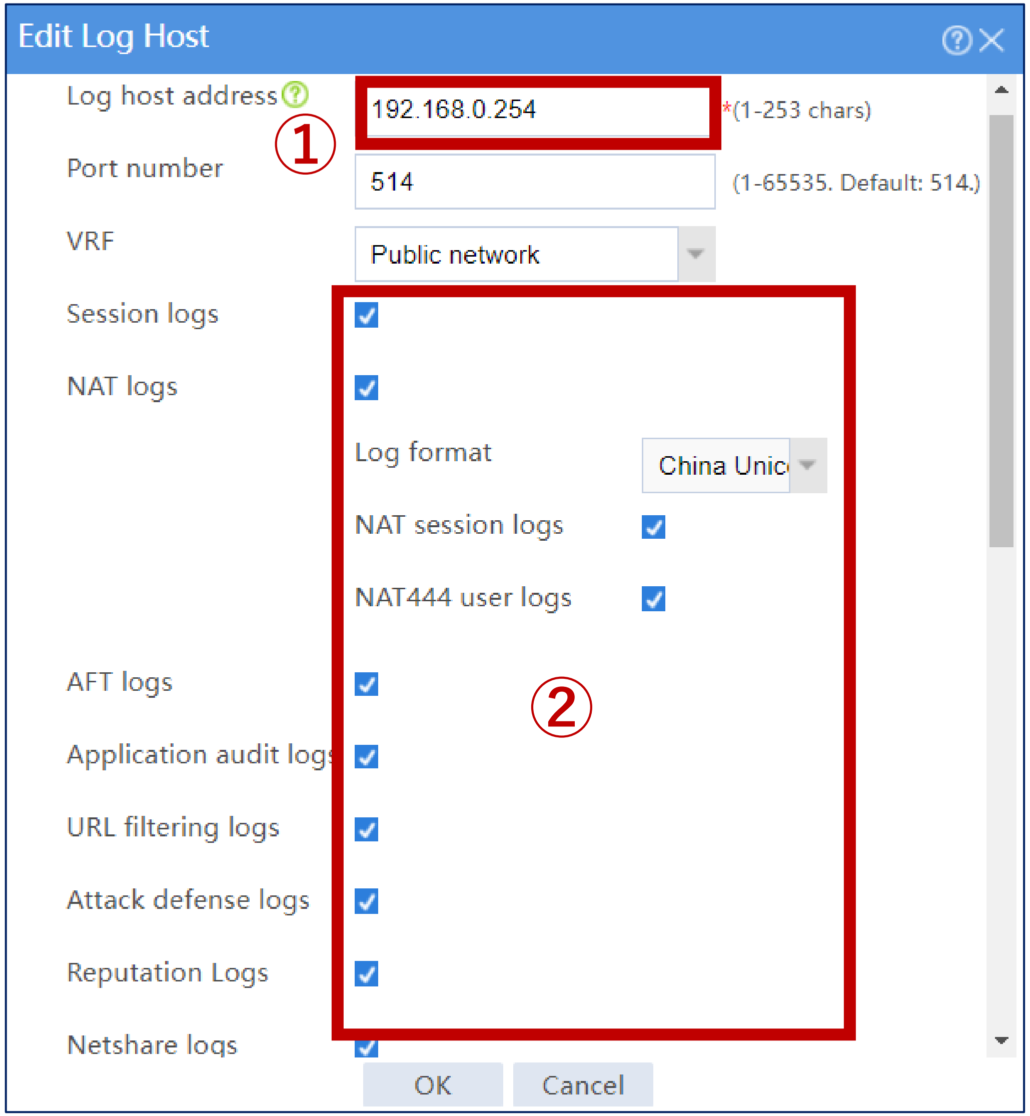
Log timestamp ● Greenwich Mean Time (GMT) ○ Local time

Source IP for log packets

Log character encoding Default encoding

□	Log ...	Port...	VRF	Sess...	Atta...	Rep...	AFT...	URL...	App...	Net...	Tele...	Tele...	CM...	CM...	Uni...	Uni...	Sec...
□	19...	514	P...	✓	✓	✓	✓	✓	✓	✓	⊖	⊖	⊖	⊖	✓	✓	✓

ログに書き出す検知情報の指定（続き）



Edit Log Host

① Log host address: 192.168.0.254 *(1-253 chars)

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

VRF: Public network

②

Session logs ☑

NAT logs ☑

- Log format: China Unic
- NAT session logs ☑
- NAT444 user logs ☑

AFT logs ☑

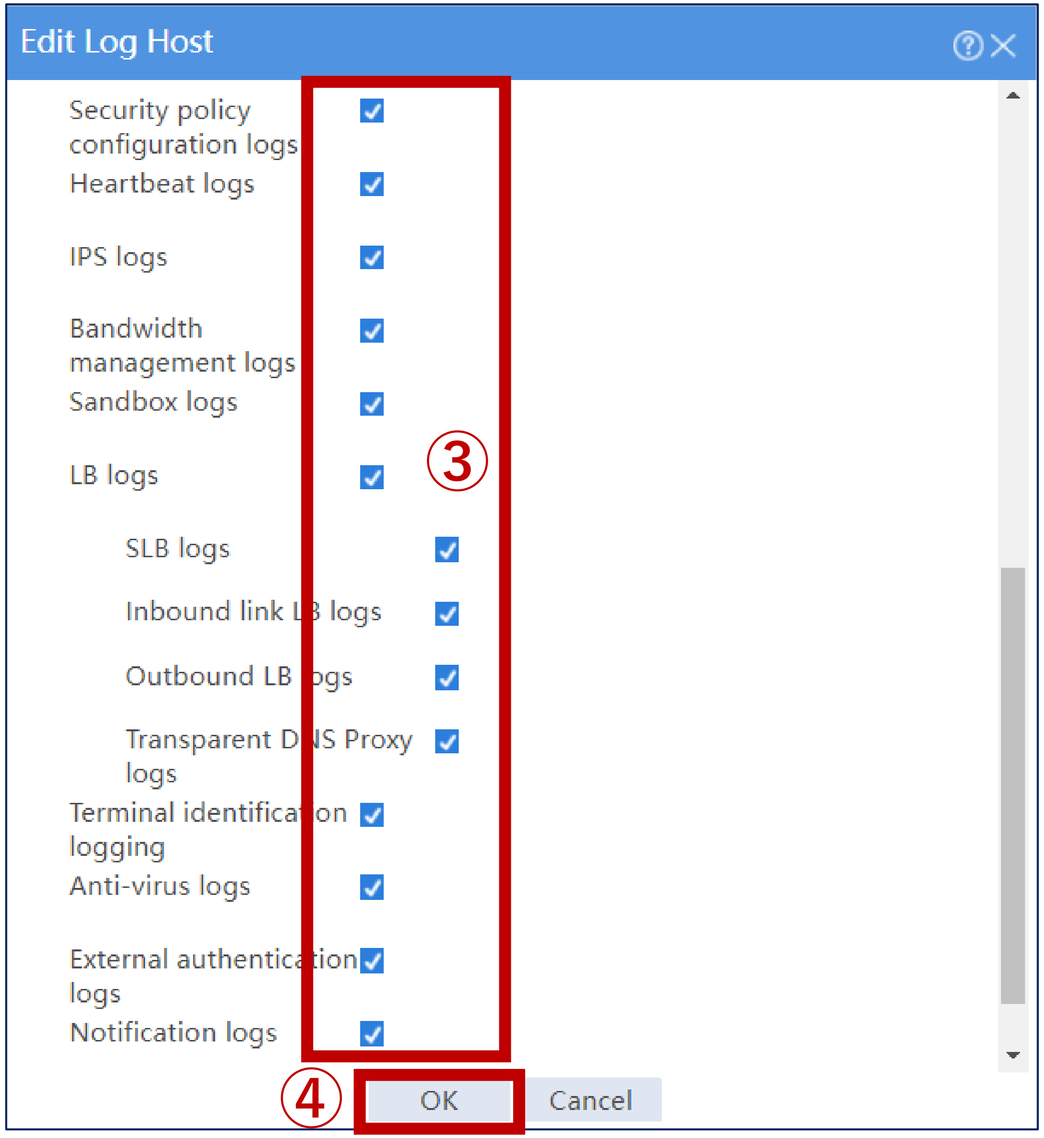
Application audit logs ☑

URL filtering logs ☑

Attack defense logs ☑

Reputation Logs ☑

Netshare logs ☑



Edit Log Host

③

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 ☑

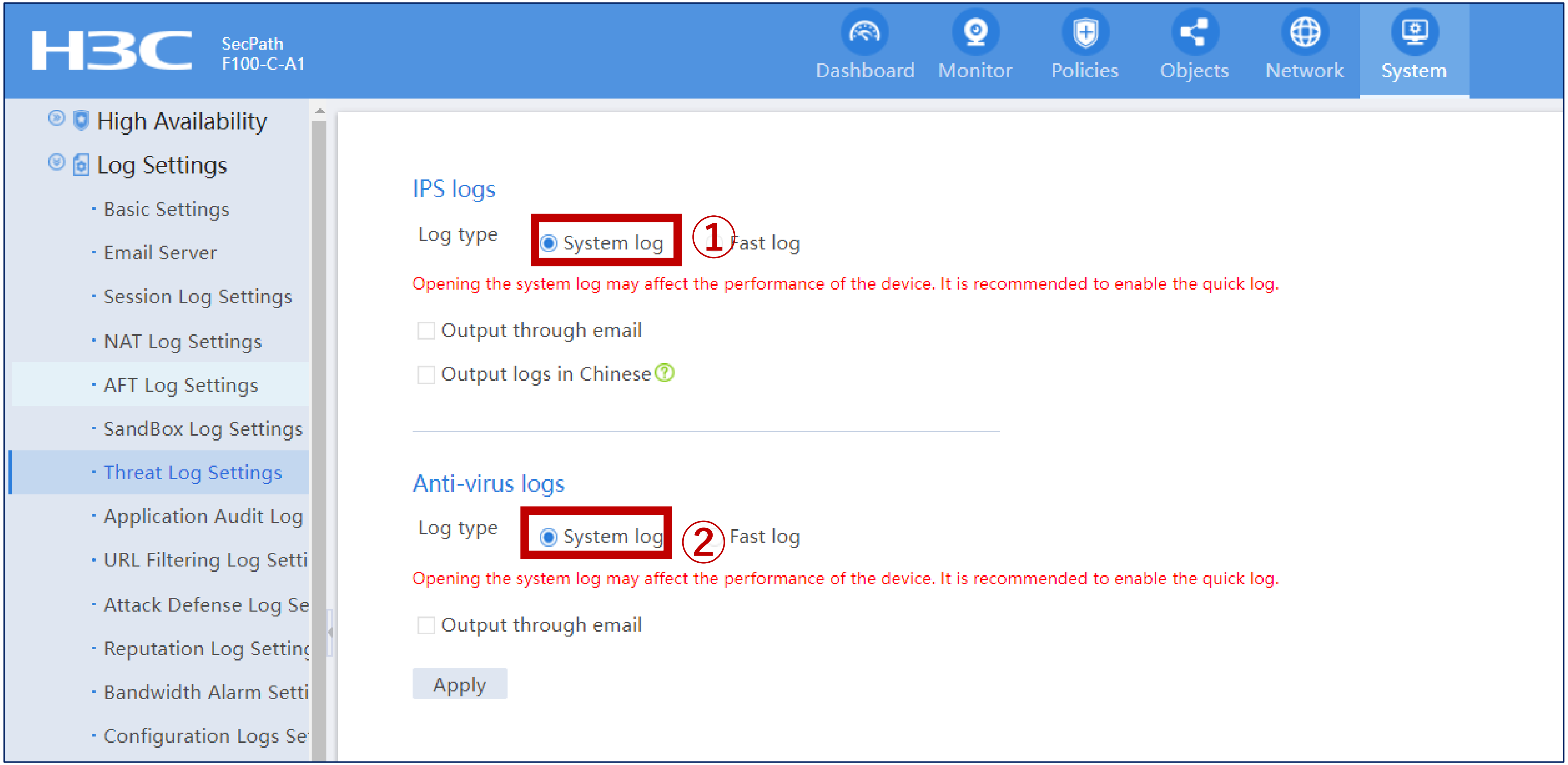
Anti-virus logs ☑

External authentication logs ☑

Notification logs ☑

④ OK

ログに書き出す検知情報の指定(続き)



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

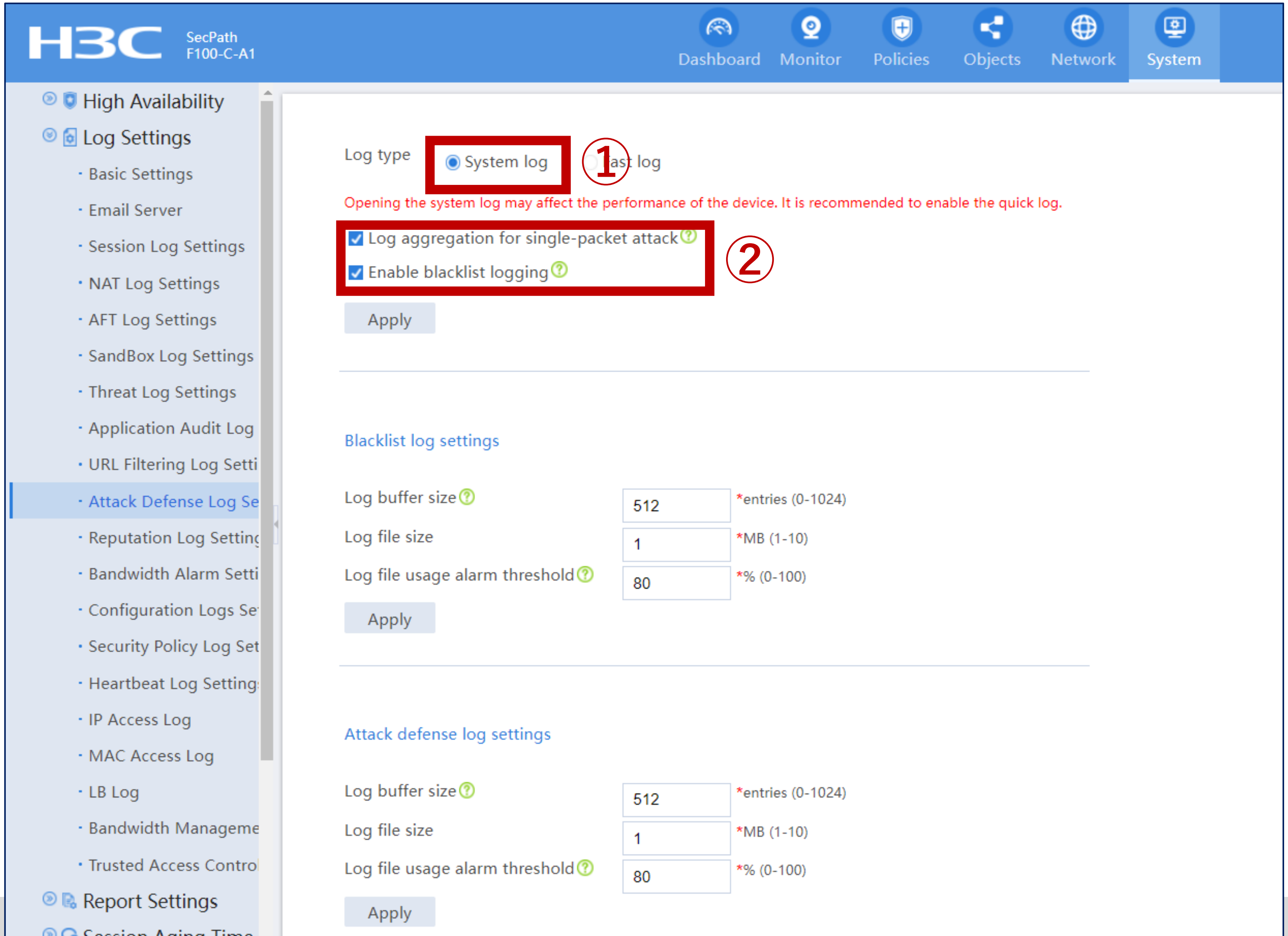
Log type ● System log ② ○ Fast log

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)



Log type ● System log ① ast 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 ②

Apply

Blacklist log settings

Log buffer size	512	*entries (0-1024)
Log file size	1	*MB (1-10)
Log file usage alarm threshold	80	*% (0-100)

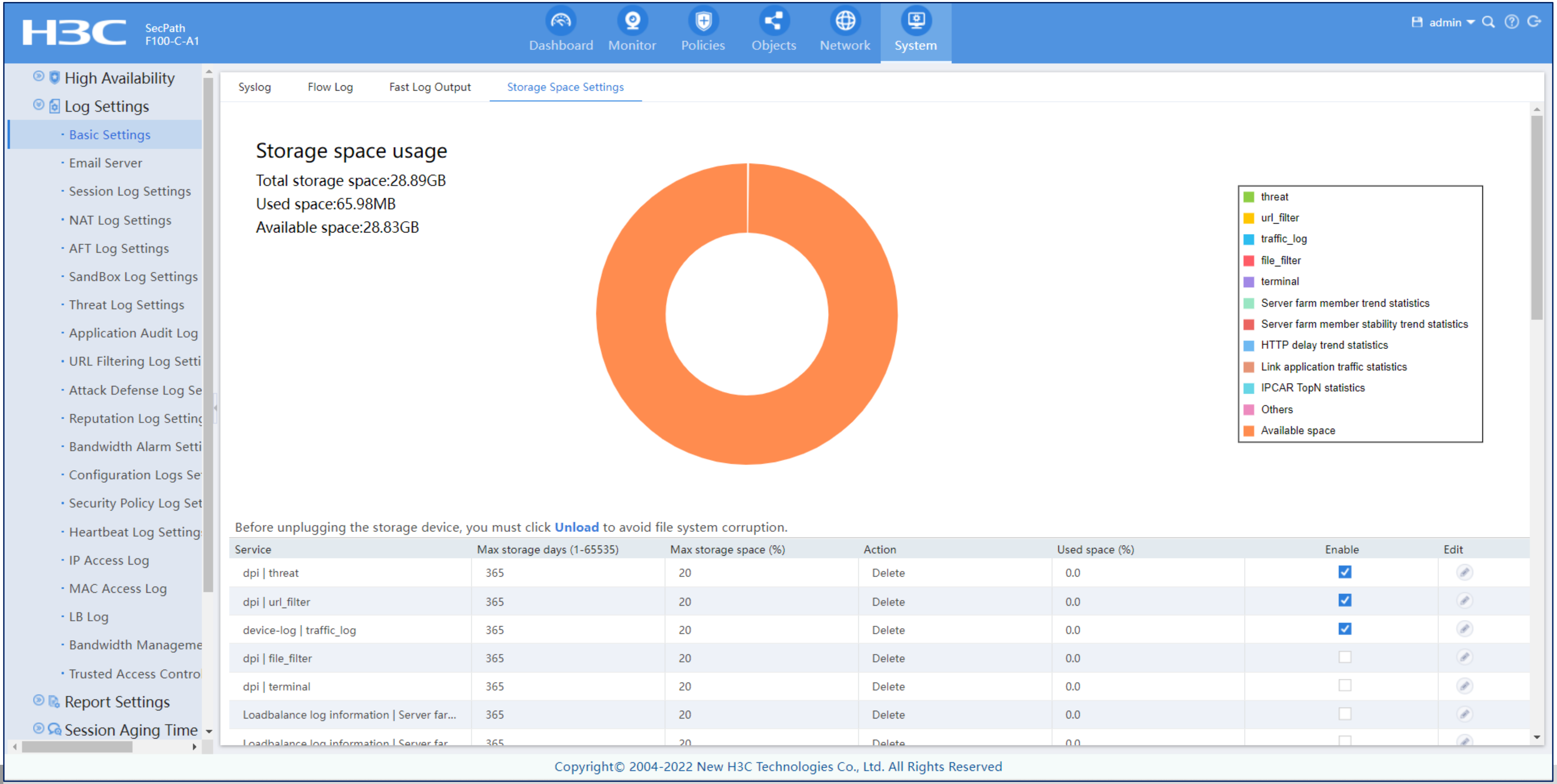
Apply

Attack defense log settings

Log buffer size	512	*entries (0-1024)
Log file size	1	*MB (1-10)
Log file usage alarm threshold	80	*% (0-100)

Apply

usba0:/のディスク使用状況



Storage space usage

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

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	☑	✎
dpi | url_filter	365	20	Delete	0.0	☑	✎
device-log | traffic_log	365	20	Delete	0.0	☑	✎
dpi | file_filter	365	20	Delete	0.0	□	✎
dpi | terminal	365	20	Delete	0.0	□	✎
Loadbalance log information | Server far...	365	20	Delete	0.0	□	✎
Loadbalance log information | Server far...	365	20	Delete	0.0	□	✎

