Configuração de log do sistema nos roteadores VPN RV320 e RV325 Series

Objetivo

Os registros do sistema são registros de eventos da rede. Os registros são uma ferramenta importante usada para entender como uma rede opera. Eles são úteis para gerenciamento de rede e solução de problemas de rede.

Este artigo explica como configurar os tipos de logs a serem gravados, como exibir os logs na Série RV32x VPN Router e como enviar os logs a um destinatário por SMS, a um servidor de log do sistema ou a um destinatário por e-mail.

Dispositivos aplicáveis

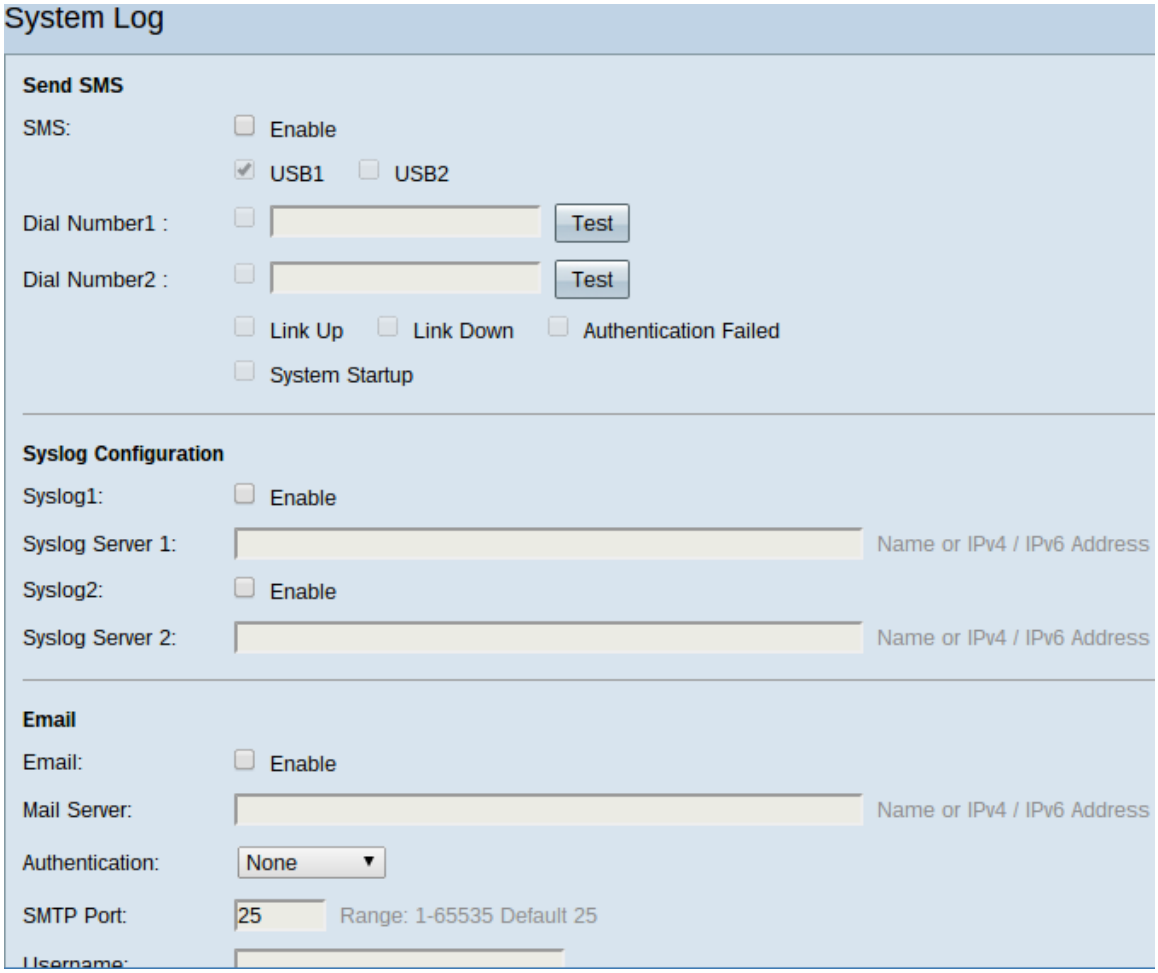
RV320 Roteador VPN WAN duplo
Roteador VPN WAN duplo RV325 Gigabit

Versão de software

•v1.1.0.09

Configuração do log do sistema

Etapa 1. Efetue login no Utilitário de configuração da Web e escolha **Log > System Log**. A página *Log do Sistema* é aberta:



Consulte as seções a seguir para obter informações sobre a página *Log do sistema*.

·Registros do sistema por SMS — Como enviar os registros do sistema para um telefone por SMS.

·Registros do sistema em Servidores de registro do sistema — Como enviar os registros do sistema a um servidor de registro do sistema.

·Email System Logs — Como enviar os registros do sistema para um endereço de e-mail.

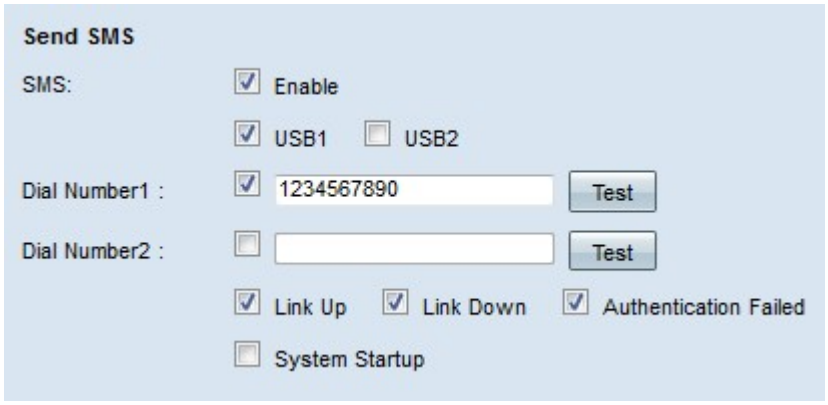
·Configurações de log — Como configurar o tipo de mensagem salva no log.

