

**Item 2.1.9.1** A CONTRATADA deve entregar a quantidade de transceivers equivalente ao dobro da quantidade mínima de portas exigidas em cada lote conforme os itens 3.15.1.4, 3.22.1.4 e 3.29.1.4.

Resposta:

Entendemos que o item está comprovado na proposta comercial técnica onde apresenta o modelo e descrição do item conforme a quantidade exigida no item 3.22.1.4 a comprovação do item 2.1.9.1 apenas referencia a concordância que será entregue o dobro com o “de acordo”.

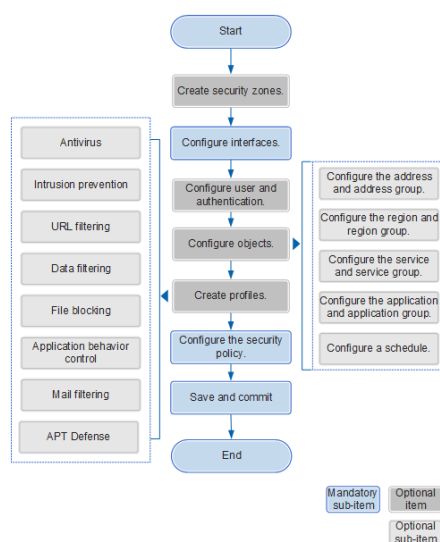
**Item 2.1.45.6.** Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoramento e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.

Resposta:

Abaixo segue um “configuration Guide” de como criar uma “Security Policy” utilizando um objeto.

DOC : HUAWEI USG6000&USG9500 V500R001C60 Product Documentation Issue:02 Release Date:2017-08-18

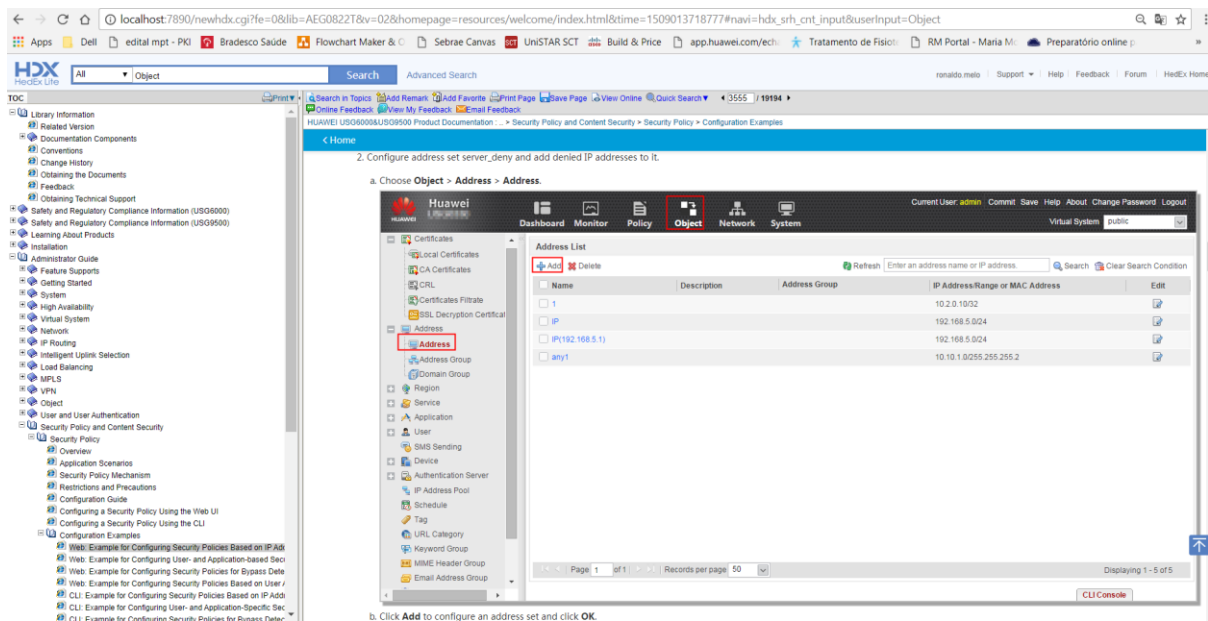
Pag. 3551 “Configuration Guide”



Segue um exemplo de configuração de uma “security policy” utilizando um objeto:

DOC : HUAWEI USG6000&USG9500 V500R001C60 Product Documentation Issue:02 Release Date:2017-08-18

Pag. 3555 “Web: Example for Configuring Security Policies Based on IP Addresses and Ports”



**2.1.45.9.** Deve suportar a geração de alertas automáticos via email, SNMP e Syslog.

Resposta:

Abaixo segue exemplo de configuração de logs para Syslog.

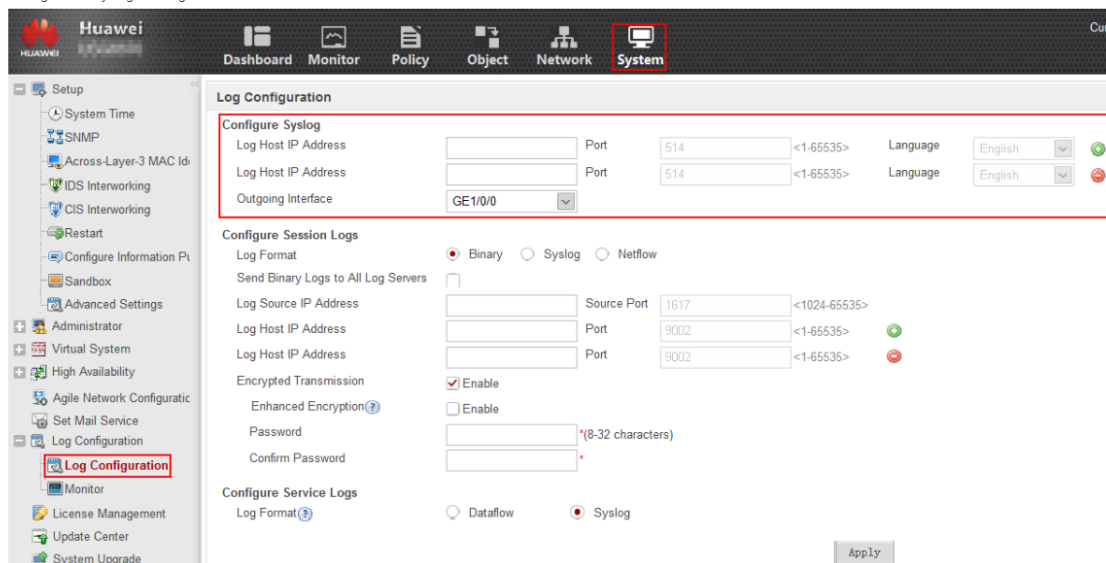
DOC : HUAWEI USG6000&USG9500 V500R001C60 Product Documentation Issue:02 Release Date:2017-08-18