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-threathost
  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-overviewrs
40 drw-          - Jul 07 2022 10:13:42   lb-overviewsf
41 drw-          - Jul 07 2022 10:13:40   lb-overviewvs
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)
```

syslogファイル

```
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

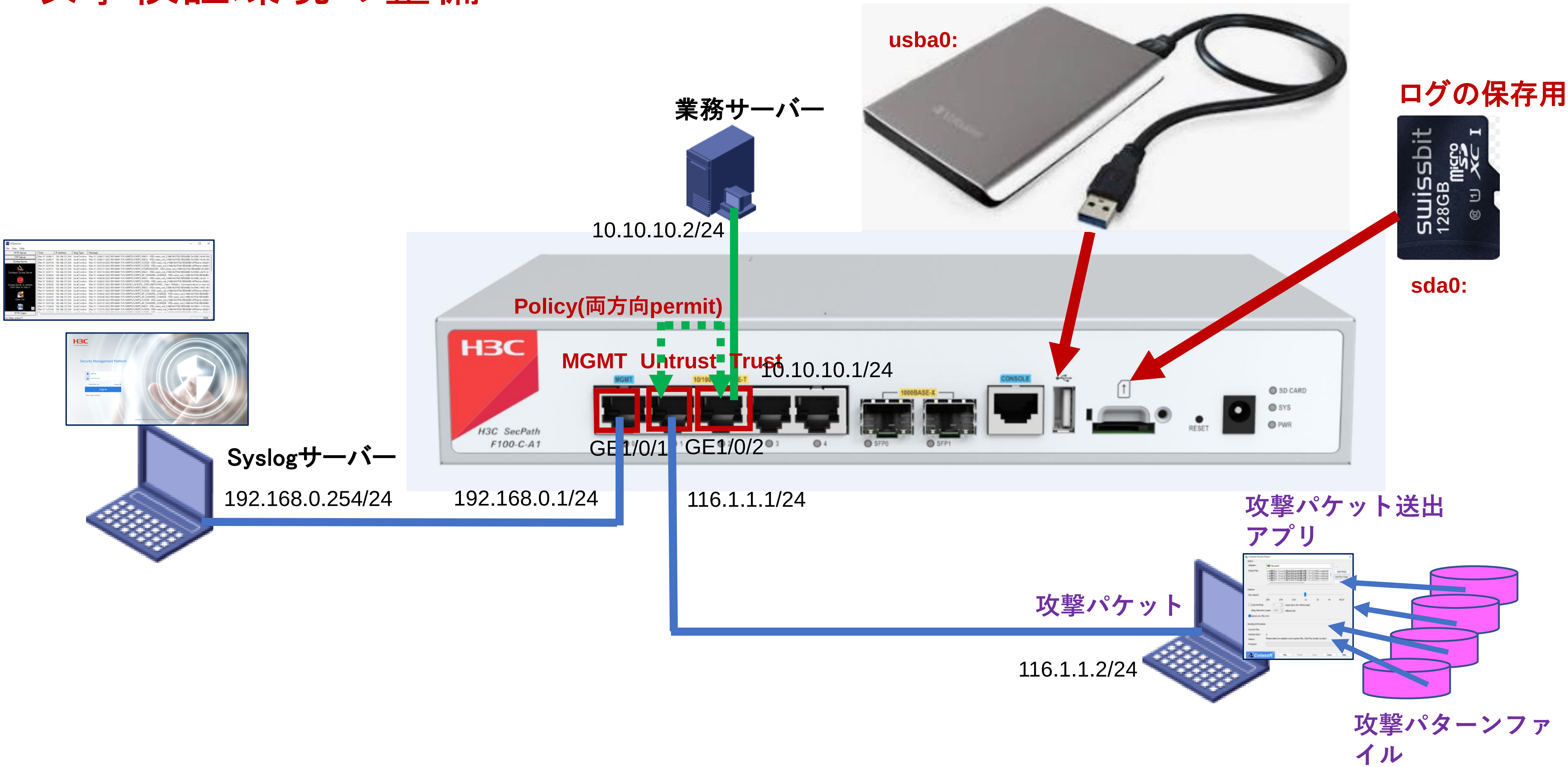
05 各種ログの環境整備

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



ログの保存用

usba0:

ログの保存用

sda0:

業務サーバー

10.10.10.2/24

Policy(両方向permit)

MGMT Untrust Trust

10.10.10.1/24

GE1/0/1 GE1/0/2

Syslogサーバー

192.168.0.254/24

192.168.0.1/24

116.1.1.1/24

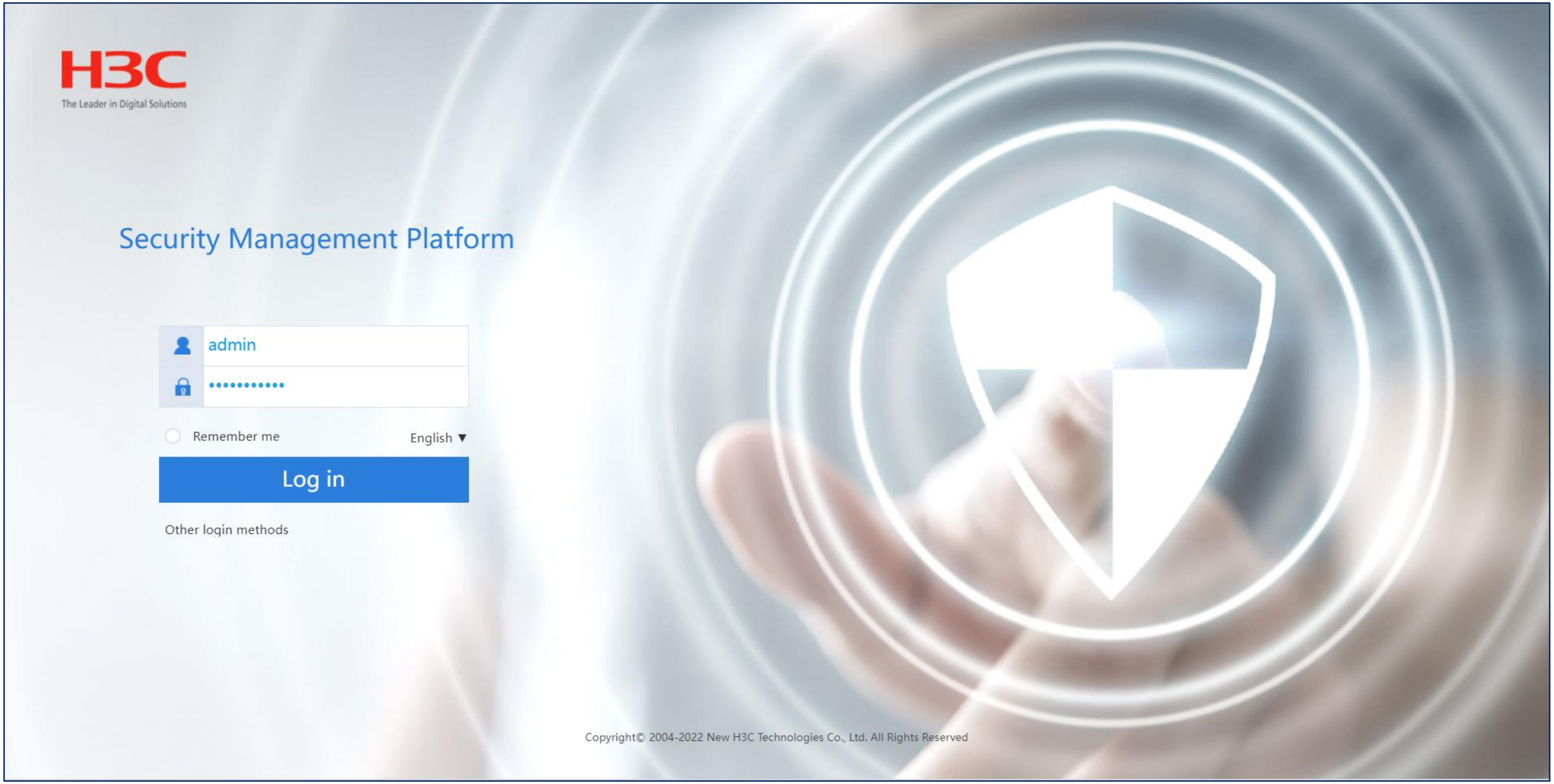
攻撃パケット送出アプリ

攻撃パケット

116.1.1.2/24

攻撃パターンファイル

https://192.168.0.1/でGUIにアクセス



H3C

The Leader in Digital Solutions

Security Management Platform

admin

••••••••••••

○ Remember me

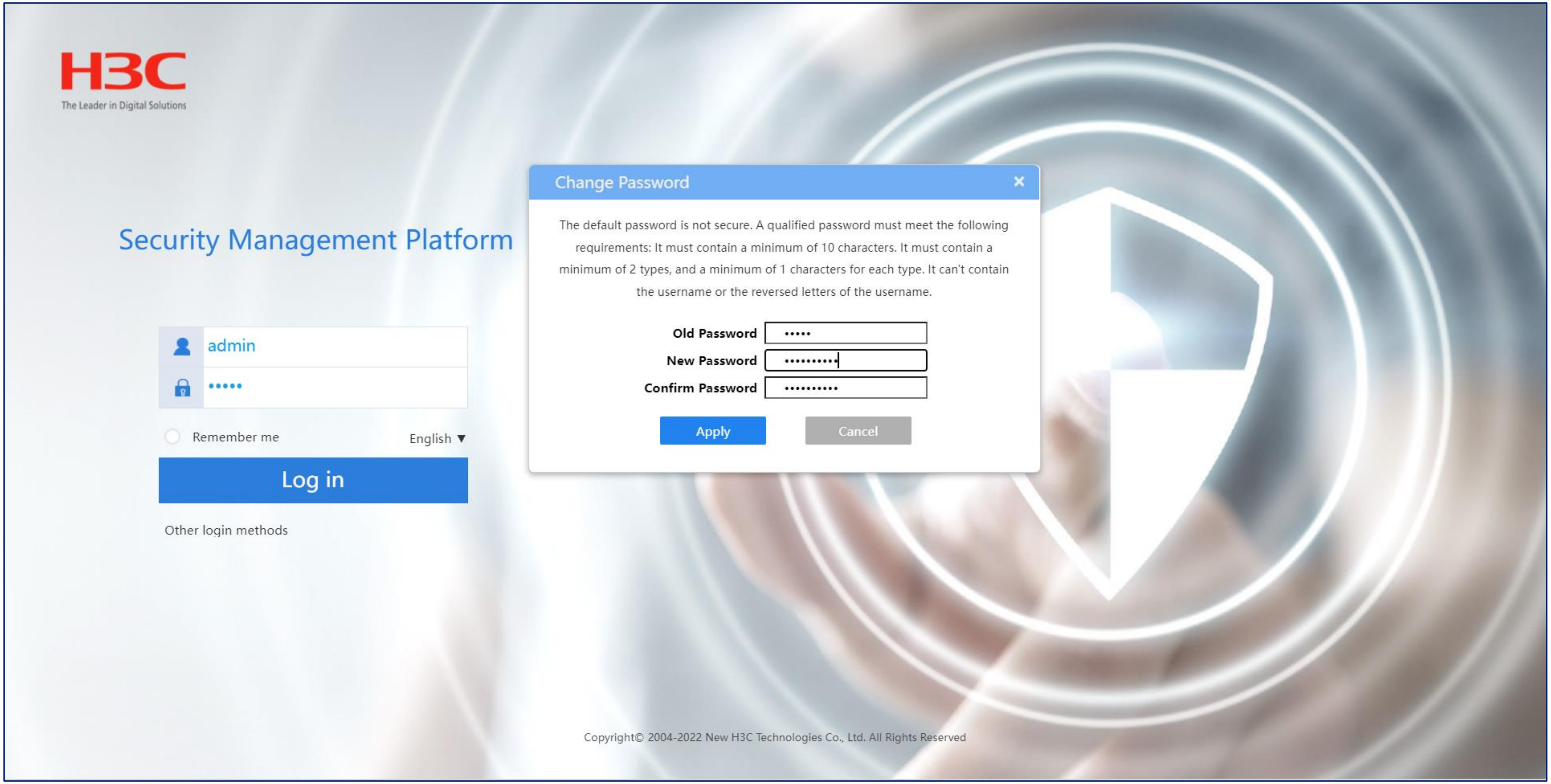
English ▼

Log in

Other login methods

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

初期パスワードの変更



Change Password ×

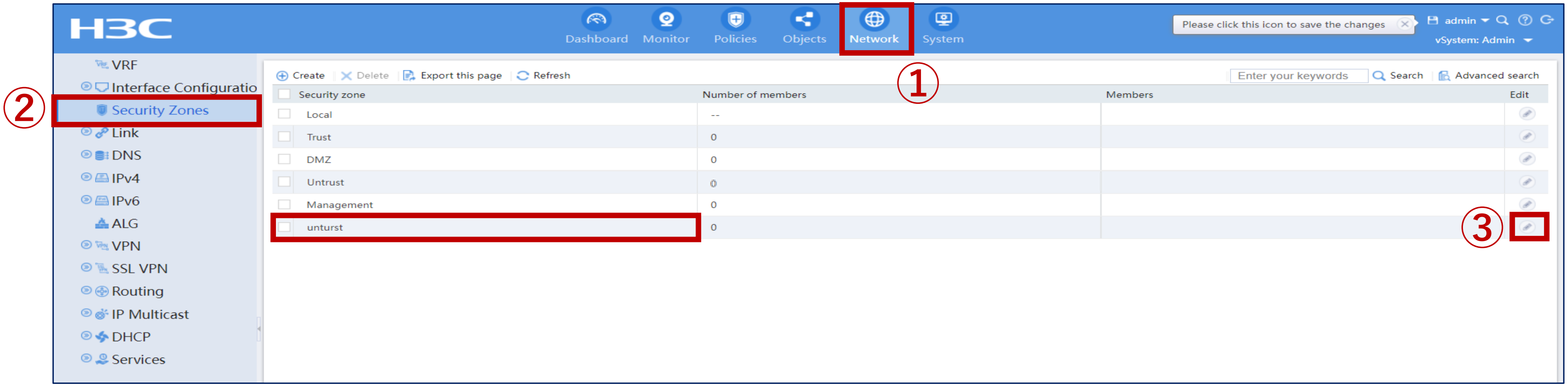
The default password is not secure. A qualified password must meet the following requirements: It must contain a minimum of 10 characters. It must contain a minimum of 2 types, and a minimum of 1 characters for each type. It can't contain the username or the reversed letters of the username.

Old Password •••••
New Password ••••••••••
Confirm Password ••••••••••

Apply Cancel

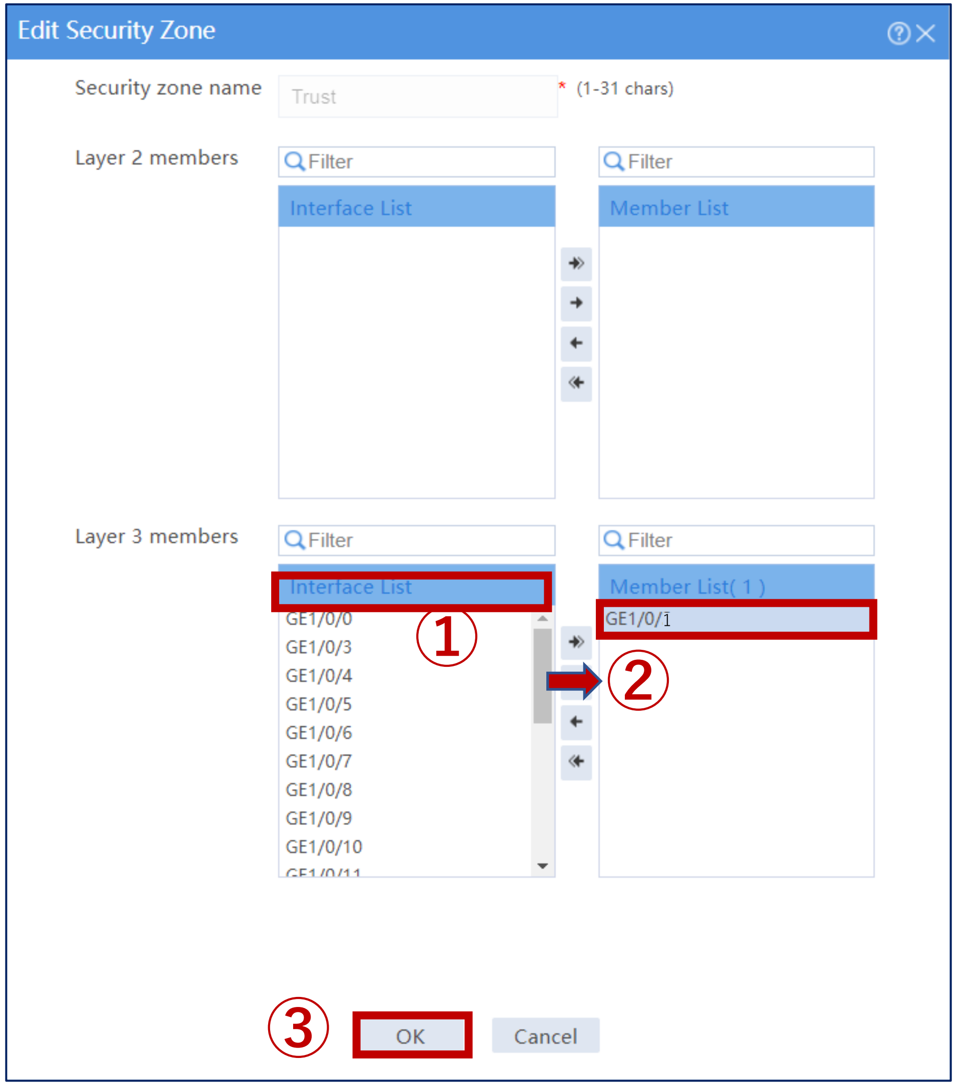
Copyright© 2004-2022 New H3C Technologies Co., Ltd. All Rights Reserved

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



Security zone	Number of members	Members	Edit
Local	--		
Trust	0		
DMZ	0		
Untrust	0		
Management	0		
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



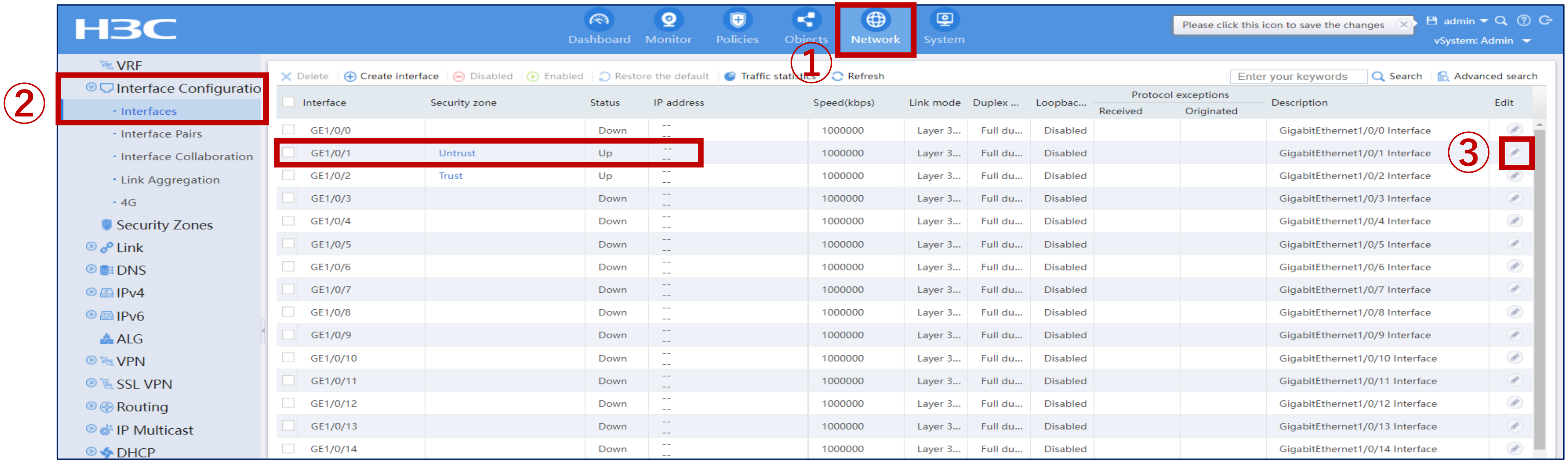
Edit Security Zone

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

Layer 2 members

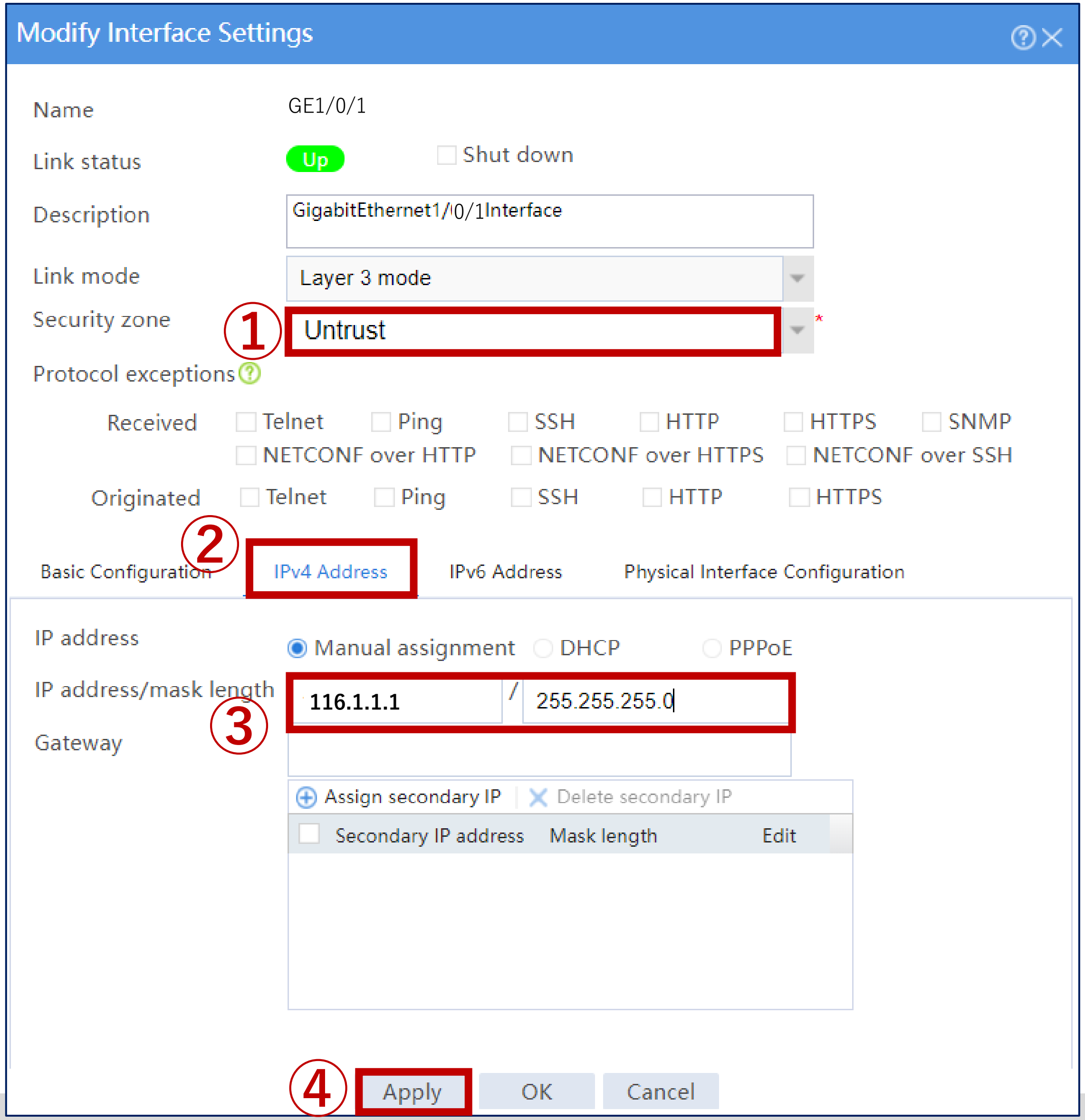
Layer 3 members

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



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

① Security zone: 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

② IPv4 Address

IP address: ● Manual assignment ○ DHCP ○ PPPoE

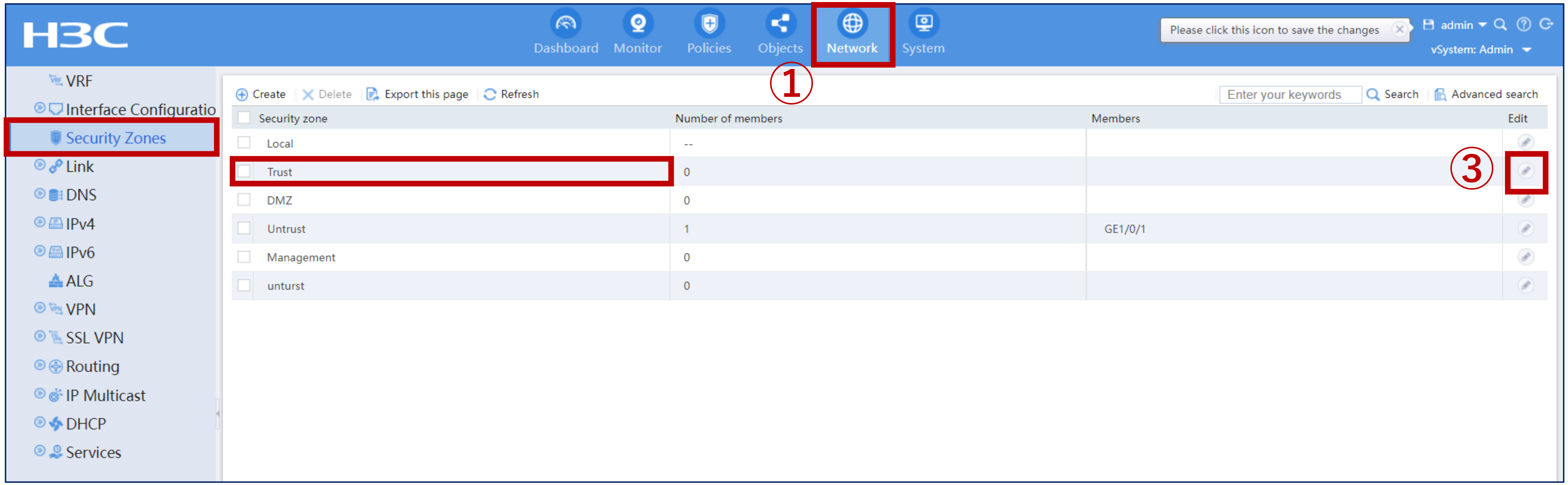
③ IP address/mask length: 116.1.1.1 / 255.255.255.0

Gateway:

□	Secondary IP address	Mask length	Edit

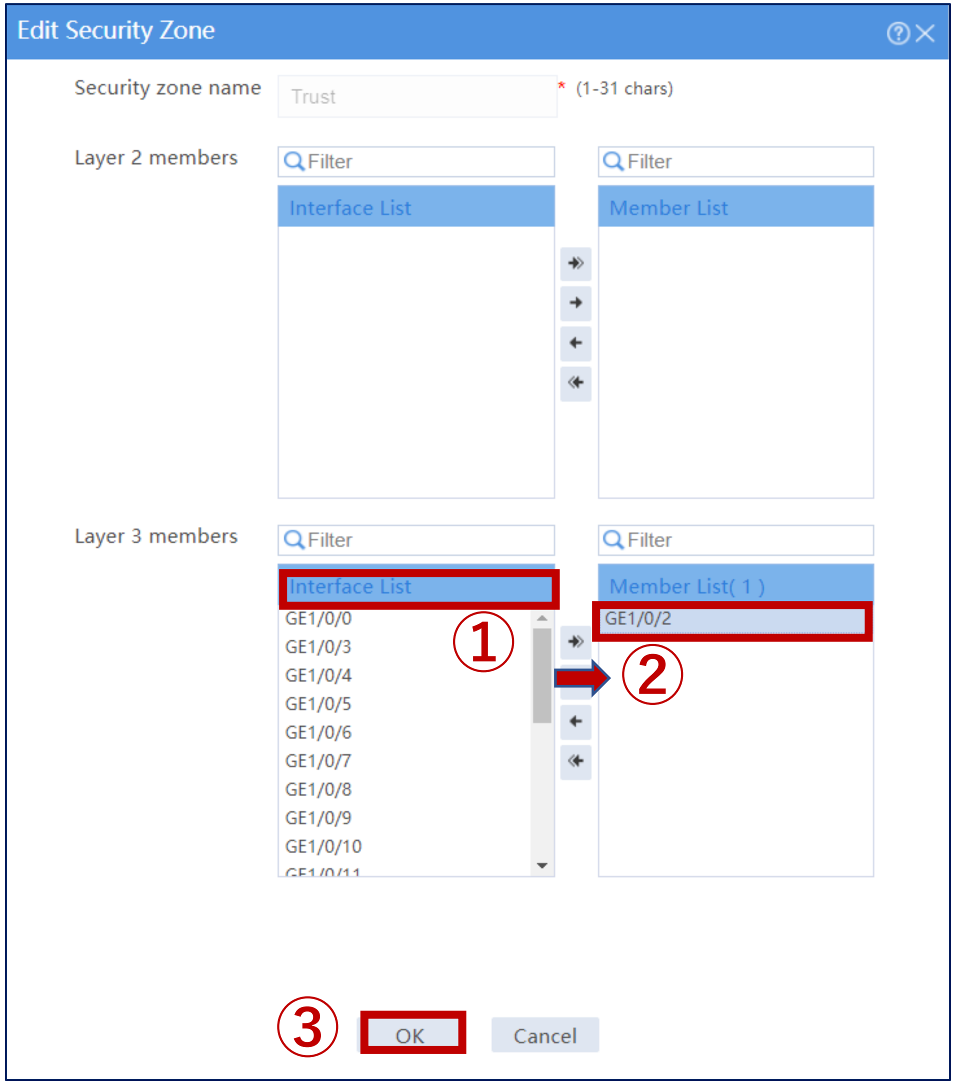
④ Apply

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



Security zone	Number of members	Members	Edit
Local	--		
Trust	0		
DMZ	0		
Untrust	1	GE1/0/1	
Management	0		
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



Edit Security Zone

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

Layer 2 members

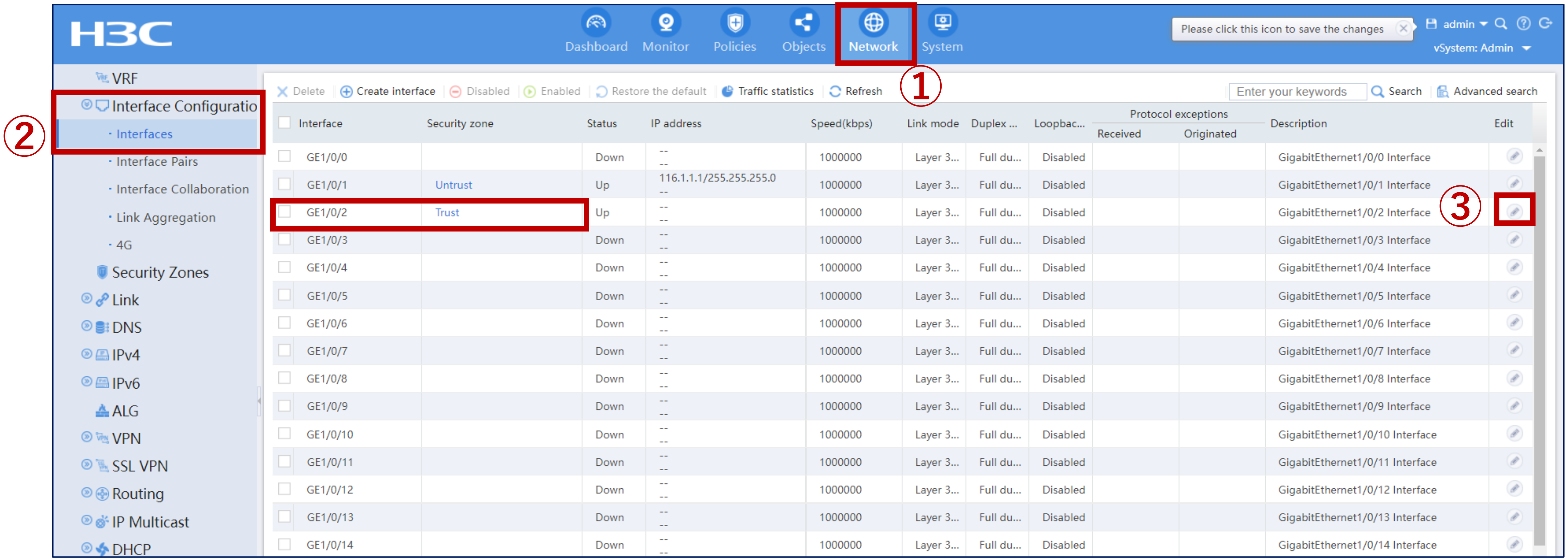
Layer 3 members

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

Member List(1)

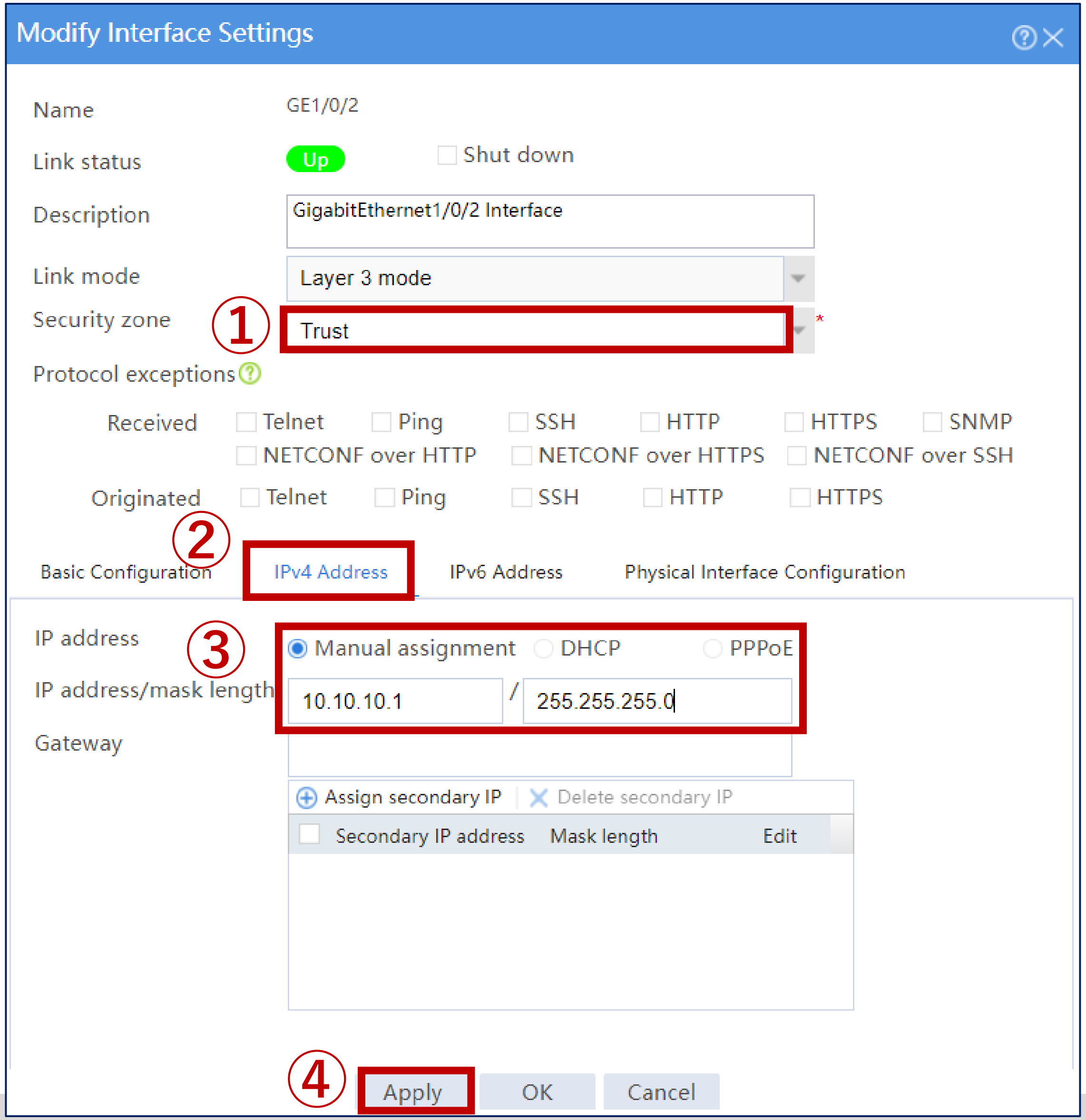
GE1/0/2

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



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

①
Security zone: 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

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

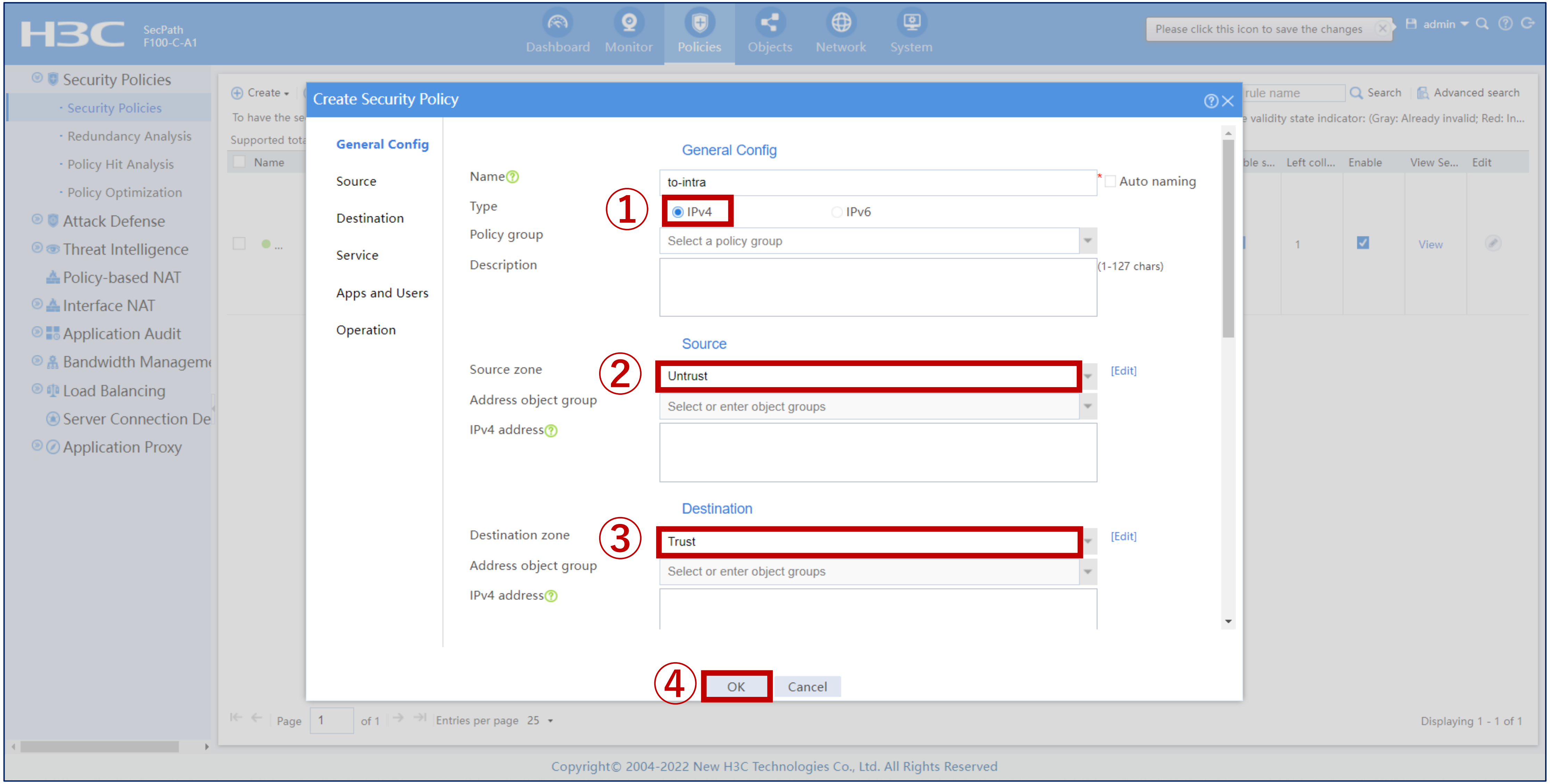
③
IP address: ● Manual assignment ○ DHCP ○ PPPoE

IP address/mask length: 10.10.10.1 / 255.255.255.0

Gateway:

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



Create Security Policy

General Config

Name: to-intra * □ Auto naming

① Type: ● IPv4 ○ IPv6

Policy group: Select a policy group

Description: (1-127 chars)

Source

② Source zone: Untrust [Edit]

Address object group: Select or enter object groups

IPv4 address:

Destination

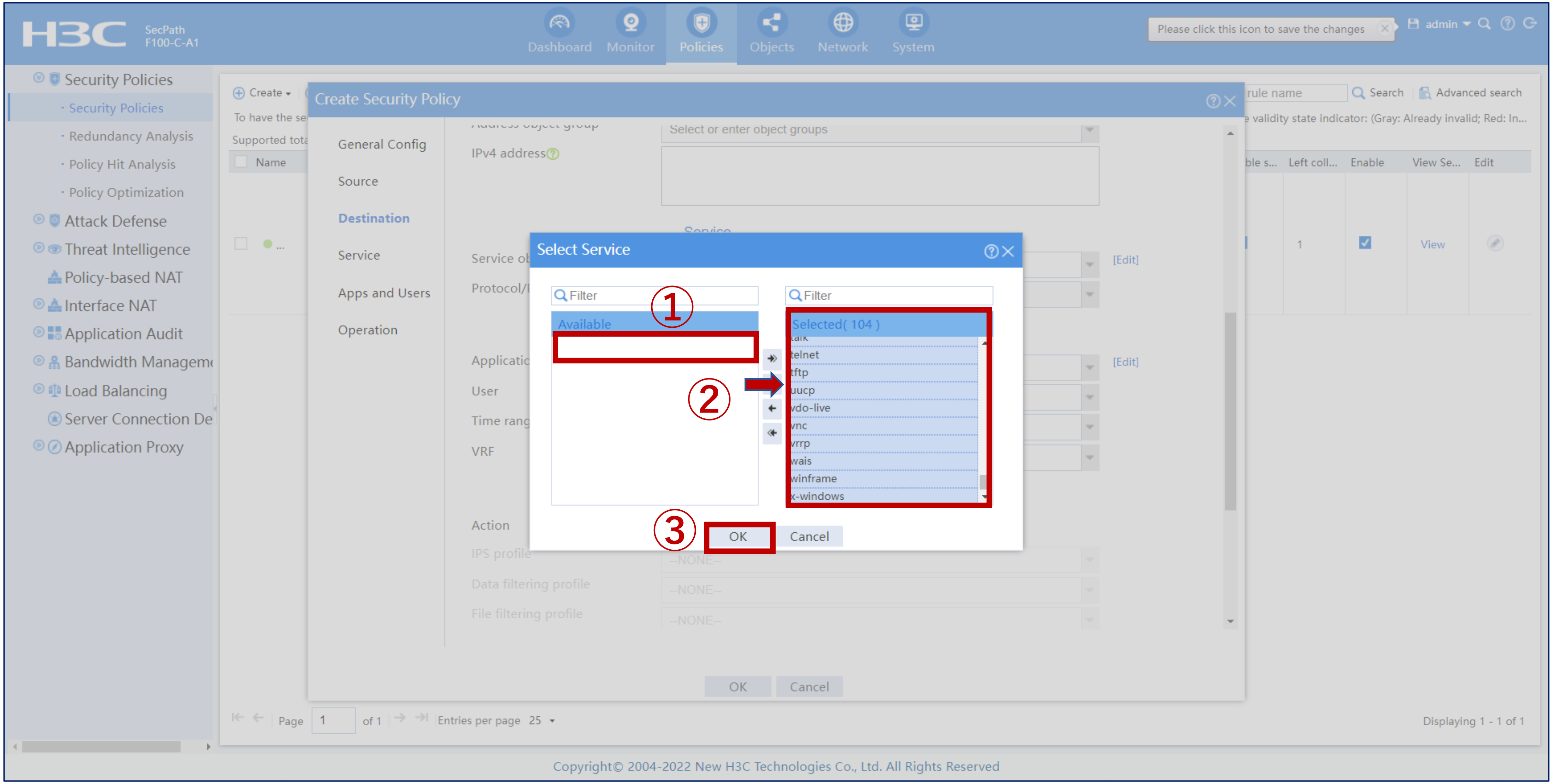
③ Destination zone: Trust [Edit]

Address object group: Select or enter object groups

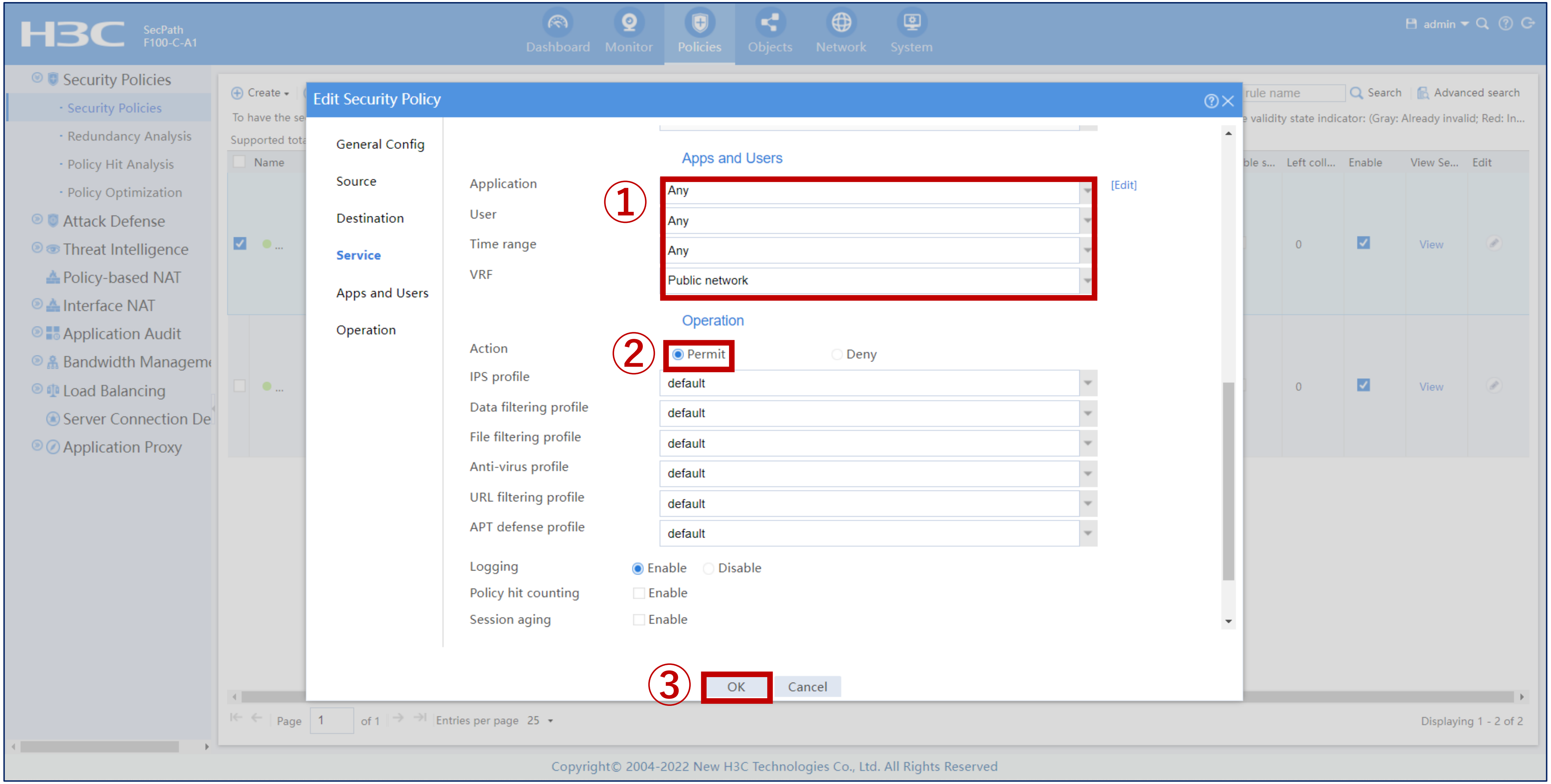
IPv4 address:

④ 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



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



To have the se…

Supported tota…

…validity state indicator: (Gray: Already invalid; Red: In...

Edit Security Policy

Apps and Users

①
Application: Any
User: Any
Time range: Any
VRF: Public network

Operation

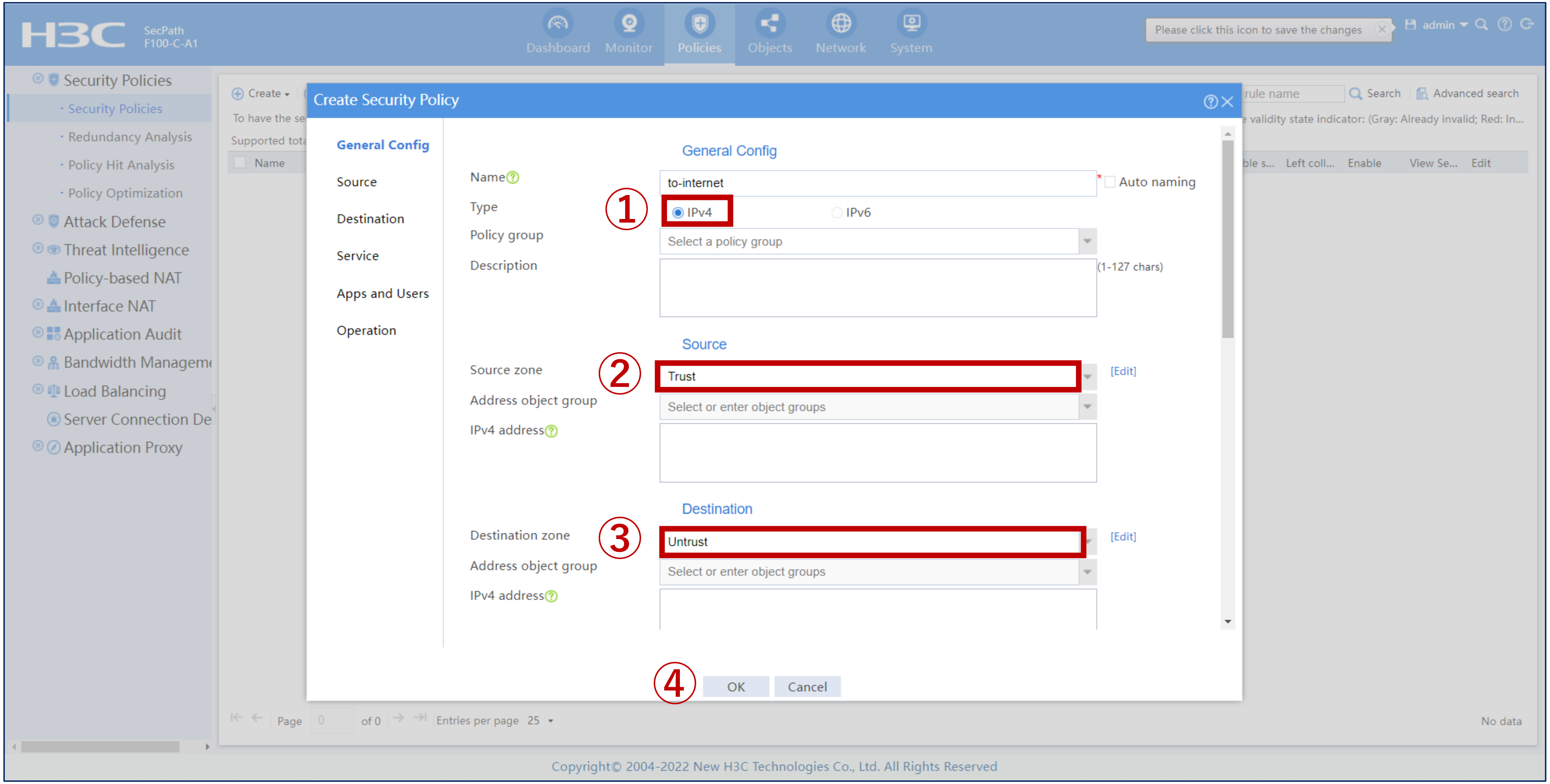
② Action: ● Permit ○ Deny

IPS profile: default
Data filtering profile: default
File filtering profile: default
Anti-virus profile: default
URL filtering profile: default
APT defense profile: default
Logging: ● Enable ○ Disable
Policy hit counting: □ Enable
Session aging: □ Enable

③ OK Cancel

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通過させます



Create Security Policy

General Config

Name: to-internet * □ Auto naming

Type: ① ● IPv4 ○ IPv6

Policy group: Select a policy group

Description: (1-127 chars)

Source

Source zone: ② Trust [Edit]

Address object group: Select or enter object groups

IPv4 address:

Destination

Destination zone: ③ Untrust [Edit]

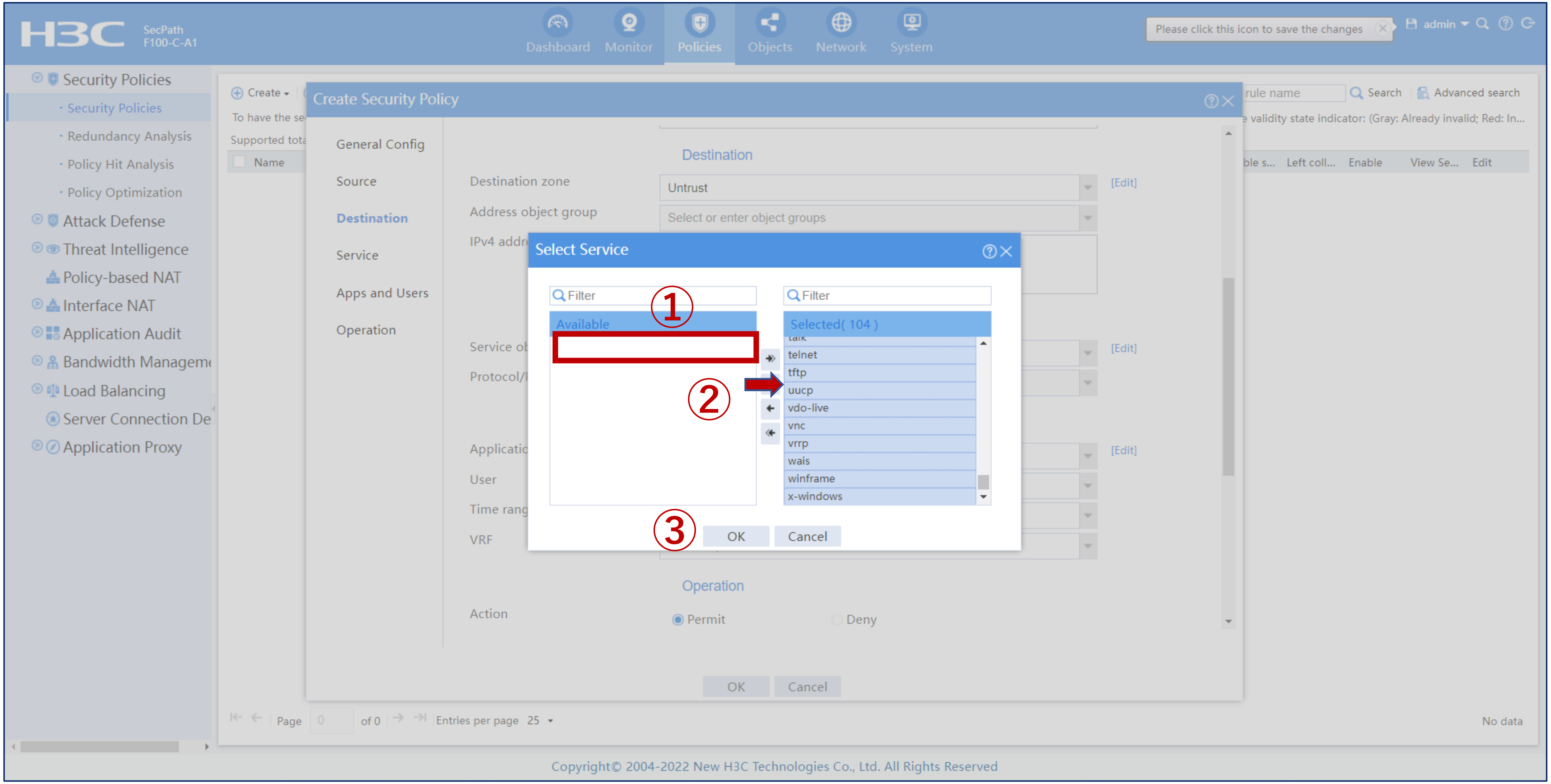
Address object group: Select or enter object groups

IPv4 address:

④ OK Cancel

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通過させます



To have the se

Supported tota

validity state indicator: (Gray: Already invalid; Red: In...

Create Security Policy

Destination

Destination zone: Untrust

Address object group: Select or enter object groups

IPv4 addr

Service ob

Protocol/I

Applicatio

User

Time rang

VRF

Select Service

Selected(104)

- talk
- telnet
- tftp
- uucp
- vdo-live
- vnc
- vrrp
- wais
- winframe
- x-windows

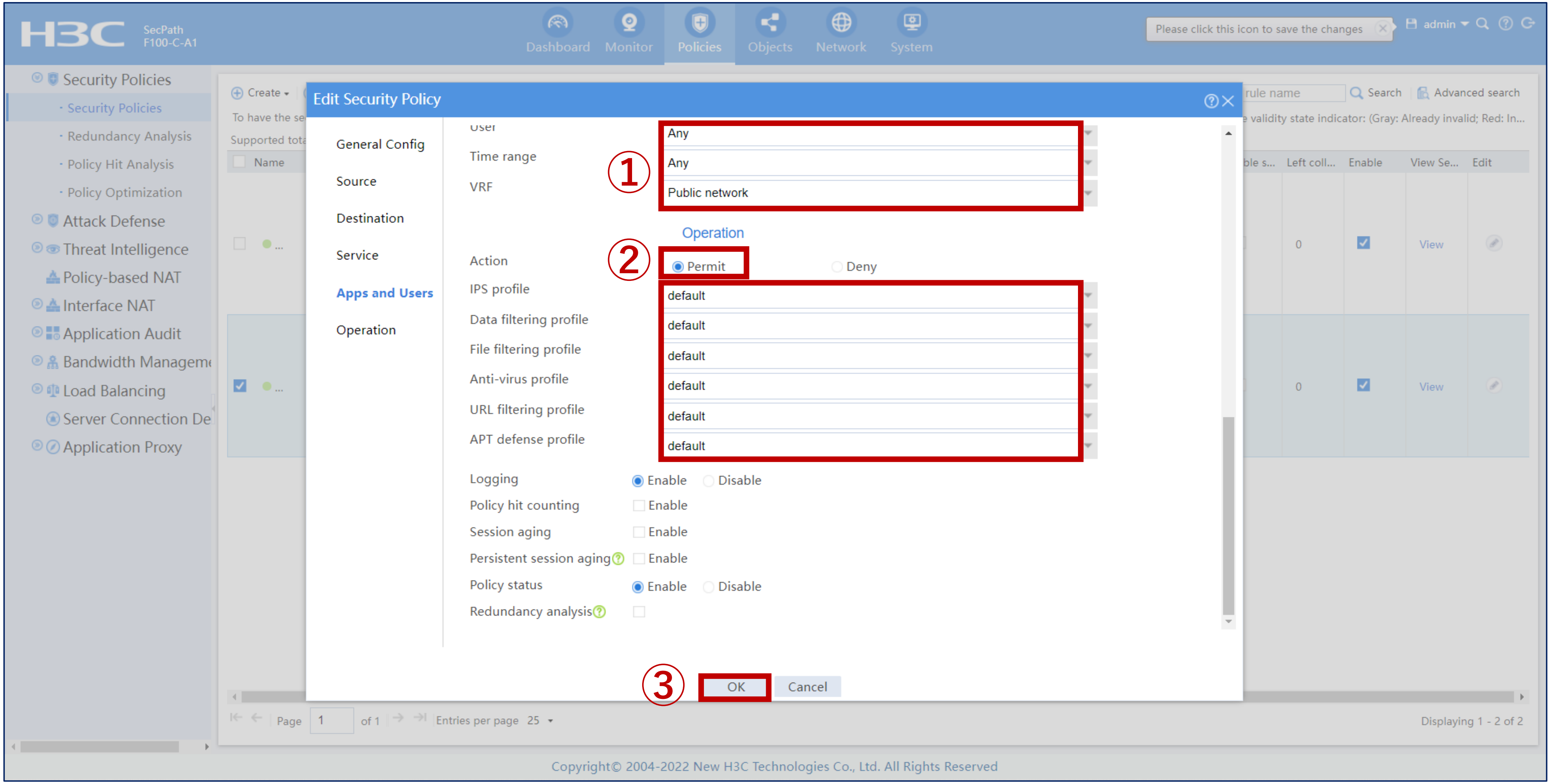
Operation

Action: ● Permit ○ Deny

Page 0 of 0 Entries per page 25

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通過させます



Edit Security Policy

①
User: Any
Time range: Any
VRF: Public network

Operation

② Action: ● Permit ○ Deny

IPS profile: default
Data filtering profile: default
File filtering profile: default
Anti-virus profile: default
URL filtering profile: default
APT defense profile: default