Pag. 952 “Configuring Log Output”

#### Configuring Syslog Output

You need to configure the syslog host for system logs and service logs in syslog format. After the syslog host is configured, the FW sends generated syslogs to the host for it to perform analysis and management.

1. Choose **System** > **Log Configuration** > **Log Configuration**.
2. Configure the syslog sending function.

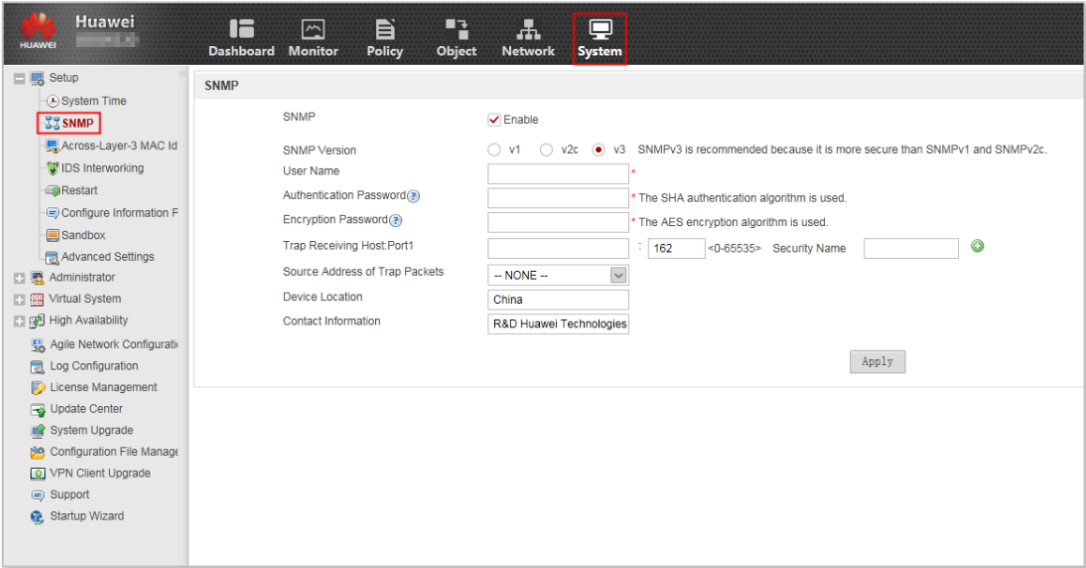


Abaixo segue exemplo de configuração de logs para SNMP.

Configuring SNMP Using the Web UI

This section describes how to use the Web UI to configure SNMP. After you configure SNMP, the network management station (NMS) can monitor and manage the managed device.

1. Choose **System** > **Setup** > **SNMP**.

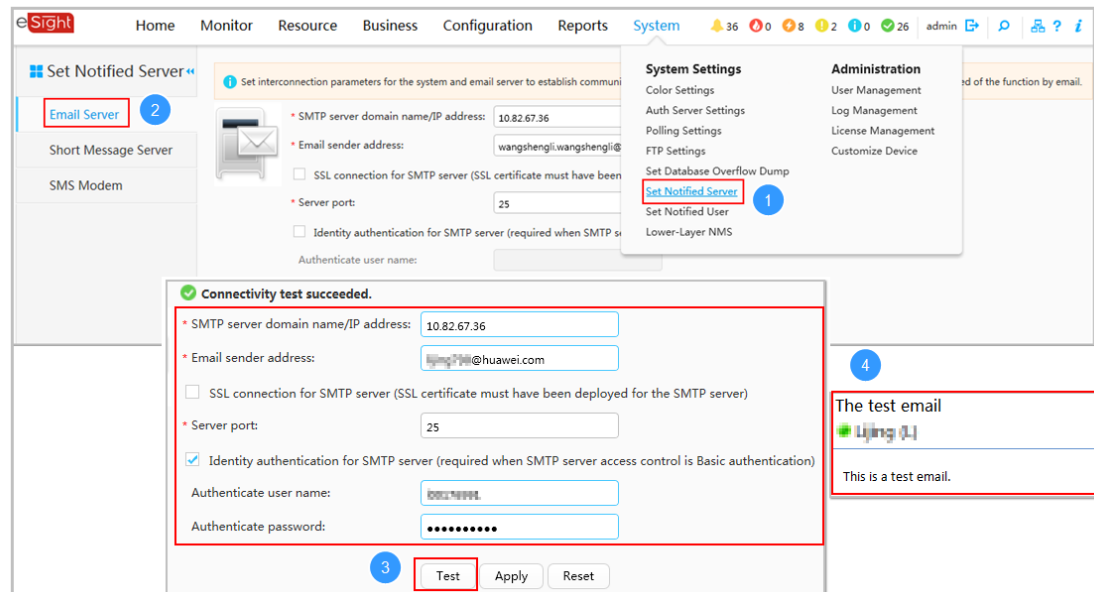


Abaixo segue exemplo de configuração do e-mail para envio dos alertas.

Example for Configuring an Email Server to Send Alarm Notifications

In daily network monitoring, O&M engineers can monitor the network status based on alarm notifications emails they receive. This example illustrates how to configure an email server on an enterprise campus network to send alarm notifications to O&M engineers.