Logging: ● Enable ○ Disable
Policy hit counting: □ Enable
Session aging: □ Enable
Persistent session aging: □ Enable
Policy status: ● Enable ○ Disable
Redundancy analysis: □

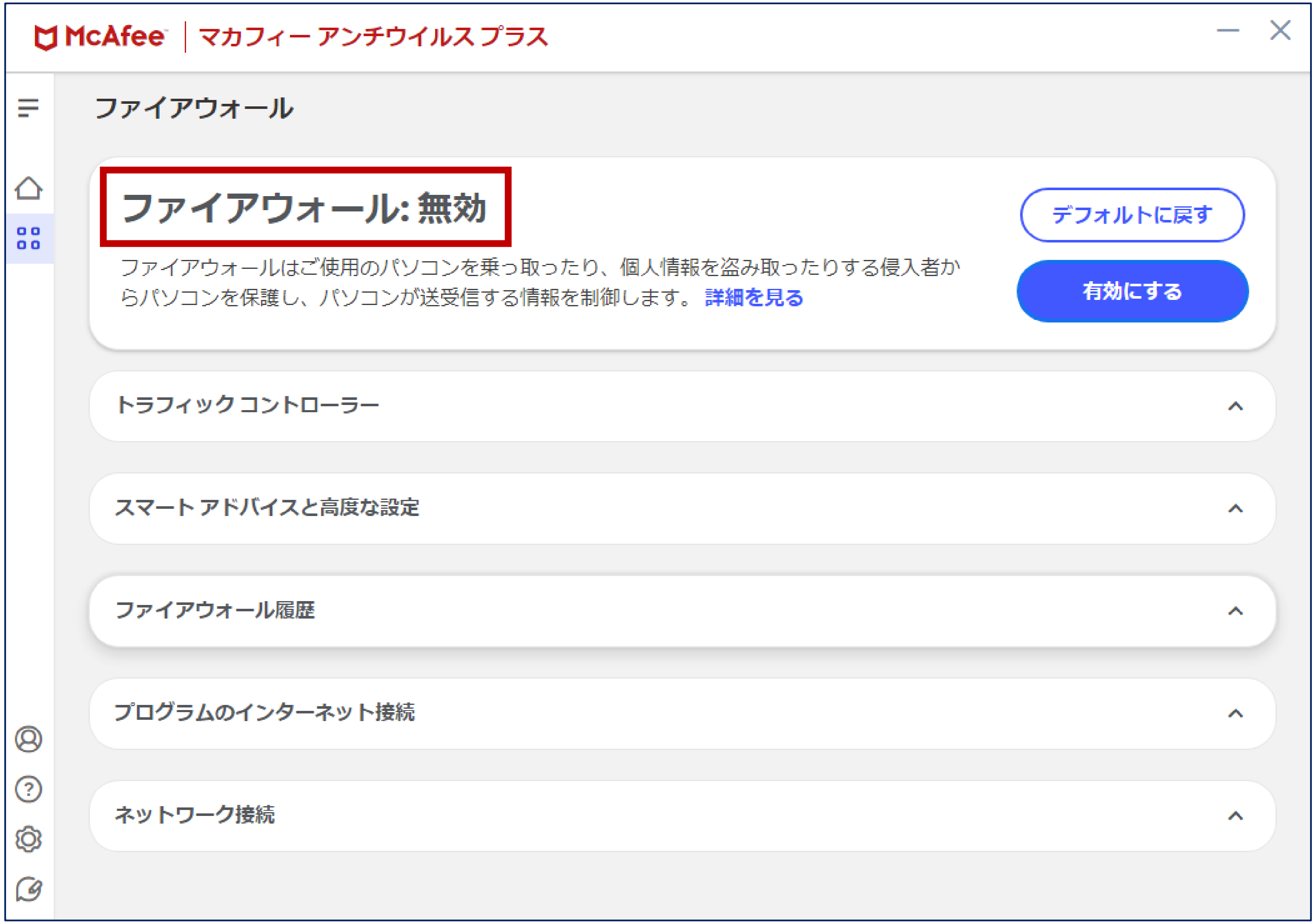
③ OK Cancel

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



McAfee | マカフィー アンチウイルス プラス

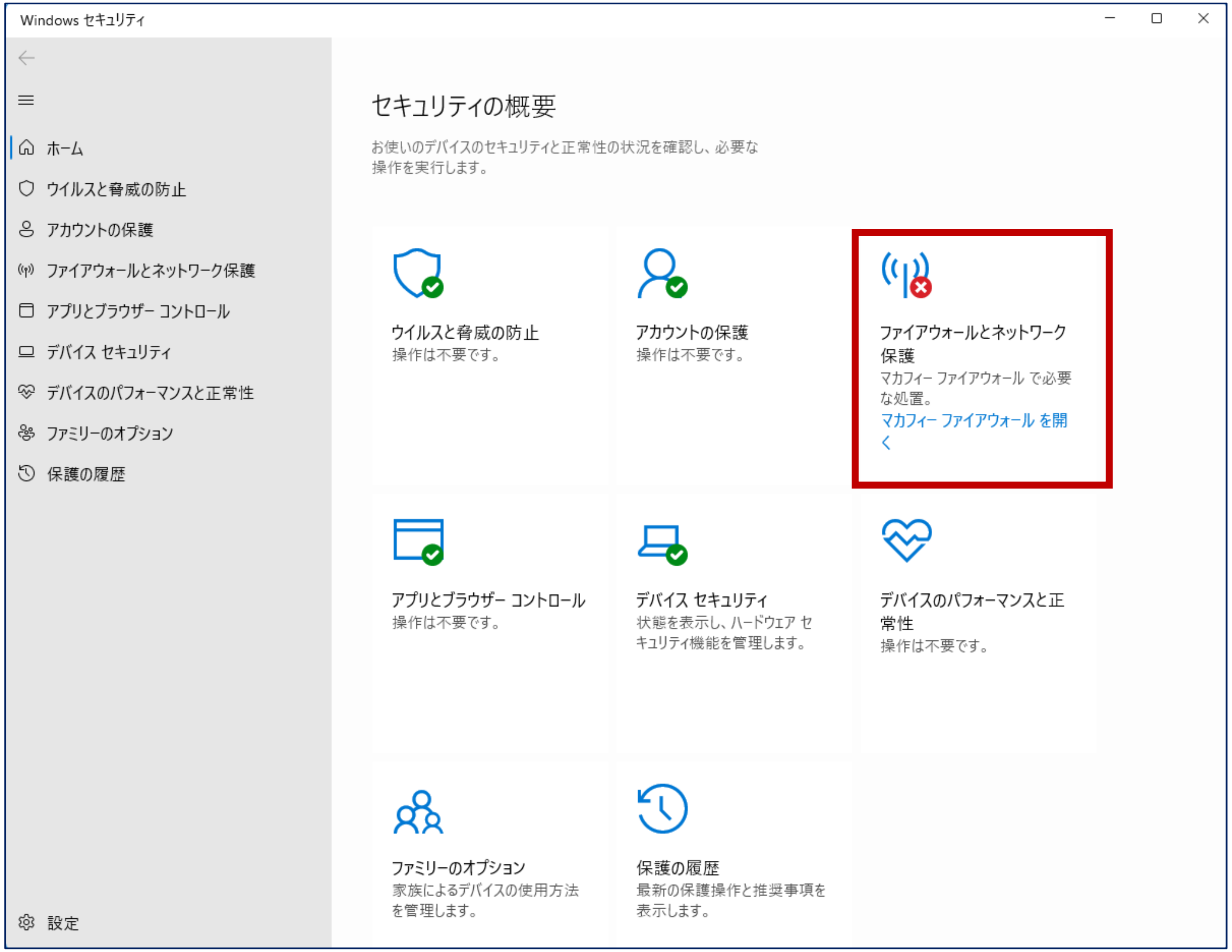
ファイアウォール

ファイアウォール: 無効

ファイアウォールはご使用のパソコンを乗っ取ったり、個人情報を盗み取ったりする侵入者からパソコンを保護し、パソコンが送受信する情報を制御します。 詳細を見る

デフォルトに戻す
有効にする
トラフィック コントローラー
スマート アドバイスと高度な設定
ファイアウォール履歴
プログラムのインターネット接続
ネットワーク接続

テストする際にWindowsファイアウォールを無効にする



Windows セキュリティ

セキュリティの概要

お使いのデバイスのセキュリティと正常性の状況を確認し、必要な操作を実行します。

ウイルスと脅威の防止
操作は不要です。

アカウントの保護
操作は不要です。

ファイアウォールとネットワーク保護
マカフィー ファイアウォール で必要な処置。
マカフィー ファイアウォール を開く

アプリとブラウザー コントロール
操作は不要です。

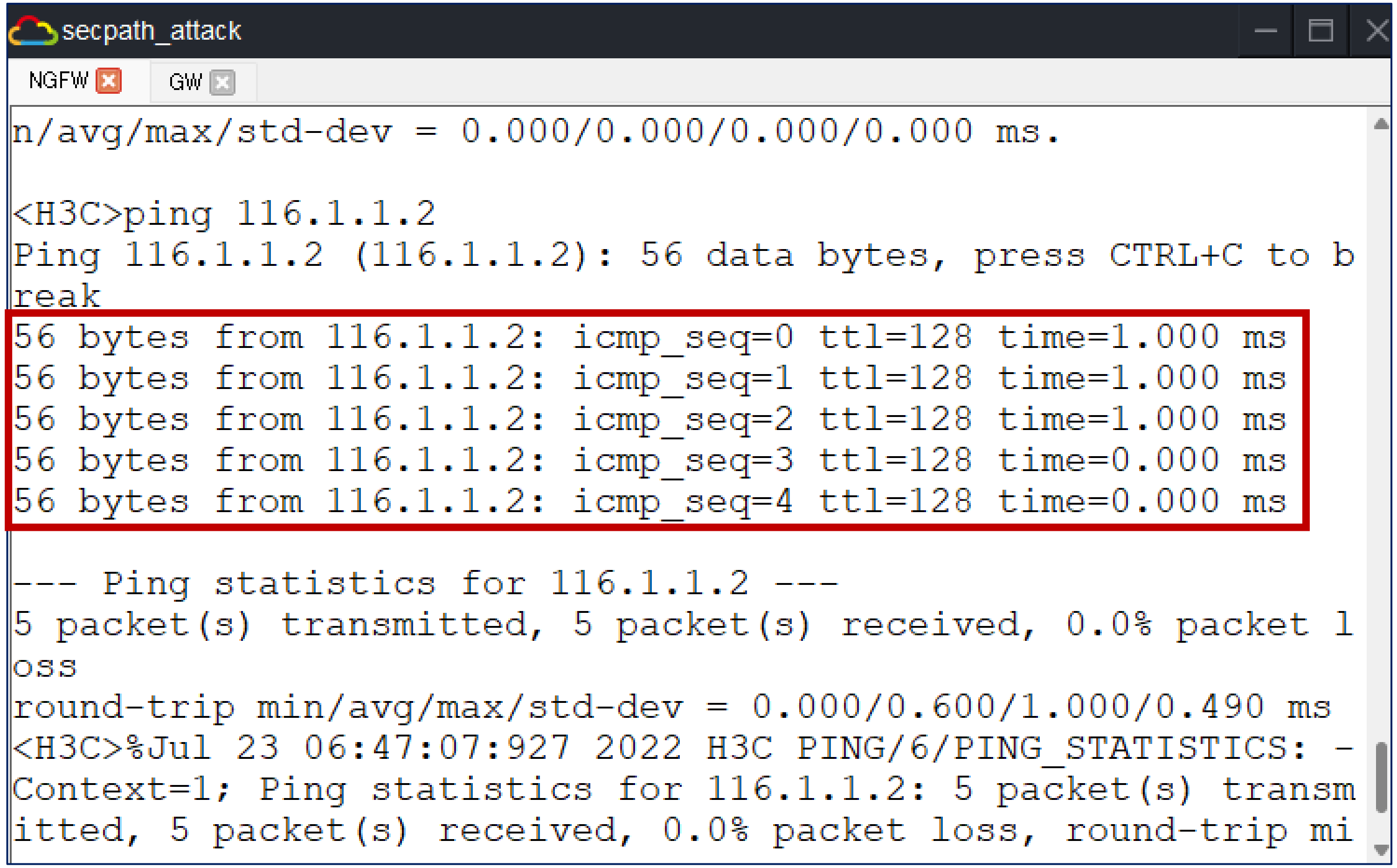
デバイス セキュリティ
状態を表示し、ハードウエア セキュリティ機能を管理します。

デバイスのパフォーマンスと正常性
操作は不要です。

ファミリーのオプション
家族によるデバイスの使用方法を管理します。

保護の履歴
最新の保護操作と推奨事項を表示します。

SecPathからhostへの疎通OK

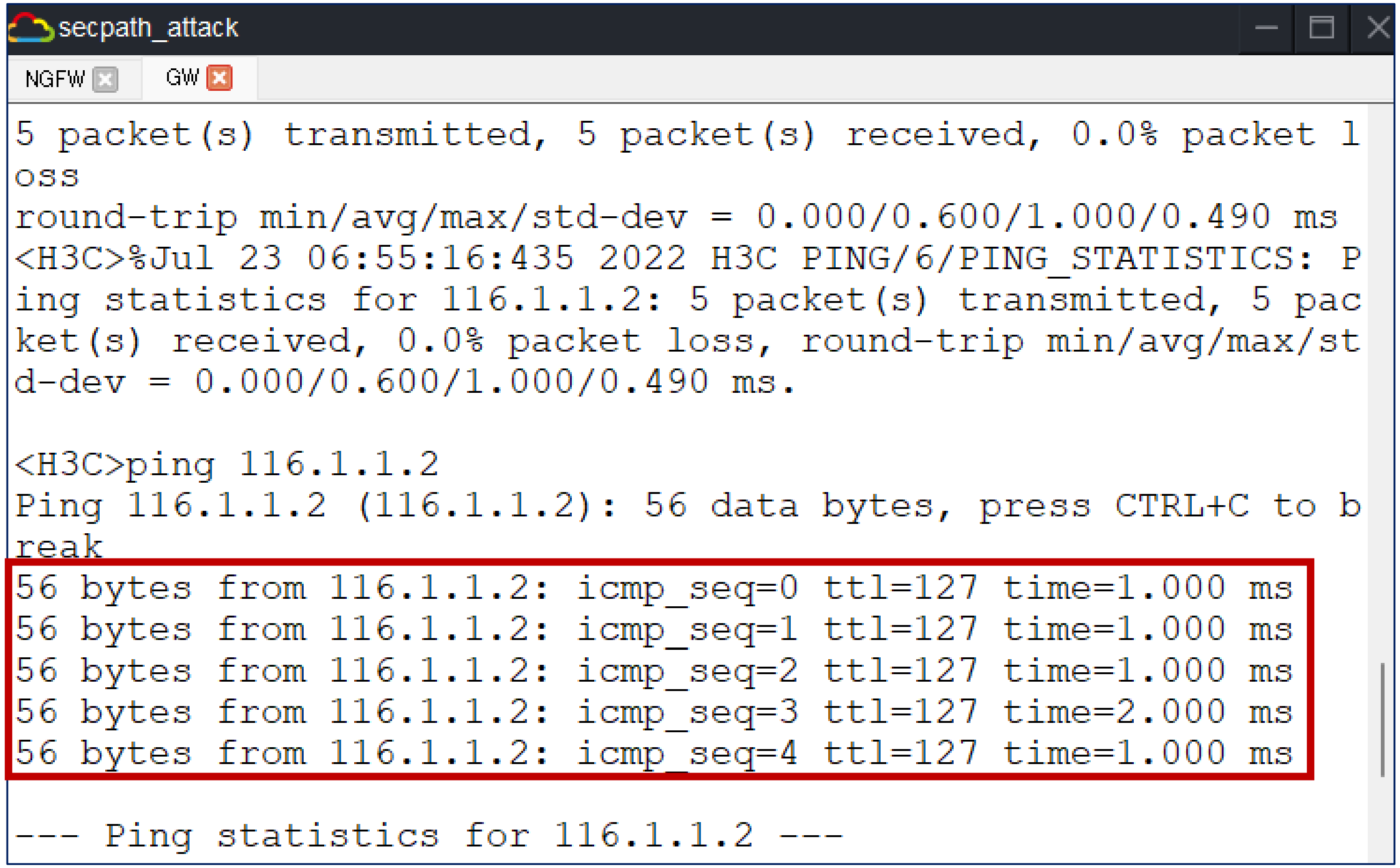


```
n/avg/max/std-dev = 0.000/0.000/0.000/0.000 ms.

<H3C>ping 116.1.1.2
Ping 116.1.1.2 (116.1.1.2): 56 data bytes, press CTRL+C to b
reak
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 l
oss
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) transm
itted, 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



```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet l
oss
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: P
ing statistics for 116.1.1.2: 5 packet(s) transmitted, 5 pac
ket(s) received, 0.0% packet loss, round-trip min/avg/max/st
d-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 b
reak
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

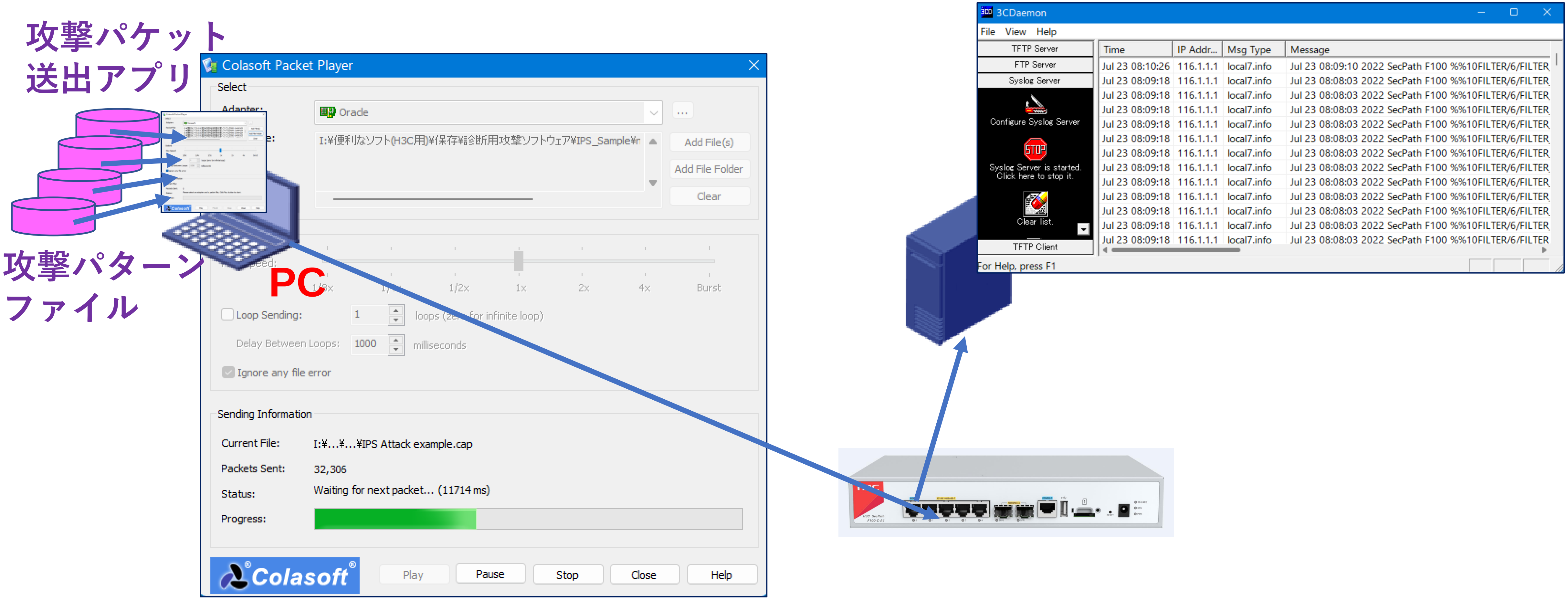
05 各種ログの環境整備

06 攻撃検証環境の整備

07 検証結果

08 トラブルシュート

攻撃開始



攻撃パケット
送出アプリ

攻撃パターン
ファイル

PC

Colasoft Packet Player

Select

Adapter: Oracle

File: I:¥便利なソフト(H3C用)¥保存¥診断用攻撃ソフトウェア¥IPS_Sample¥r

□ Loop Sending: 1 loops (zero for infinite loop)

Delay Between Loops: 1000 milliseconds

☑ Ignore any file error

Sending Information

Current File: I:¥...¥...¥IPS Attack example.cap

Packets Sent: 32,306

Status: Waiting for next packet... (11714 ms)

Progress:

3CDaemon

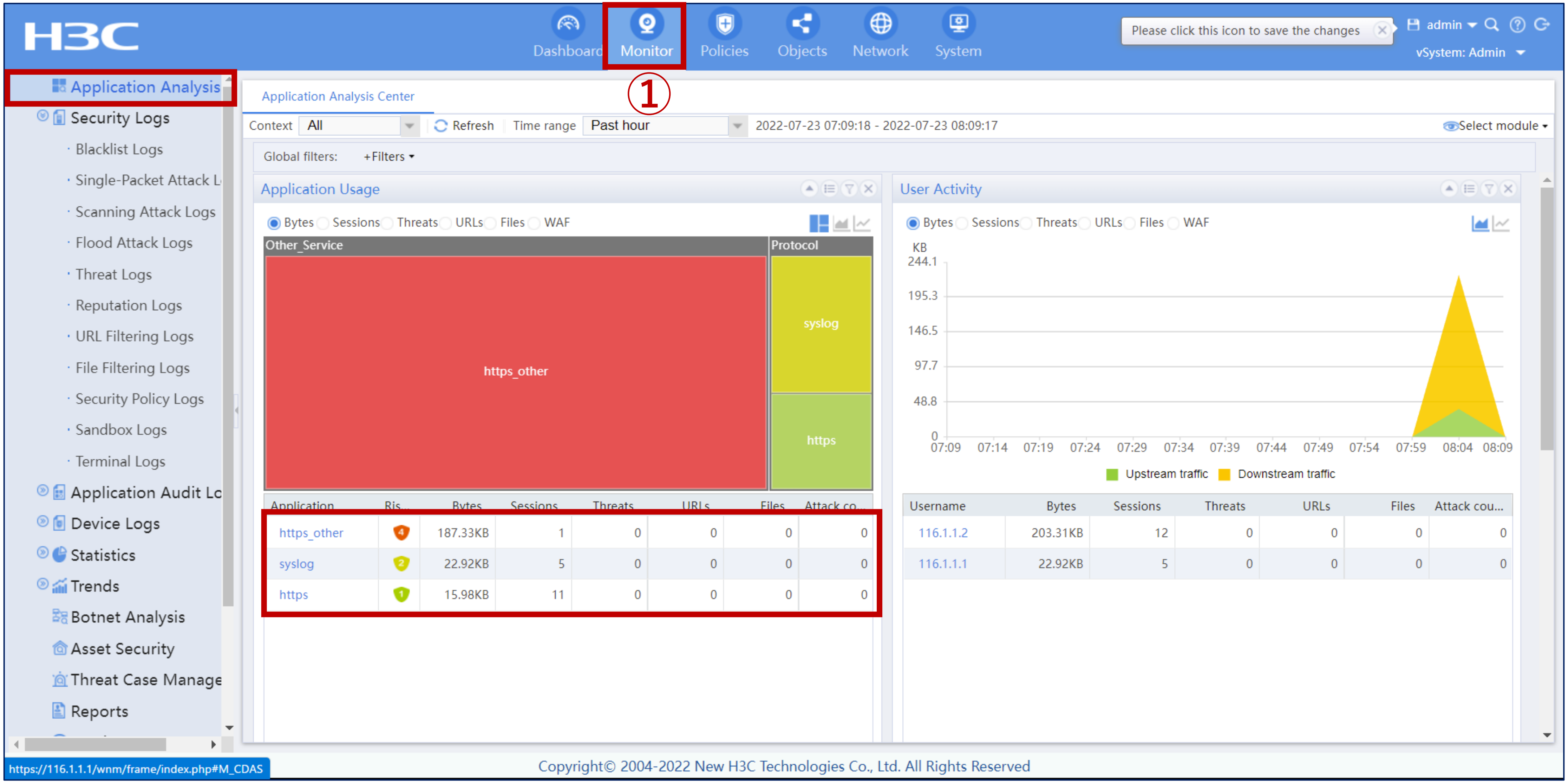
Syslog Server is started.
Click here to stop it.

Time	IP Addr...	Msg Type	Message
Jul 23 08:10:26	116.1.1.1	local7.info	Jul 23 08:09:10 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER
Jul 23 08:09:18	116.1.1.1	local7.info	Jul 23 08:08:03 2022 SecPath F100 %%10FILTER/6/FILTER

For Help, press F1

Application Usageログ

②



①

Context: All

Time range: Past hour 2022-07-23 07:09:18 - 2022-07-23 08:09:17

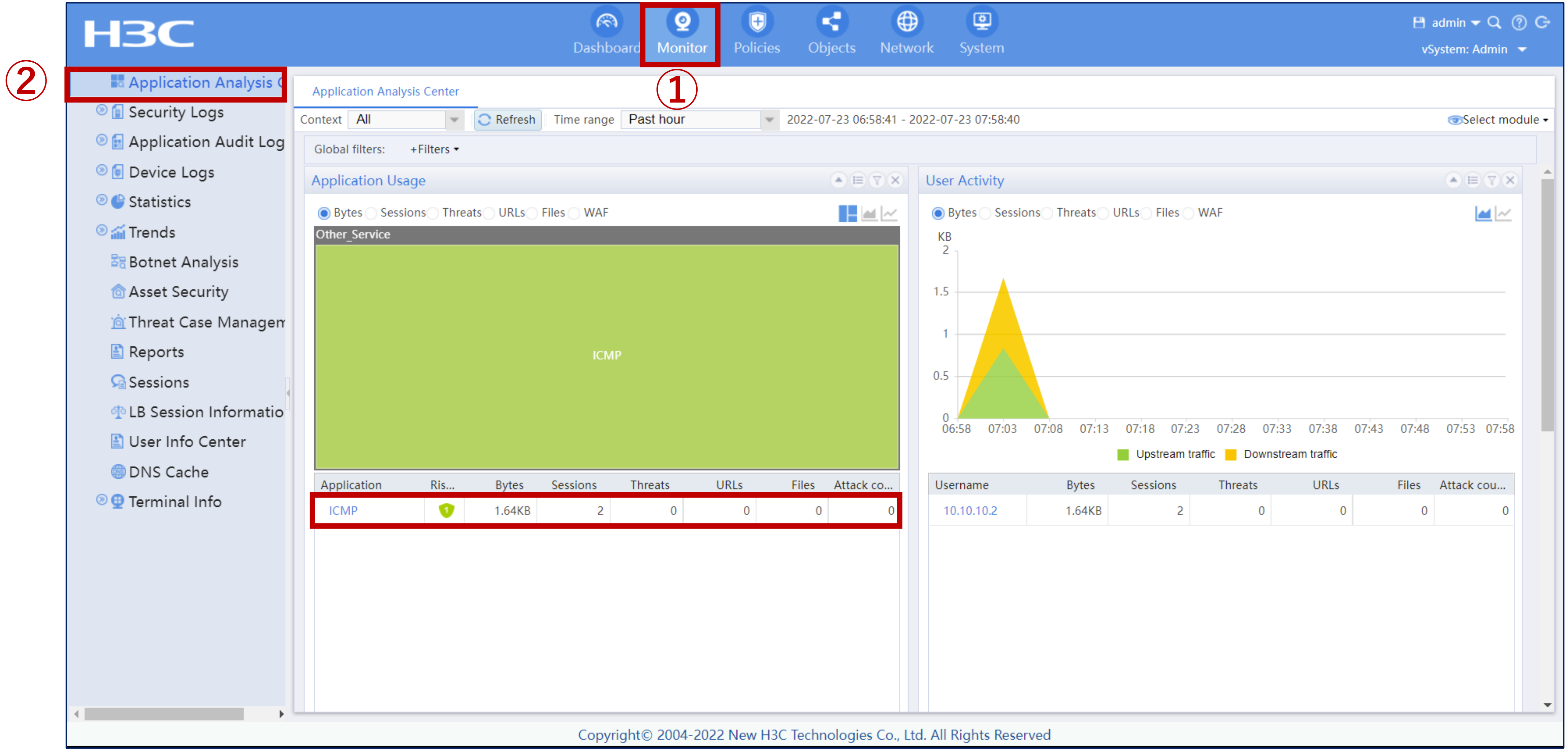
Application	Ris...	Bytes	Sessions	Threats	URLs	Files	Attack co...
https_other	4	187.33KB	1	0	0	0	0
syslog	2	22.92KB	5	0	0	0	0
https	1	15.98KB	11	0	0	0	0

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



Context: All

Time range: Past hour

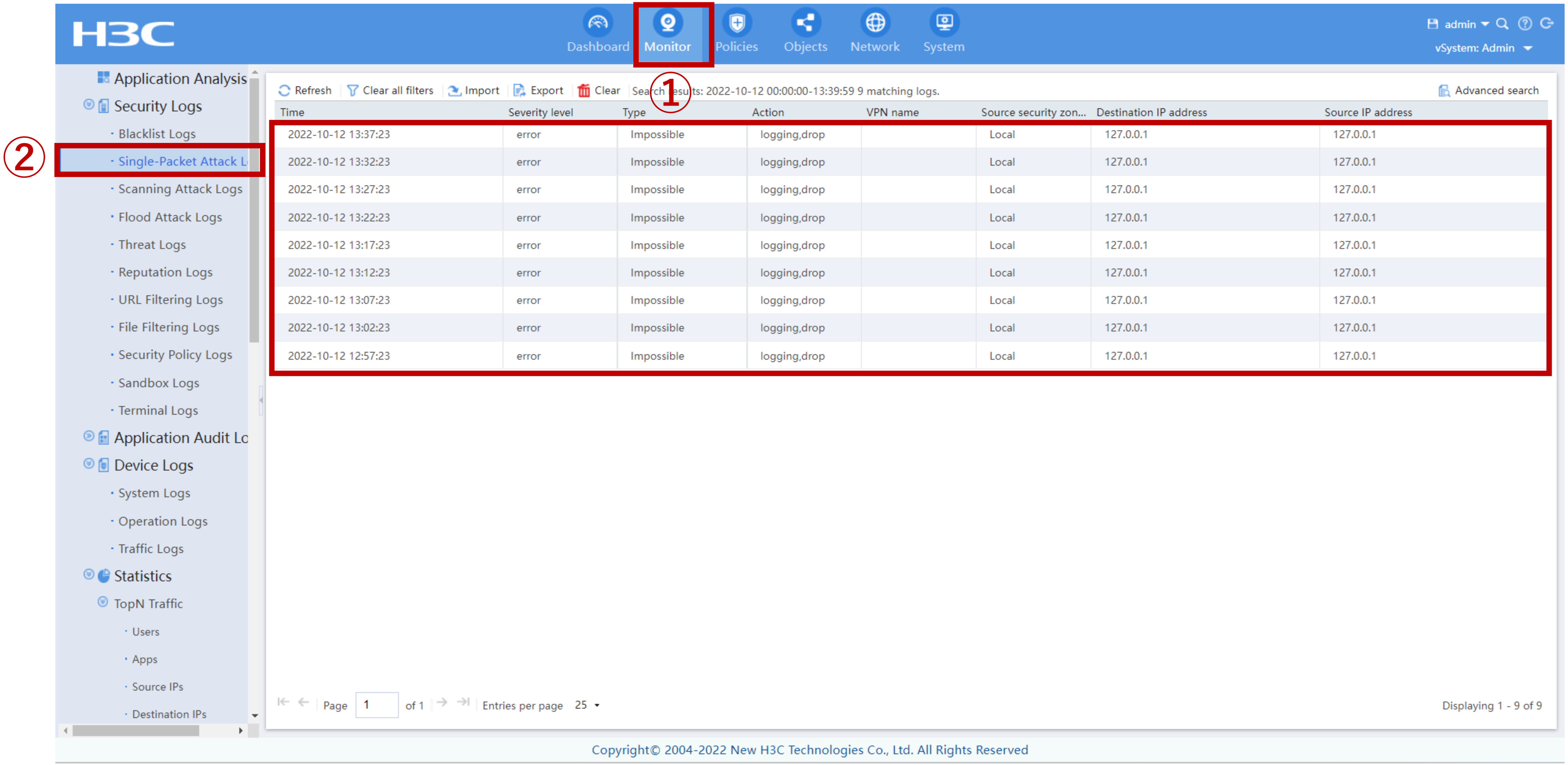
2022-07-23 06:58:41 - 2022-07-23 07:58:40

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

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



Search results: 2022-10-12 00:00:00-13:39:59 9 matching logs.

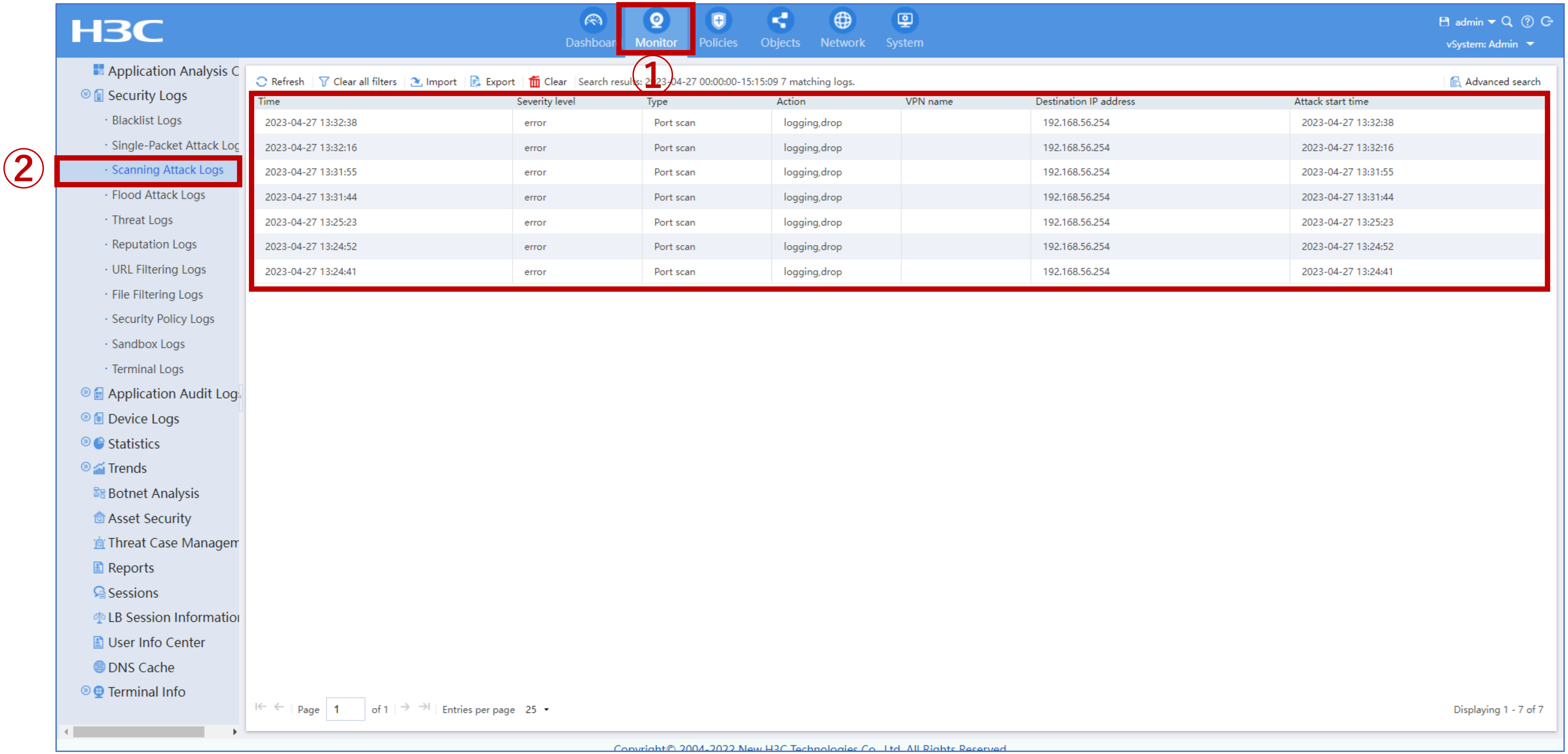
Time	Severity level	Type	Action	VPN name	Source security zon...	Destination IP address	Source IP address
2022-10-12 13:37:23	error	Impossible	logging,drop		Local	127.0.0.1	127.0.0.1
2022-10-12 13:32:23	error	Impossible	logging,drop		Local	127.0.0.1	127.0.0.1
2022-10-12 13:27:23	error	Impossible	logging,drop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



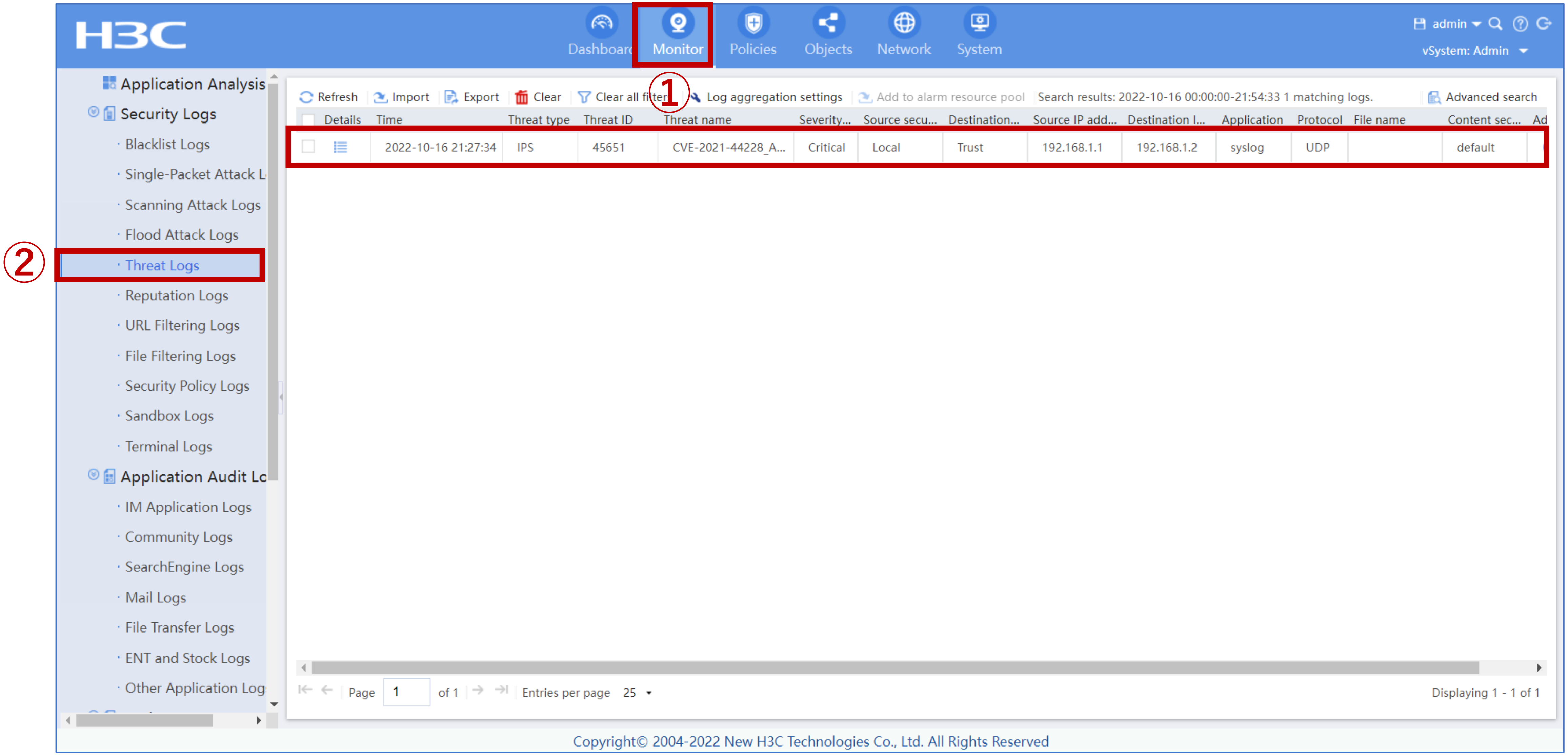
Search results: 2023-04-27 00:00:00-15:15:09 7 matching logs.