2. Set interworking parameters for eSight and the email server.



**2.1.45.10.** Deve permitir a exportação de logs via SCP ou FTP.

Resposta:

DOC : HUAWEI USG6000&USG9500 V500R001C60 Product Documentation Issue:02 Release Date:2017-08-18

Pag. 4640

## System Logs

System Logs record system events and hardware environments. System Logs help you learn if the system has been functioning properly and perform troubleshooting when a fault occurs.

### Context

System logs include all logs on system alarms, user login and logout, system operations, and blacklist.

#### NOTE:

Before querying system logs, you have run the [log type syslog enable](#) command on the FW to enable the recording of system logs.

### Procedure

1. Choose **Monitor > Log > System Log** to view system logs.
2. **Optional:** Click **Export** to export system logs in CSV format to the management PC.
3. Click **Advanced Search** and enter **Security Level** or **Log Type**. Click **Export** to export logs. Only the logs filtered based on advanced search conditions are exported.

### Log Sample

The following figure shows the system logs generated within a specific time range:

Time	Log Type	Log Severity	Description	Virtual System
2016/11/08 19:23:57	Login	Informational	User admin(IP:172.16.5.156 ID:181) login succeeded	public
2016/11/08 19:23:32	Running	Debug	Last message repeated 1 times (InfoID=2880114721, ModuleName=HTTPD, InfoAlias=COMM_SUCC)	public

Field	Description
Time	Time when a system log is generated
Log Type	System log types:

**2.1.45.12.** Deve informar o número de sessões simultâneas e de novas sessões por segundo dos equipamentos gerenciados.



Resposta:

## Checking the Session Table Using the Web UI

This section describes how to check the session table using the Web UI to locate faults.

### Context

You can check the session table to locate faults.

- If a session entry has been established and traffic is permitted by security policies, the possible causes of service interruptions include but are not limited to:
  - Hardware faults on the outgoing interface (such as physical damage of an interface card or bad cable connections)
  - Packet drop on the downstream device
  - Incorrect routing configuration (To display the outgoing interface and next hop, choose **Monitor** > **Session Table** and click  in the **Details** column.)
  - Incorrect packet count on the outgoing interface (To display the traffic statistics, choose **Dashboard** > **Traffic History** and click .)
  - Administratively denied packets (packets dropped due to bandwidth management and attack defense policies)
  - Configuration errors
- If no session entry is established for a service, possible causes include but are not limited to the following:
  - Packets are not forwarded to the FW because of faults on an upstream device or incorrect route configuration.
  - The security policy configured on the FW blocks the packets. For example, the security policy action is configured as **Deny**, or the source IP address is blacklisted.
  - A hardware fault occurs at the incoming interface. For example, an interface card is damaged, or a network cable is not securely connected.
  - Attack defense functions, except blacklist, discard packets.
  - The bandwidth management function restricts the number of sessions. When the number of sessions exceeds the upper threshold, new sessions cannot be established, and packets are therefore discarded.
  - Configuration errors.

### Example

The session table of a specified time range is displayed as follows:

**Figure 1** The session table of a specified time range is displayed

Details	Proto...	Source ...	Desti...	Source Address	Destination Addr...	Source P...	Destination ...	Left Time	Outbound In...	Next Hop
	https	trust	local	172.16.10.178	10.18.74.29	62001	8443	00:10:00	InLoopBack0	127.0.0.1
	https	trust	local	172.16.10.133	10.18.74.29	51513	8443	00:10:00	InLoopBack0	127.0.0.1
	https	trust	local	172.16.10.134	10.18.74.29	59740	8443	00:09:56	InLoopBack0	127.0.0.1
	https	trust	local	172.16.10.134	10.18.74.29	59723	8443	00:08:24	InLoopBack0	127.0.0.1

Click  in the **Details** column to view details on the session table. The following table lists the meaning of each field.

**2.1.49.** As funcionalidades de VPN não podem possuir qualquer restrição de licenciamento, inclusive em relação ao número de clientes, aos softwares instalados nos clientes, IPs e máquinas, limitado apenas à capacidade de throughput do equipamento para VPN.

### Resposta:

Na proposta comercial deixa claro que serão fornecidas todas as licenças necessárias para o pleno atendimento do edital, conforme abaixo:

“Obs: Todos os equipamentos são acompanhados de todos os itens e acessórios necessários para o seu pleno funcionamento e atendimento completo aos requisitos do edital. Os itens e acessórios citados incluem: todos os cabos solicitados no Termo de Referência, memórias RAM e Flash, **licenças de software**, manuais para instalação e operação do produto e peças e acessórios necessários para fixação e montagem em rack padrão 19”.

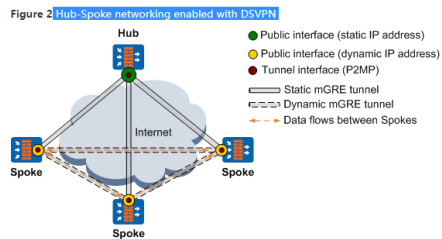
Neste caso a licença referenciada no Hedex pág.3082 refere-se ao limite máximo de “Concurrent Users” que para o modelo ofertado suporta o máximo de 5.000.

**2.1.50.** Deve permitir a arquitetura de VPN hub and spoke IPSec, tanto para topologias site-to-site ("Full Meshed" e "Estrela") como para client-to-site (remote access);

Resposta:

DOC : HUAWEI USG6000&USG9500 V500R001C60 Product Documentation Issue:02 Release Date:2017-08-18

Pag. 2972



#### Benefits

- Reduce costs on VPN construction.  
DSVPN implements dynamic connections between the Hub and Spokes, and between Spokes. Spokes do not need to purchase static public network addresses.
- Simplify configuration on the Hub and Spokes.  
The Hub and Spokes use an mGRE tunnel interface but not multiple GRE tunnel interfaces to establish tunnels. When a new Spoke is added to the network, the network administrator does not need to change configurations on the Hub or any existing Spokes. The administrator only needs to configure the new Spoke, and then the Spoke dynamically registers with the Hub.
- Reduce the forwarding delay between Spokes.  
Spokes can dynamically establish tunnels to directly exchange service data, reducing the forwarding delay and improving forwarding performance and efficiency.