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

Displaying 1 - 7 of 7

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

IPS攻撃ログ

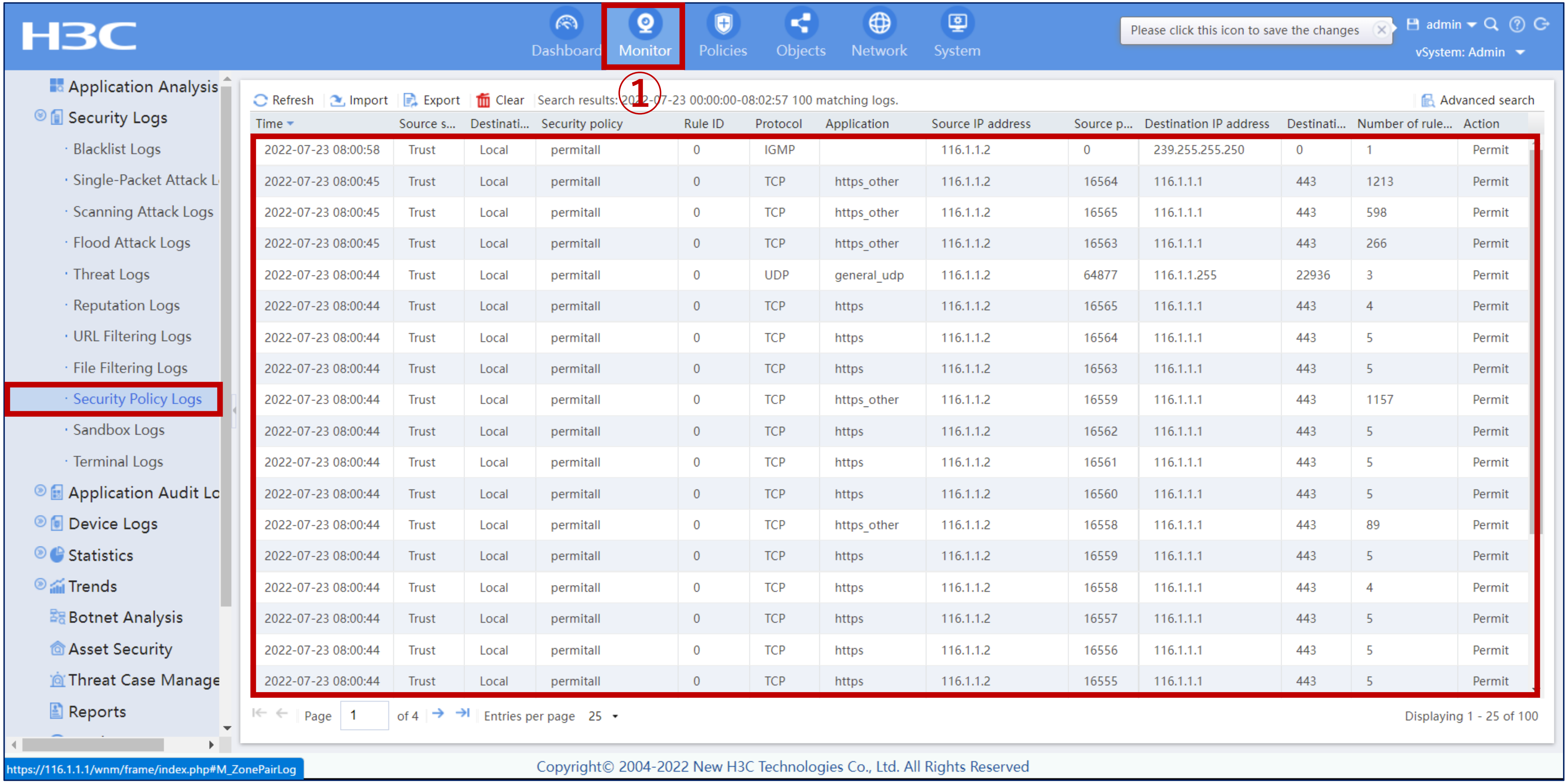


Search results: 2022-10-16 00:00:00-21:54:33 1 matching logs.

□	Details	Time	Threat type	Threat ID	Threat name	Severity...	Source secu...	Destination...	Source IP add...	Destination I...	Application	Protocol	File name	Content sec...	Ad
□	☰	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	

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

Security policy攻撃ログ



Search results: 2022-07-23 00:00:00-08:02:57 100 matching logs.

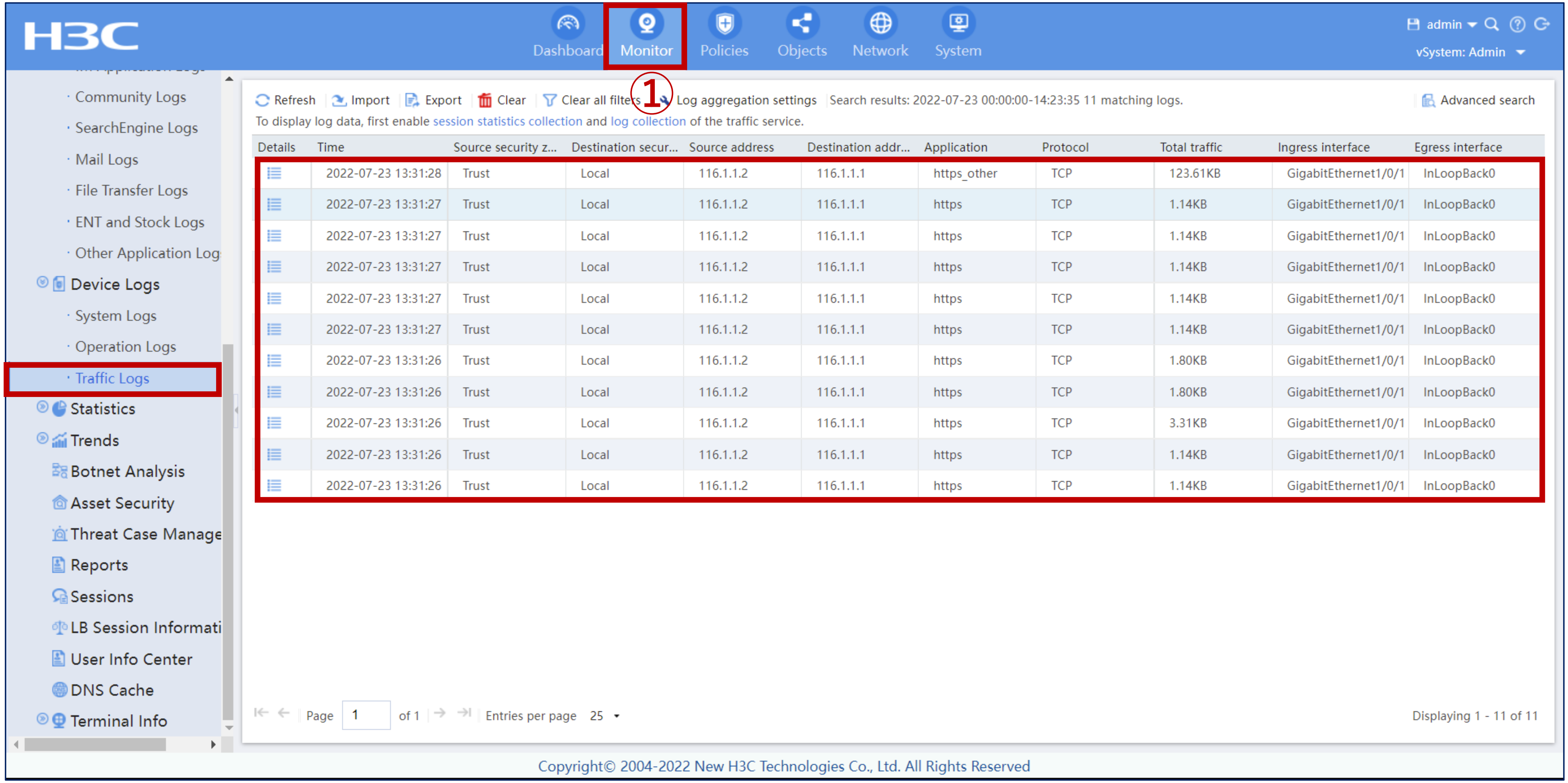
Time	Source s...	Destinati...	Security policy	Rule ID	Protocol	Application	Source IP address	Source p...	Destination IP address	Destinati...	Number of rule...	Action
2022-07-23 08:00:58	Trust	Local	permitall	0	IGMP		116.1.1.2	0	239.255.255.250	0	1	Permit
2022-07-23 08:00:45	Trust	Local	permitall	0	TCP	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



Search results: 2022-07-23 00:00:00-14:23:35 11 matching logs.

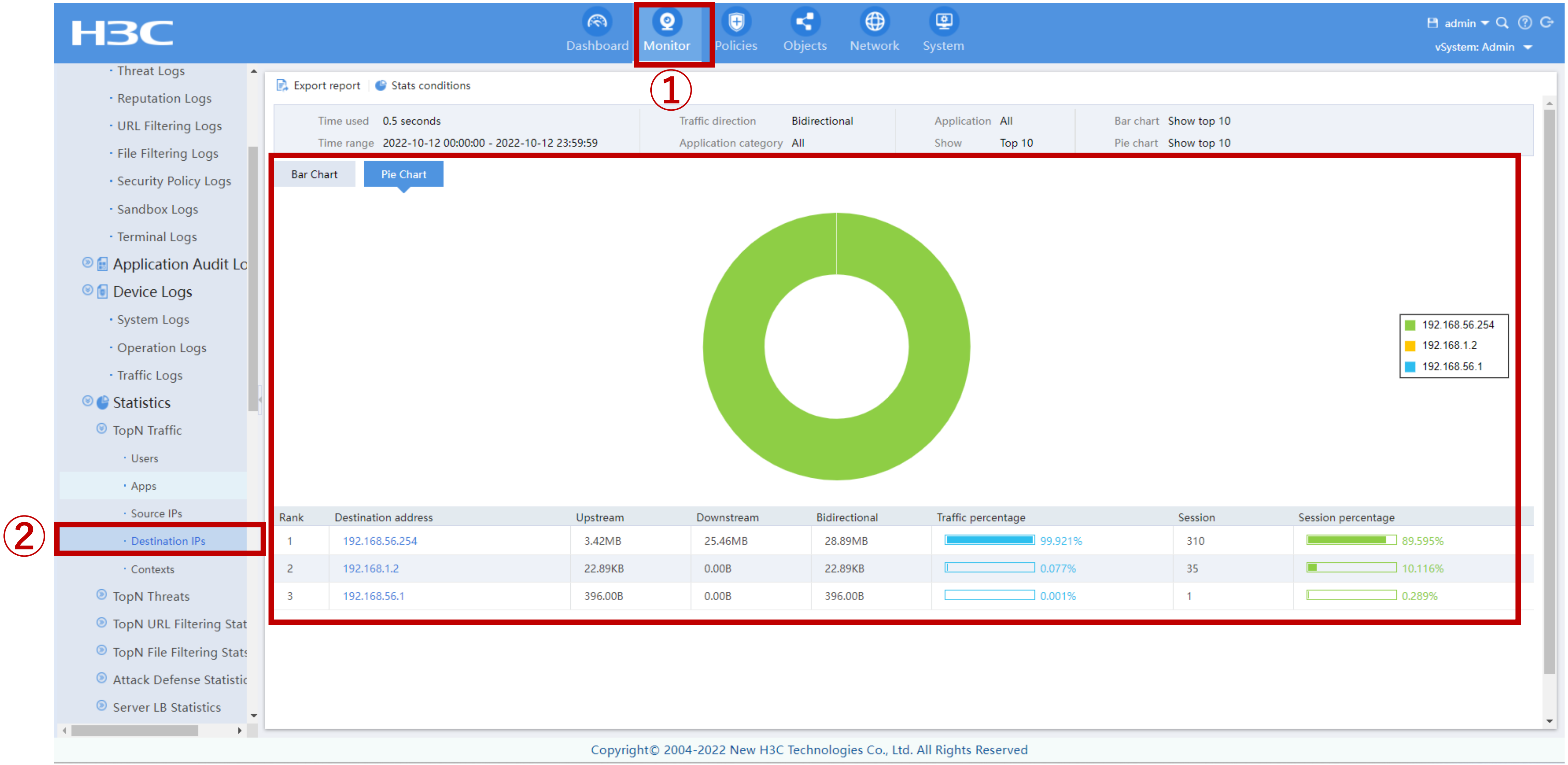
To display log data, first enable session statistics collection and log collection of the traffic service.

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

Displaying 1 - 11 of 11

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

Destination IPログ

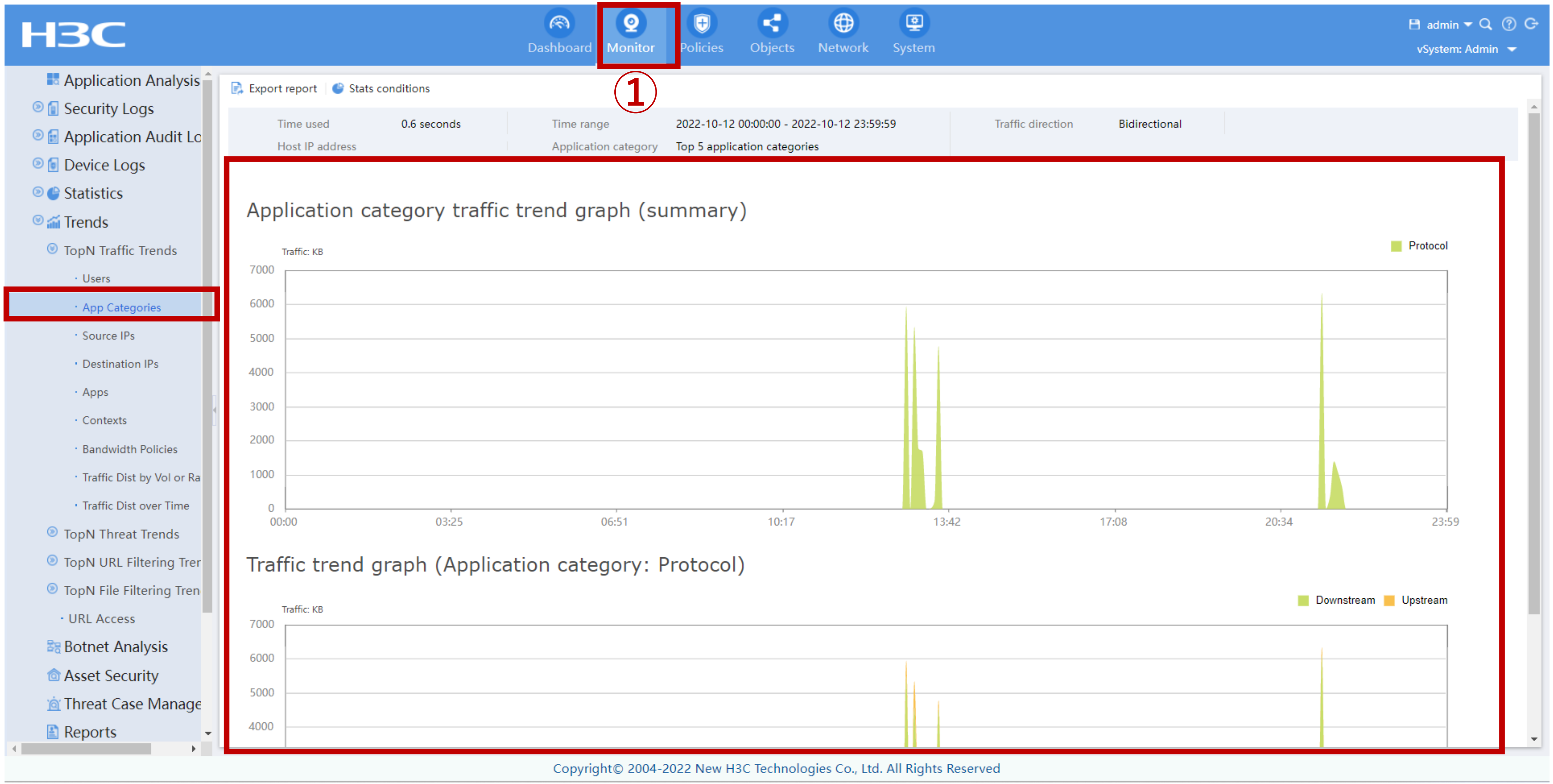


Time used 0.5 seconds
Time range 2022-10-12 00:00:00 - 2022-10-12 23:59:59
Traffic direction Bidirectional
Application category All
Application All
Show Top 10
Bar chart Show top 10
Pie chart Show top 10

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%

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

攻撃Application categoryログ



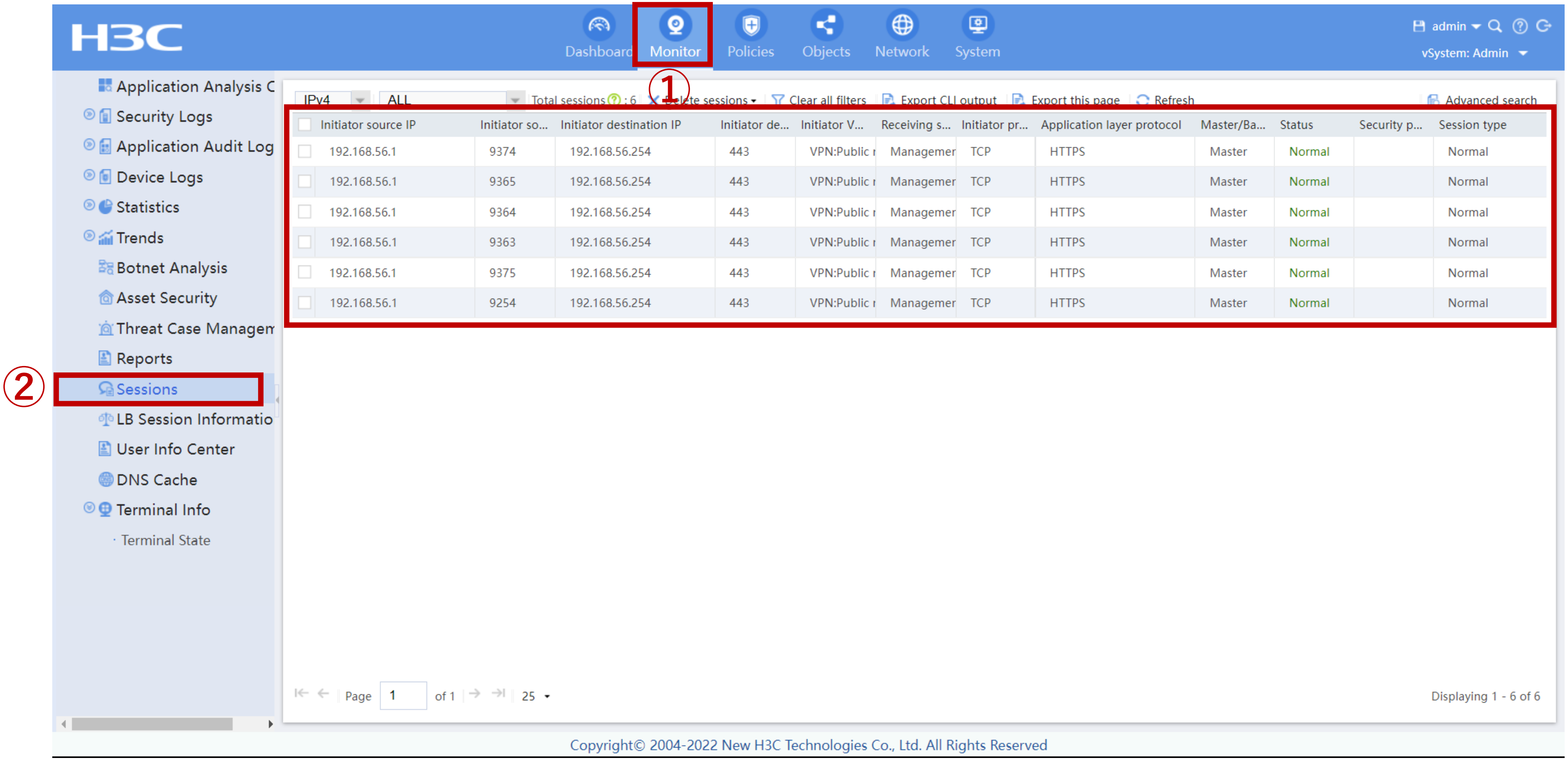
Time used: 0.6 seconds
Time range: 2022-10-12 00:00:00 - 2022-10-12 23:59:59
Traffic direction: Bidirectional
Host IP address:
Application category: Top 5 application categories

Application category traffic trend graph (summary)

Traffic trend graph (Application category: Protocol)