**2.1.55.** Deve suportar a customização da interface Web para acesso a VPN pelos administradores do sistema, incluindo quais aplicativos, servidores e sistemas estarão acessíveis via portal;

Resposta:

DOC : HUAWEI USG6000&USG9500 V500R001C60 Product Documentation Issue:02 Release Date:2017-08-18

Pag. 3058

#### Web: Example for Configuring the Web Link Function for Mobile Employees to Access Intranet Servers

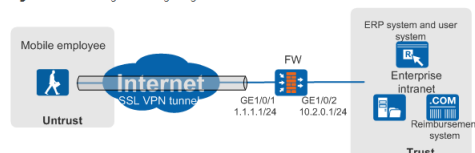
This section describes how to configure the web link function and local authentication.

##### Networking Requirements

Figure 1 shows the enterprise network. Mobile users are expected to access intranet servers using SSL VPNs. The local authentication mode of the FW is used for access users' identity authentication. Requirements are as follows:

- Mobile employees can access the ERP system through the web UI, and the problem that the ERP system is abnormally displayed on the SSL VPN client is avoided.
- The ERP system has two sublinks (used to link to the user system and reimbursement system respectively). When accessing the ERP system, mobile employees can access sublinks through the web UI.

Figure 1 Networking for configuring the web link function



**2.1.64** Implementar autenticação de usuários utilizando LDAP, Microsoft Active Directory, RADIUS e certificados digitais e suportar, no mínimo, autenticação two-way com certificado digital e LDAP ou Microsoft Active Directory ou RADIUS.

Resposta:

HCX  
Huawei Cloud X

Search  
Certificate-challenge Authentication

Advanced Search

Log In | Support | Help | Feedback | For

TOC

- Library Information
- Safety and Regulatory Compliance Information (USG6000)
- Safety and Regulatory Compliance Information (USG9500)
- Learning About Products
- Installation
- Administrator Guide
- Feature Supports
- Getting Started
- System
- High Availability
- Virtual System
- Network
- IP Routing
- Intelligent Uplink Selection
- Load Balancing
- MPLS
- VPN
- VPN Overview
- IPSec
- L2TP
- L2TP over IPSec
- GRE
- QSVN
- SSL VPN
- Overview
- Application Scenarios
- Mechanism
- Overall Flow
- Local Certificate Authentication
- User Authentication
- New Proxy
- File Sharing
- Port Forwarding
- Network Extension
- Restrictions and Precautions
- Configuring SSL VPN
- Logging in to the SSL VPN Gateway
- SSL VPN Gateway

Search in Topics | Add Remark | Add Favorite | Print Page | Save Page | Show Path | Quick Search | 3033 | 19194

HUAWEI USG6000&USG9500 Product Documentation : > VPN > SSL VPN > Mechanism

### Certificate-anonymous Authentication

The FW verifies the identity of a user by authenticating only the user's client certificate.  
Figure 4 shows certificate-anonymous authentication.

Figure 4 Certificate-anonymous authentication

System running flow  
System administrator's operations

The authentication procedure is as follows:

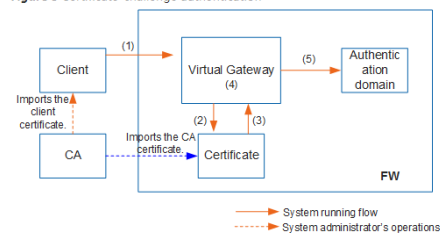
1. A user selects a client certificate on the SSL VPN gateway login page on the SSL VPN client. The client then sends the client certificate to the SSL VPN gateway module on the FW.
2. The SSL VPN gateway module forwards the client certificate and the certificate authority (CA) certificate that the gateway is referencing to the certificate module.
3. The certificate module verifies the client certificate based on the CA certificate that the gateway is referencing and returns the verification result to the SSL VPN gateway module.

- If the CA certificate and the client certificate are issued by the same CA and the client certificate does not expire, the certificate module considers the client certificate valid (trusted) and user authentication succeeds. In this case, go to 4.
- If the CA certificate and the client certificate are not issued by the same CA or the client certificate has expired, the certificate module considers the client certificate invalid (untrusted) and user authentication fails. In this case, go to 5.

### Certificate-challenge Authentication

Certificate-challenge authentication is to combine local authentication or server authentication with authentication of the client certificate.  
Figure 5 shows certificate-challenge authentication.

Figure 5 Certificate-challenge authentication



The authentication procedure is as follows:

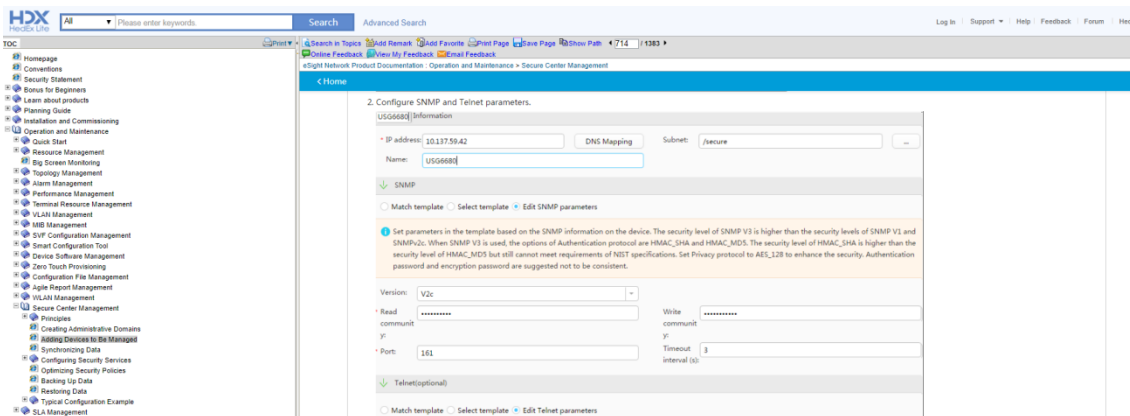
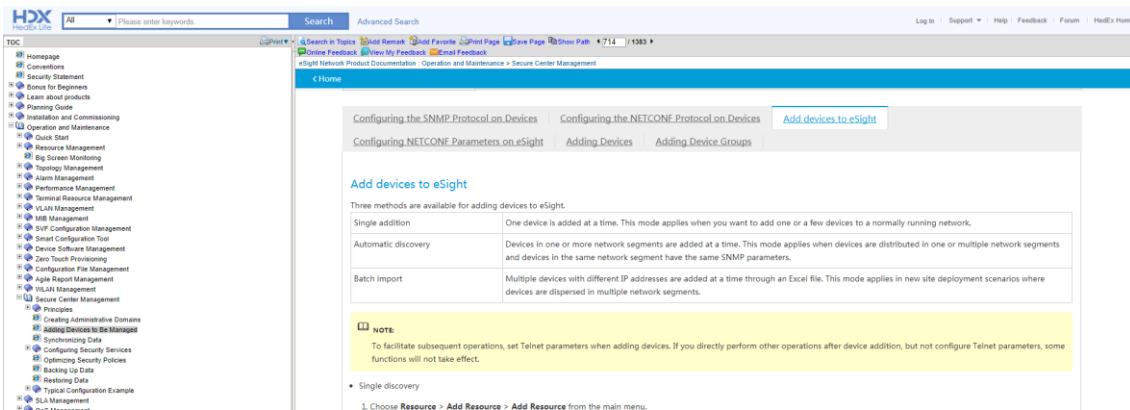
1. A user enters the password and selects a client certificate on the SSL VPN gateway login page on the SSL VPN client. The client then sends the user name and password and client certificate to the SSL VPN gateway module on the FW.
  2. The SSL VPN gateway module forwards the client certificate and the CA certificate that the gateway is referencing to the certificate module.
  3. The certificate module verifies the client certificate based on the CA certificate that the gateway is referencing and returns the verification result to the SSL VPN gateway module.
- If the CA certificate and the client certificate are issued by the same CA and the client certificate does not expire, the certificate module considers the client certificate valid (trusted). In this case, go to the next step.
  - If the CA certificate and the client certificate are not issued by the same CA or the client certificate has expired, the certificate module considers the client certificate invalid (untrusted) and returns an authentication failure result to the SSL VPN gateway module and then to the client.

**2.2.11** Deverá utilizar comunicação segura criptografada entre a solução de gerência e os equipamentos gerenciados.

### Resposta:

DOC : eSight Network V300R007C00 Product Documentation Library Version:05 Date: 2017-04-22

Pag. 714 “Adding Devices to Be Managed”

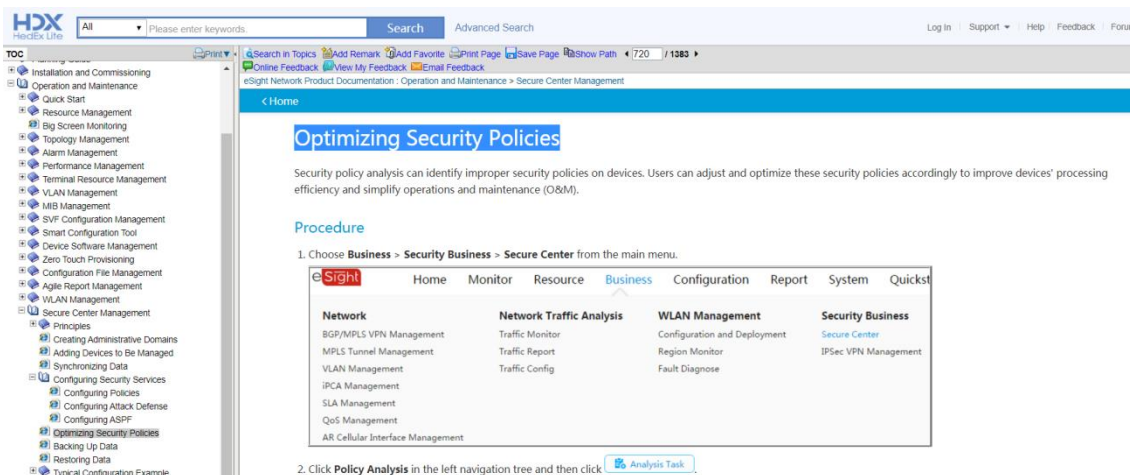


**2.2.14** Deve permitir validar as regras antes, durante ou depois de aplicá-las.

Resposta:

DOC : eSight Network V300R007C00 Product Documentation Library Version:05 Date: 2017-04-22

Pag. 720 “Optimizing Security Policies”





2.2.15 Deve ser capaz de testar a conectividade dos equipamentos gerenciados.

Resposta:

DOC : eSight Network V300R007C00 Product Documentation Library Version:05 Date: 2017-04-22

Pag. 61 “Fault Management”

The screenshot shows the 'Fault Management' section of the eSight Network V300R007C00 Product Documentation Library. The page includes a search bar, a navigation menu on the left, and a main content area. The main content area is titled 'Fault Management' and contains the following text:

eSight has the following alarm management functions:

- Monitors network-wide alarms and remotely sends alarm notifications to notify maintenance engineers in a timely manner, ensuring troubleshooting efficiency.
- Provides customized functions such as alarm filtering, alarm masking, and alarm severity redefinition to meet requirements in various scenarios.

**Basic Alarm Concepts**

- Alarm Severity: There are four alarm severities: Critical, Major, Minor, and Warning, as shown in Table 1. You can take different measures to process the alarms by the severity level.

**Table 1 Alarm severity**

Alarm Severity	Description
Critical	An alarm severity that indicates a severe resource problem disrupting or severely impeding normal use.
Major	An alarm severity that indicates the possibility of some service-related problems with the resource. The severity of the problem is relatively high and the normal use of the resource is likely to be impaired.
Minor	An alarm severity that indicates the problems without affecting services. The problems of this severity may result serious faults, and therefore you need to take some corrective actions.
Warning	An alarm severity that indicates a condition exists that could potentially cause a problem with the resource.

2.2.16 Deve prover funcionalidade de detecção de regras conflitantes ou regras equivalentes.

Resposta:

DOC : eSight Network V300R007C00 Product Documentation Library Version:05 Date: 2017-04-22

Pag. 720 “Optimizing Security Policies”

The screenshot shows the 'Optimizing Security Policies' section of the eSight Network V300R007C00 Product Documentation Library. The page includes a search bar, a navigation menu on the left, and a main content area. The main content area is titled 'Optimizing Security Policies' and contains the following text:

**security policy analysis can identify improper security policies on devices.** Users can adjust and optimize these security policies accordingly to improve devices' processing efficiency and simplify operations and maintenance (O&M).

**Procedure**

- Choose **Business > Security Business > Secure Center** from the main menu.

The screenshot shows the eSight Network V300R007C00 Product Documentation Library interface. The main content area is titled 'Optimizing Security Policies'. It includes a search bar, a navigation menu on the left, and a main content area. The main content area is titled 'Optimizing Security Policies' and contains the following text:

**security policy analysis can identify improper security policies on devices.** Users can adjust and optimize these security policies accordingly to improve devices' processing efficiency and simplify operations and maintenance (O&M).

**Procedure**

- Choose **Business > Security Business > Secure Center** from the main menu.

The screenshot shows the eSight Network V300R007C00 Product Documentation Library interface. The main content area is titled 'Optimizing Security Policies'. It includes a search bar, a navigation menu on the left, and a main content area. The main content area is titled 'Optimizing Security Policies' and contains the following text:

**security policy analysis can identify improper security policies on devices.** Users can adjust and optimize these security policies accordingly to improve devices' processing efficiency and simplify operations and maintenance (O&M).

**Procedure**

- Choose **Business > Security Business > Secure Center** from the main menu.

**2.3.2** Possuir, no mínimo, um conjunto de 2.000 (duas mil) assinaturas de detecção e prevenção de ataques, devendo também detectar ataques baseados em anomalias;

Resposta:

DOC:

<http://e.huawei.com/en/material/onLineView?materialid=d150e7fa28414d42b55beb5e4d04ae88>

Página: 8

Intrusion prevention	Provides over 5000 signatures for attack identification.
	Provides protocol identification to defend against abnormal protocol behaviors.
	Supports user-defined IPS signatures.
	Supports APT defense. Interworking with the Sandbox to detect and block the malicious files in the network.

DOC: HUAWEI USG6000&USG9500\_V500R001C60\_02\_en\_AEG0822T

Página: 3612

9. **Optional:** Configure protocol anomaly detection in the IPS profile view.

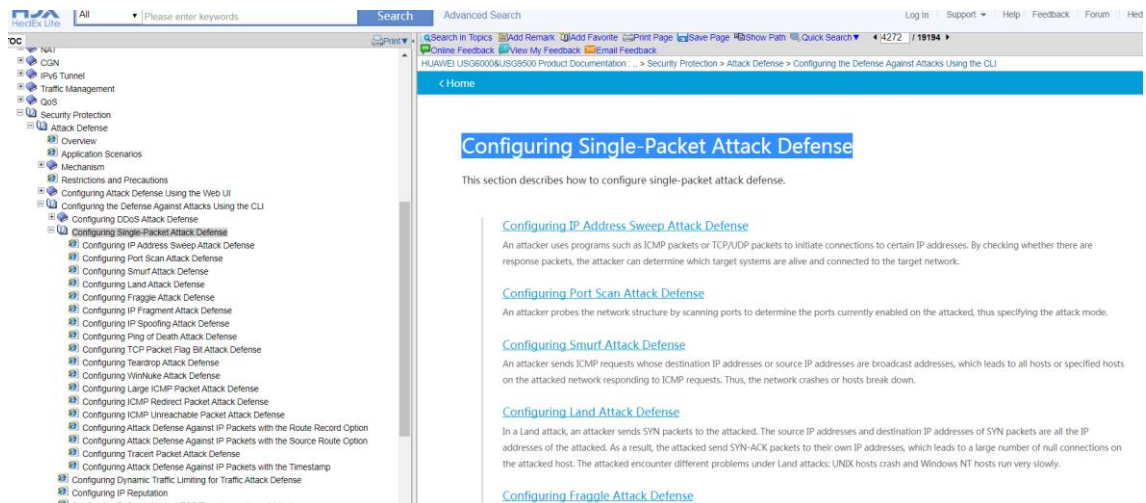
Item	Command
Detecting whether an HTTP traffic contains the SSH traffic	<a href="#">http ssh-over-http check</a> action { alert   block }
Detecting whether an HTTP packet contains multiple <b>Host</b> fields	<a href="#">http multi-host check</a> action { alert   block }
Detecting the <b>X-Online-Host</b> field in an HTTP packet	<a href="#">http x-online-host check</a> { any   blacklist   multiple } action { alert   block } <a href="#">http x-online-host blacklist</a> <i>blacklist</i>
Detecting the <b>X-Forwarded-For</b> field in an HTTP packet	<a href="#">http x-forwarded-for check</a> { any   whitelist } action { alert   block } <a href="#">http x-forwarded-for whitelist</a> <i>ipv4 ip-address</i>
Detecting whether the protocol format of a DNS packet is abnormal	<a href="#">dns malformed-packet check</a> action { alert   block }
Detecting the query of a DNS packet	<a href="#">dns request-type check</a> { start-type { to end-type } action { default-action } { alert   allow   block }

**2.3.13** Deve resistir a técnicas de evasão ou ataques direcionados ao próprio equipamento, suportando, no mínimo, as técnicas: IP Packet Fragmentation, Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, Payload Encoding, FTP Evasion e Layered Evasions.