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

Sessionsログ

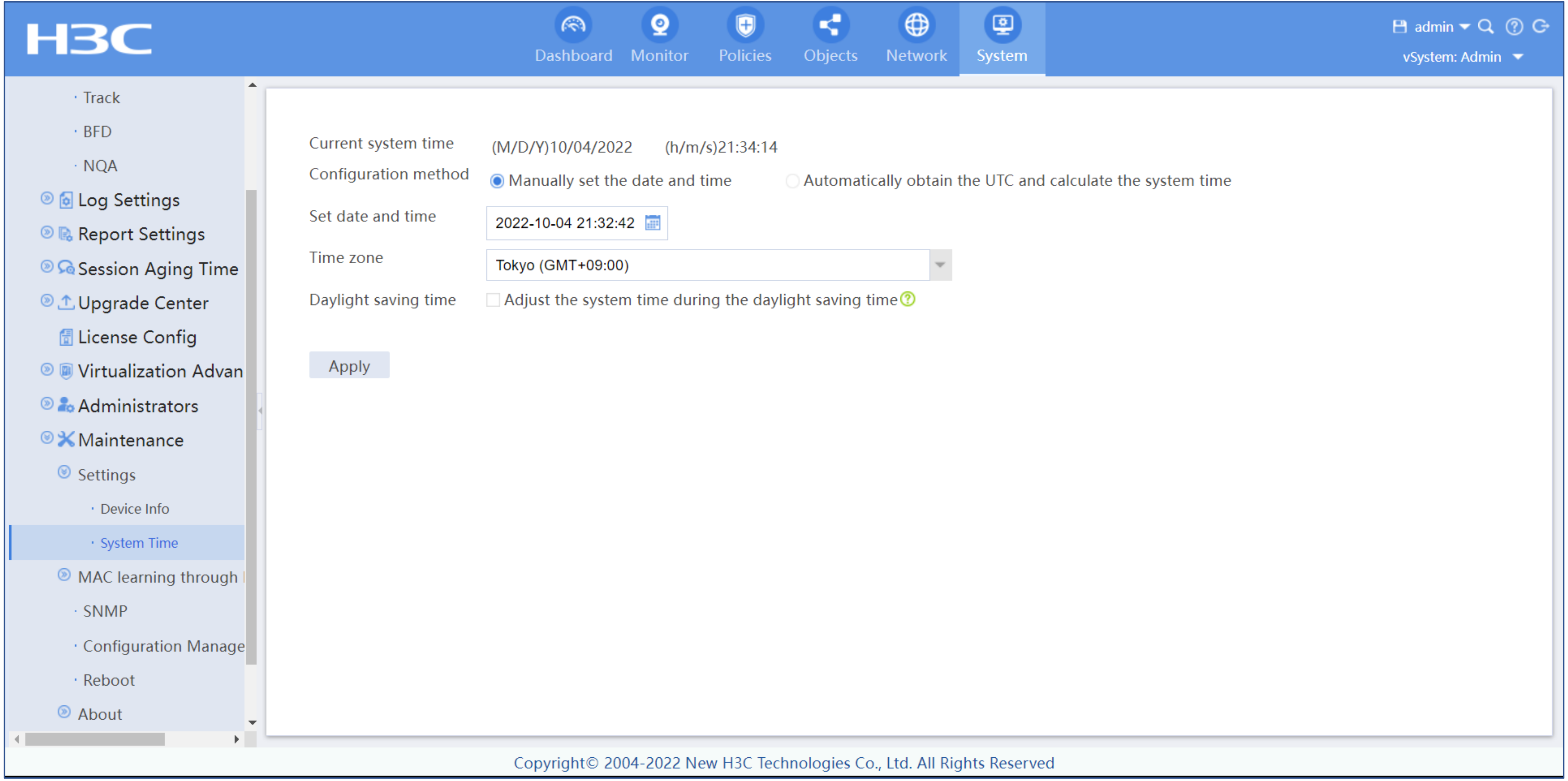


□	Initiator source IP	Initiator so...	Initiator destination IP	Initiator de...	Initiator V...	Receiving s...	Initiator pr...	Application layer protocol	Master/Ba...	Status	Security p...	Session type
□	192.168.56.1	9374	192.168.56.254	443	VPN:Public	Managemer	TCP	HTTPS	Master	Normal		Normal
□	192.168.56.1	9365	192.168.56.254	443	VPN:Public	Managemer	TCP	HTTPS	Master	Normal		Normal
□	192.168.56.1	9364	192.168.56.254	443	VPN:Public	Managemer	TCP	HTTPS	Master	Normal		Normal
□	192.168.56.1	9363	192.168.56.254	443	VPN:Public	Managemer	TCP	HTTPS	Master	Normal		Normal
□	192.168.56.1	9375	192.168.56.254	443	VPN:Public	Managemer	TCP	HTTPS	Master	Normal		Normal
□	192.168.56.1	9254	192.168.56.254	443	VPN:Public	Managemer	TCP	HTTPS	Master	Normal		Normal

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。



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)

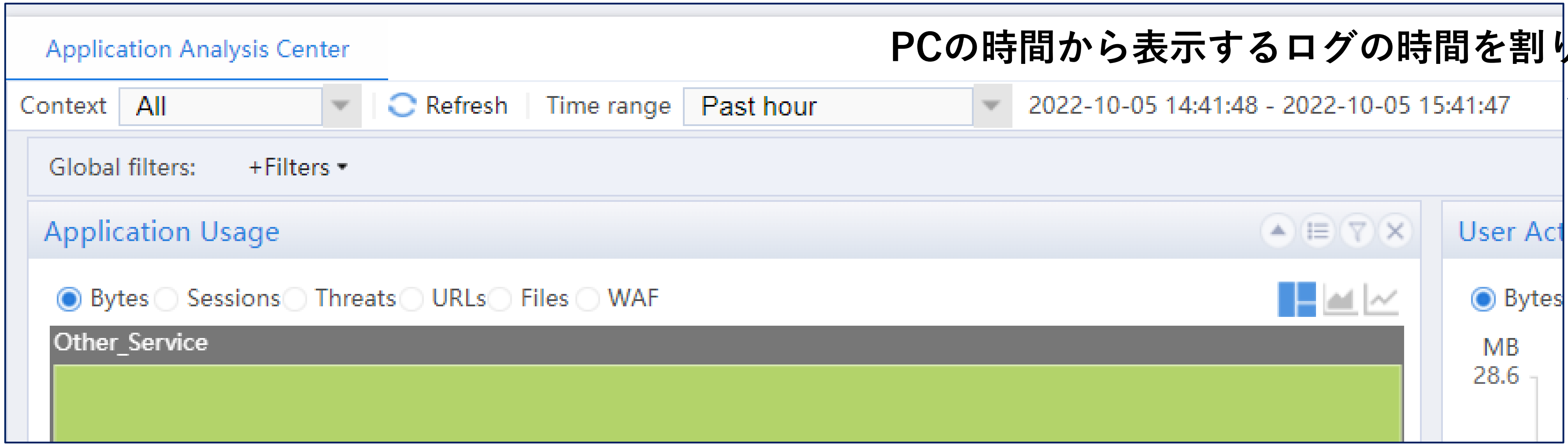
Daylight saving time □ Adjust the system time during the daylight saving time

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。

PCの時間から表示するログの時間を割り出す



Application Analysis Center

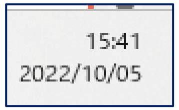
Context: All | Refresh | Time range: Past hour | 2022-10-05 14:41:48 - 2022-10-05 15:41:47

Global filters: +Filters

Application Usage

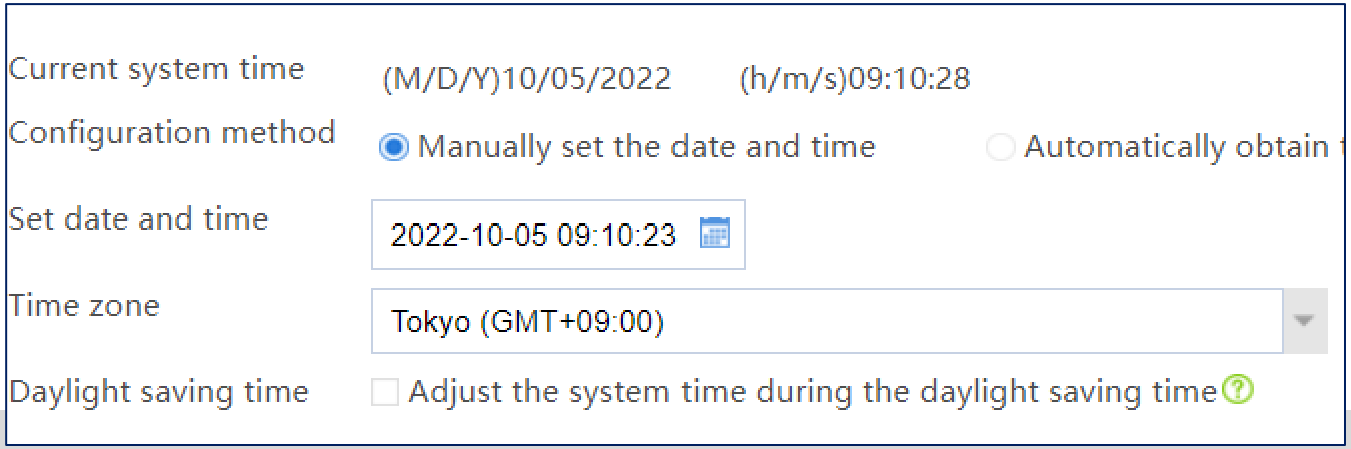
● Bytes ○ Sessions ○ Threats ○ URLs ○ Files ○ WAF

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 t

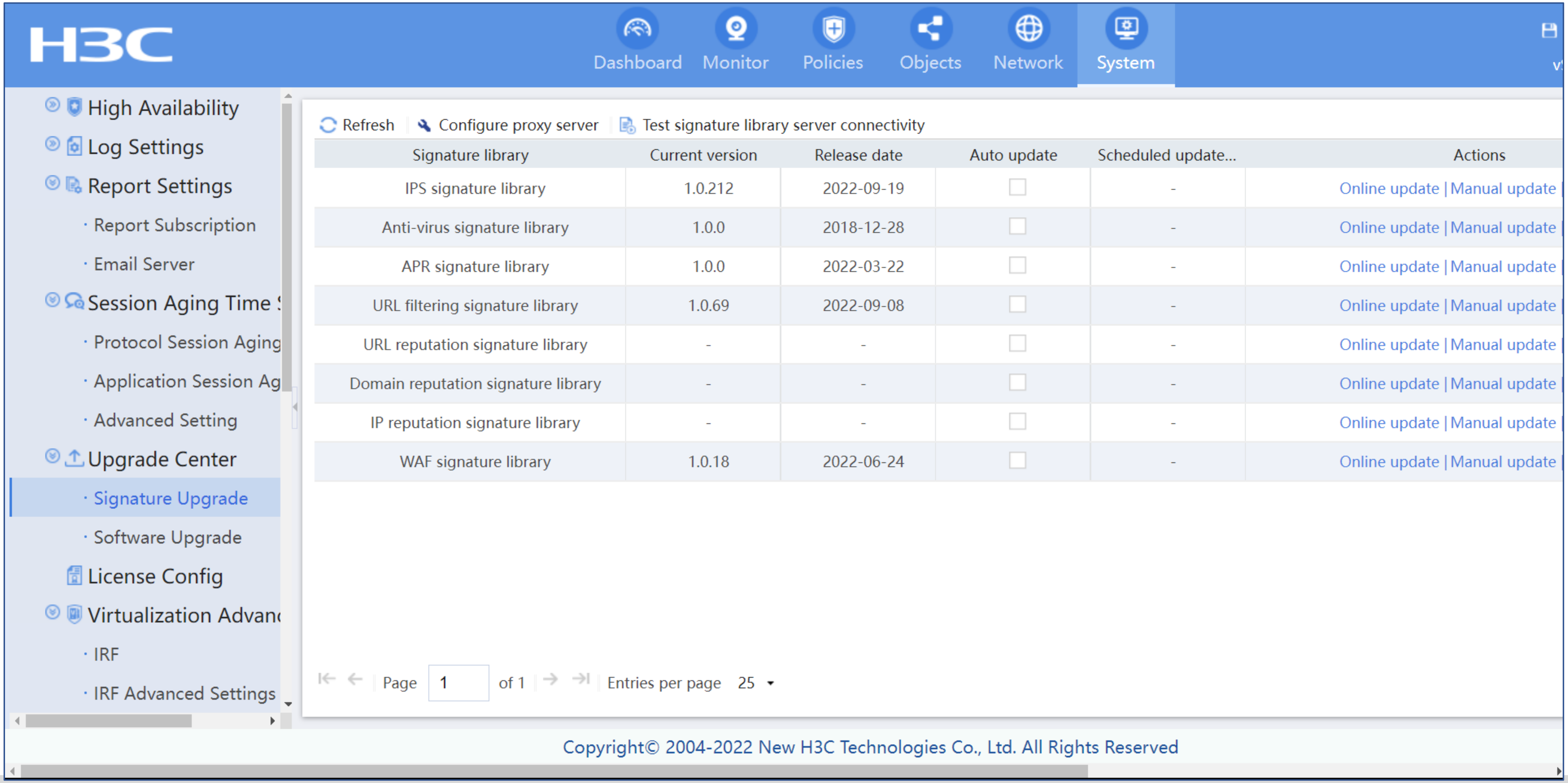
Set date and time: 2022-10-05 09:10:23

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。



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

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

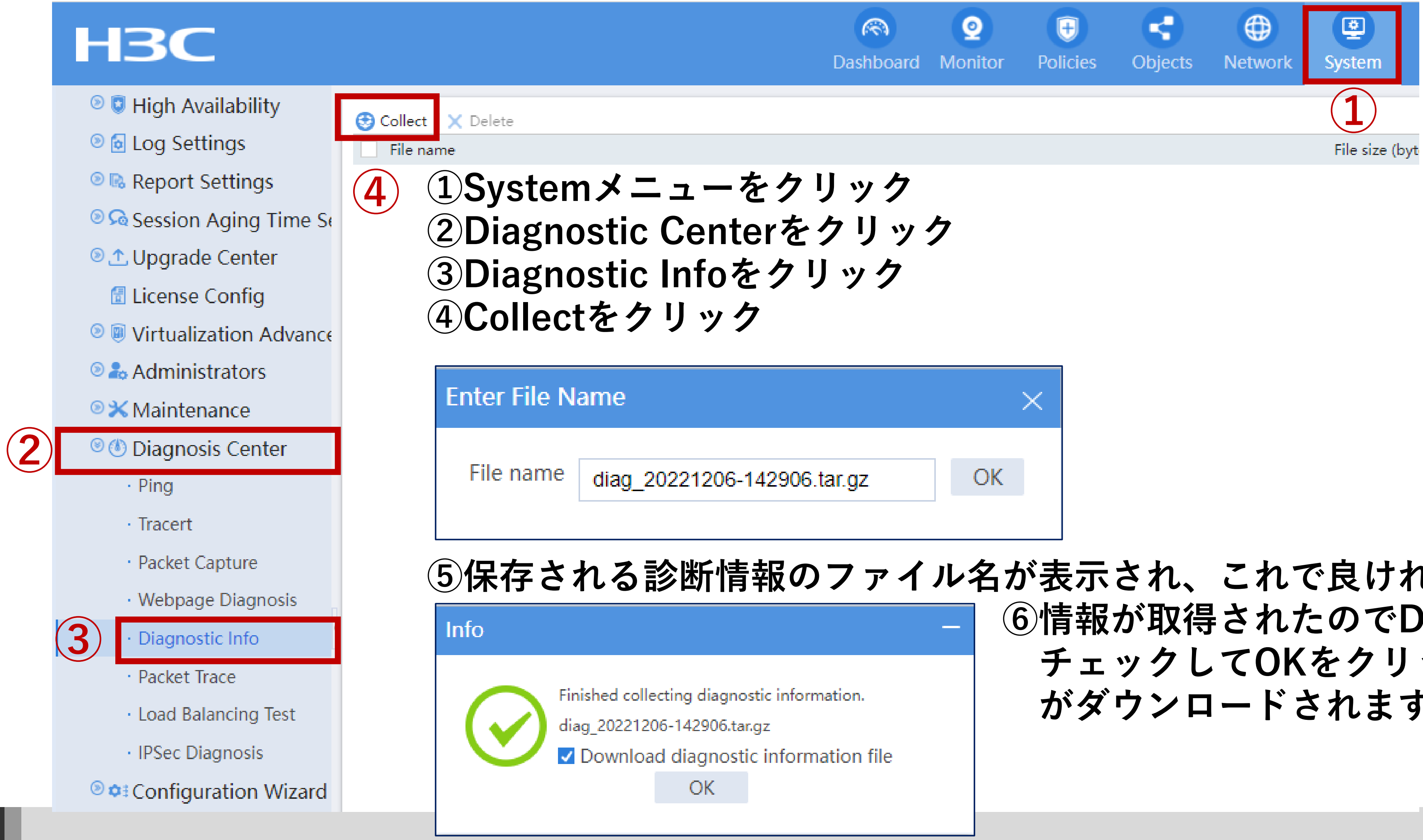
06 攻撃検証環境の整備

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。



①Systemメニューをクリック
②Diagnostic Centerをクリック
③Diagnostic Infoをクリック
④Collectをクリック

Enter File Name

File name: diag_20221206-142906.tar.gz　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

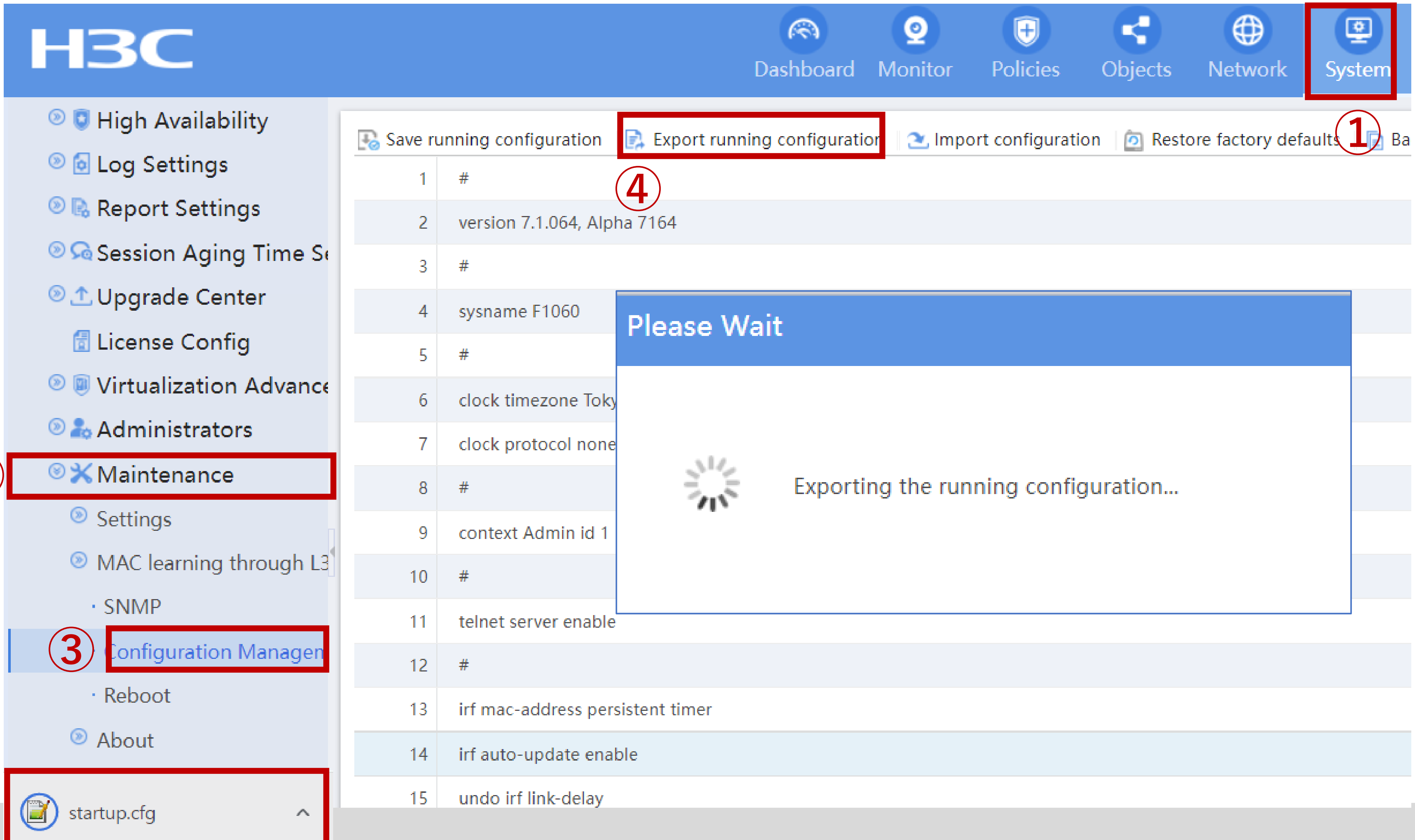
Info

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

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。



```
#
version 7.1.064, Alpha 7164
#
sysname F1060
#
clock timezone Toky
clock protocol none
#
context Admin id 1
#
telnet server enable
#
irf mac-address persistent timer
irf auto-update enable
undo irf link-delay
```

Please Wait

Exporting the running configuration...

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：

www.h3c.com