Resposta:

DOC : HUAWEI USG6000&USG9500 V500R001C60 Product Documentation Issue:02 Release Date:2017-08-18

Pag. 4272 “Configuring Single-Packet Attack Defense”



**2.4.3** Deve ser capaz de, se houver algum atraso ou falha na realização da atualização automática, o equipamento deve ter a capacidade de alertar imediatamente o administrador através de logs, e-mail ou outros meios de alerta;

DOC: HUAWEI USG6000&USG9500\_V500R001C60\_02\_en\_AEG0822T  
 Página: 889

Na página acima, há todo o ciclo de atualizações do produto.

Página: 14150

## UPDATE/4/DOWNLOAD\_FAIL

### Message

UPDATE/4/DOWNLOAD\_FAIL(1): Failed to download the new version. (SyslogId=[syslog-id], User=[username], IP=[ip-address], Module=[module], Status=[status], Duration(s)=[duration], Reason=[reason], Suggestion=[suggestion])

### Description

Failed to download the new version.

### Parameters

Parameter Name	Parameter Meaning
<i>syslog-id</i>	Log ID
<i>username</i>	User name that is used to perform the update operation. For scheduled update, <b>SystemTimer</b> is displayed for this parameter. If the system cannot obtain the user name, <b>**</b> is displayed.
<i>ip-address</i>	IP address of the user that performs the update operation. If the system cannot obtain the IP address, <b>**</b> is displayed.
<i>module</i>	Update module, which can be:

	<ul style="list-style-type: none"> <li>AV-SDB: AV signature database</li> <li>CNC: malicious domain name database</li> <li>IPS-SDB: IPS signature database</li> <li>IP-REPUTATION: IP reputation database</li> <li>SA-SDB: SA signature database</li> <li>FILE-REPUTATION: file reputation signature database</li> </ul>
<i>status</i>	<p>Update status, which can be:</p> <ul style="list-style-type: none"> <li>manual-update: manual update</li> <li>auto-update: automatic update</li> </ul>
<i>duration</i>	Duration for downloading the signature database, in seconds
<i>reason</i>	<p>Causes of the downloading failure, including:</p> <ol style="list-style-type: none"> <li>Failed to perform DNS resolution.</li> <li>Connecting to the security server failed.</li> <li>The update service of components expires.</li> <li>The update service is not activated.</li> <li>Failed to verify the update file.</li> <li>The current update request is terminated.</li> <li>Disconnected from the update server.</li> <li>Online update init error.</li> <li>The free space of the storage card is insufficient.</li> <li>The storage card is not in position or formatted.</li> <li>No signature database is available.</li> <li>The free space of the storage card on the standby MPU is insufficient.</li> <li>Failed to copy the update file to the storage card of the standby MPU.</li> <li>Failed to perform DNS of the download server.</li> <li>Connecting to the download server failed.</li> <li>The proxy server authentication failed.</li> <li>Failed to perform DNS of the proxy server.</li> <li>Connecting to the proxy server failed.</li> </ol>
<i>suggestion</i>	<p>Suggestions for rectifying the signature database loading fault:</p> <ol style="list-style-type: none"> <li>Check the Internet settings and try again later.</li> <li>Check the Internet settings and try again later.</li> <li>Update the upgrade service.</li> <li>Purchase the upgrade service.</li> </ol>

	<ol style="list-style-type: none"> <li>5. Download the upgrade file again.</li> <li>6. Confirm the operation of terminating the upgrade.</li> <li>7. Check the network condition.</li> <li>8. Check in-service upgrade configuration.</li> <li>9. Ensure that the storage card has sufficient space for the upgrade.</li> <li>10. Ensure the storage card is in position and formatted.</li> <li>11. Contact customer service engineers.</li> <li>12. Ensure that the storage card of the standby MPU has sufficient space to store the upgrade file.</li> <li>13. Ensure that the storage card of the standby MPU has sufficient space to store the upgrade file.</li> <li>14. Please check the DNS server configuration.</li> <li>15. Please check the Internet connection, and try again later.</li> <li>16. Please check the update proxy configuration.</li> <li>17. Please check the DNS server configuration.</li> <li>18. Please check the Internet connection, and try again later.</li> </ol>
--	---

**2.5.9** Deve ser capaz de exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários, na tentativa de acesso a recursos proibidos ou restringidos pela política de segurança do órgão;

**2.5.10** Permitir o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual;

**2.5.10.1** O item 2.5.10 pode ser atendido através da criação de aplicações em camada 7 customizadas.

Resposta:

Os itens acima poderão ser comprovados através de teste de bancada conforme carta enviada pelo fabricante, pois devido às características específicas exigida não possuímos tal referência no manual do fabricante.

**2.5.11** Permitir o bloqueio de URLs cujo campo CN ou DN não contém um domínio válido para o certificado SSL;

Resposta:

DOC: HUAWEI USG6000&USG9500\_V500R001C60\_02\_en\_AEG0822T

Página: 3552

## display ssl sni-cache

### Function

The **display ssl sni-cache** command displays the SNI cache list of the SSL-encrypted traffic detection policy.

### Format

**display ssl sni-cache** { *ip ip-address* | *sni server-name* | **all** } [ **all-systems** ]

### Parameters

Parameter	Description	Value
<b>ip</b> <i>ip-address</i>	Specifies the SNI cache list of a specified IP address.	The IP address must be added to the SNI cache list.
<b>sni</b> <i>server-name</i>	Specifies the SNI cache list of a specified server SNI.	The server SNI must be added to the SNI cache list.
<b>all</b>	Indicates the SNI cache list of all SSL-encrypted traffic detection policies.	-
<b>all-systems</b>	Indicates the SNI cache list of all systems.	-

### Usage Guidelines

During the SSL handshake, the FW saves the mapping between the SNI and the CN in the SNI cache list if the SNI field in the client certificate is inconsistent with the SAN/CN field in the server certificate. If the SNI field in the client certificate is inconsistent with the SAN/CN field in the server certificate, the FW does not establish the SSL connection with the server. In addition, after the FW decrypts the SSL-encrypted traffic, if the abstracted URL address matches the SAN/CN in the server certificate in the URL category of the SSL-encrypted traffic detection policy, the FW uses the SAN/CN to match the corresponding policy and performs the relevant operations.

**2.6.2** Deve ser capaz de identificar as aplicações mesmo que não estejam utilizando sua porta default.

Resposta:

DOC: HUAWEI USG6000&USG9500\_V500R001C60\_02\_en\_AEG0822T

Página: 3829

## Application Policy Tuning

This section describes how to use the policy tuning tool to facilitate policy optimization.

### Prerequisites

- The application identification function in full mode has been enabled by choosing **Object > Application > Application**, or applications/application groups have been referenced when security policies are configured.
- General security policies have been configured and running for a period of time.



#### NOTE:

Policy tuning analyzes only permitted traffic. Therefore, you must set the action for the important traffic to Permit when you configure general security policies.

### Context

Policy tuning has the following functions:

- Identifies applications and converts service (port)-based security policies into application-based policies.
- Provides tuning suggestions to optimize security policies and deploy security functions such as intrusion prevention and antivirus.

**2.6.9** Possuir perfis/políticas de segurança de aplicações pré-definidas/pré-configuradas na solução;

Resposta:

DOC: HUAWEI USG6000&USG9500\_V500R001C60\_02\_en\_AEG0822T


Página: 3552

# Configuring a Security Policy Using the Web UI

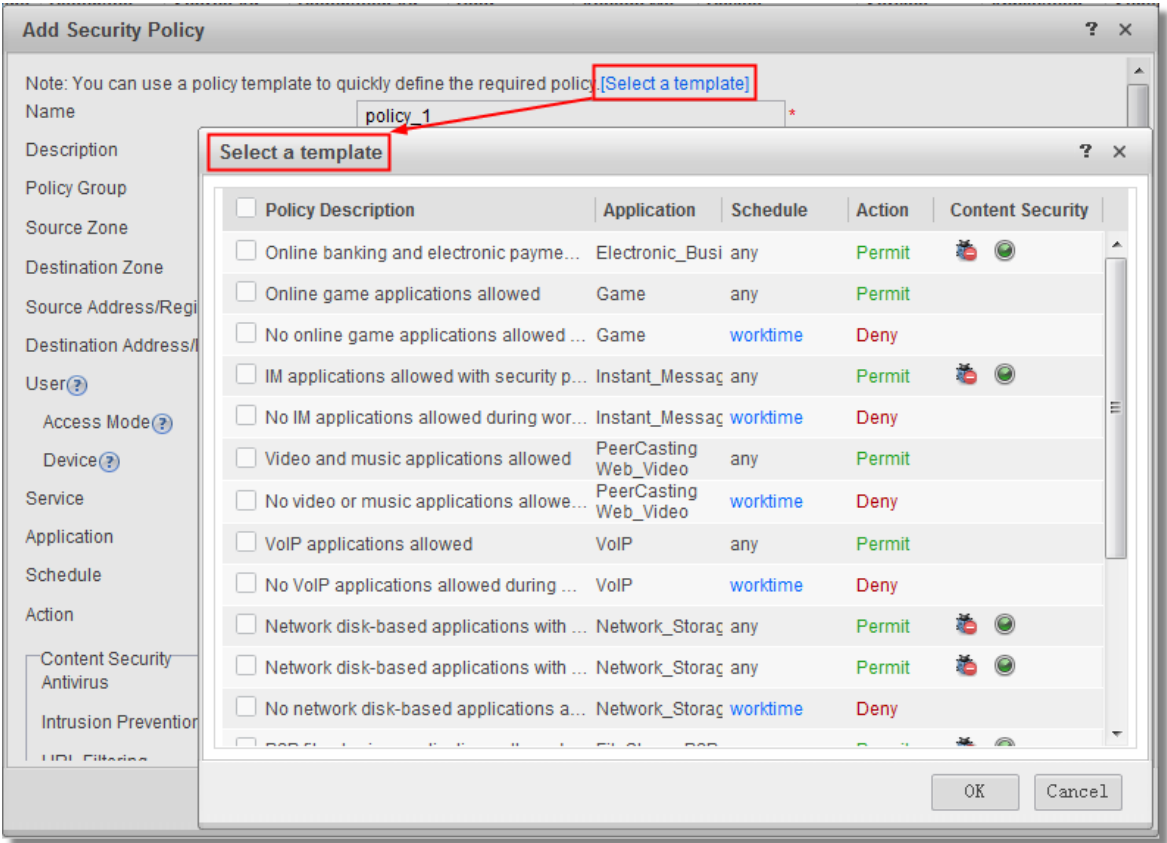
This section describes how to configure a security policy and a security policy group.

## Configuring a Security Policy

1. Choose **Policy > Security Policy**.

 **NOTE:**  
Choose **Policy > Security Policy > Security Policy** in some device models.

2. Click **Add**. On the page that is displayed, select **Add Security Policy**.
3. **Optional:** Select a template if the settings, such as application category, time range, action, and data security measures, in the template suit your needs.



3.22	Firewall multifuncional tipo 4
3.22.1	Requisitos específicos:
3.22.1.1	Atender a todos os requisitos do item 2.1;
3.23.1	Atender a todos os requisitos do item 2.3;
3.24.1.1	Atender a todos os requisitos do item 2.4;

3.24.1.2.1	A funcionalidade de APT ( Advanced Persistent Threat) e Zero Day deve possuir capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, tais como: Windows XP e Windows 7, assim como documentos do Windows Office. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.
3.25.1	Atender a todos os requisitos do item 2.5;
3.26.1	Atender a todos os requisitos do item 2.1.39 e do item 2.6;
3.28	Solução de gerência centralizada
3.28.1	Requisitos específicos:
3.28.1.1	Atender a todos os requisitos do item 2.2;

Resposta:

Os itens acima poderão ser comprovados através de teste de bancada conforme carta enviada pelo fabricante, pois devido às características específicas exigida não possuímos tal referência no manual do fabricante.

**3.28.1.2** Possuir capacidade mínima de 2 TB para armazenamento de logs e eventos.

Resposta:

Esse item se referencia em caso de entrega de “appliance especializado” e não em solução “appliance virtual” conforme item 2.2.1.1, desta forma não se aplica a nossa solução.