·Exibir log do sistema — Como exibir os logs do sistema no dispositivo.

·Exibir tabela de log de saída — Como exibir os logs do sistema que se relacionam apenas a pacotes de saída.

·Exibir tabela de log de entrada — Como exibir os logs do sistema que se relacionam apenas a pacotes de entrada.

Logs do sistema por SMS



Etapa 1. Marque **Enable** no campo SMS para enviar registros do sistema a um cliente por meio de mensagens do Short Message Service (SMS).

Etapa 2. Marque as caixas de seleção das portas USB às quais o modem USB 3G está conectado.

Etapa 3. Marque a caixa de seleção no campo Discar número 1 e digite o número do telefone para o qual as mensagens são enviadas.

Note: Clique em **Test** para testar a conexão com o número de discagem 1. Se o número configurado não receber a mensagem de teste, verifique se o número de telefone foi inserido corretamente no campo Discar número 1.

Etapa 4. (Opcional) Marque a caixa de seleção no campo Número de discagem2 e digite o número do telefone para o qual as mensagens são enviadas.

Note: Clique em **Test** para testar a conexão com o número de discagem 2. Se o número configurado não receber a mensagem de teste, verifique se o número de telefone foi inserido corretamente no campo Número de discagem 2.

Etapa 5. Marque as caixas de seleção dos eventos que dispararão um log a ser enviado.

Link Up - Uma conexão com o RV320 foi criada.

Link Down — Uma conexão com o RV320 foi desativada.

Falha na autenticação — uma autenticação falhou.

Inicialização do sistema — O roteador é inicializado.

Etapa 6. Click **Save**. O sistema faz login através do SMS.

Logs do sistema em servidores de registro do sistema

Etapa 1. Marque **Enable (Habilitar)** no campo Syslog1 para enviar logs do sistema para um

servidor de log do sistema.

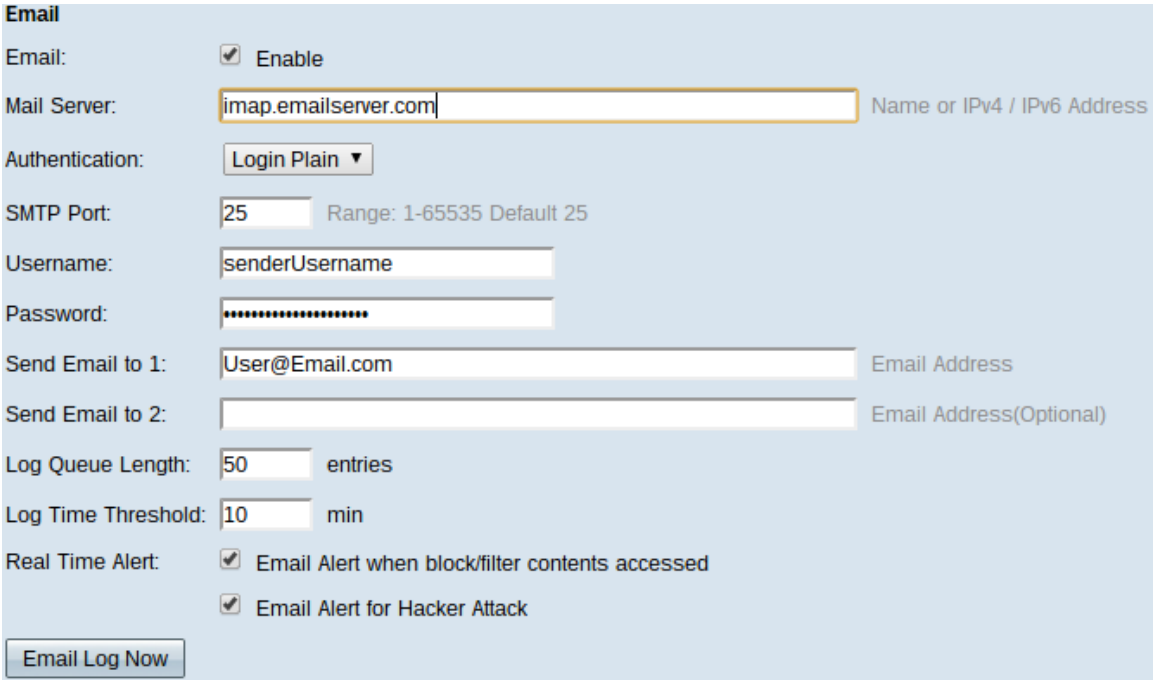
Etapa 2. Digite o nome do host ou o endereço IP do servidor de log do sistema no campo Servidor de Syslog 1.

Etapa 3. (Opcional) Para enviar logs para outro servidor de log do sistema, marque **Enable (Habilitar)** no campo Syslog2.

Etapa 4. Se a caixa de seleção estiver marcada no campo Syslog2, insira o nome do host ou o endereço IP do servidor de log do sistema no campo Syslog Server 2.

Etapa 5. Click **Save**. O sistema faz login através dos servidores de log do sistema está configurado.

Logs do sistema de e-mail



Etapa 1. Marque **Habilitar** no campo E-mail para enviar logs do sistema a um destinatário por e-mail.

Etapa 2. Insira o nome de domínio ou o endereço IP do servidor de e-mail no campo Servidor de e-mail.

Etapa 3. Escolha o tipo de Autenticação que o servidor de e-mail usa no campo Autenticação.

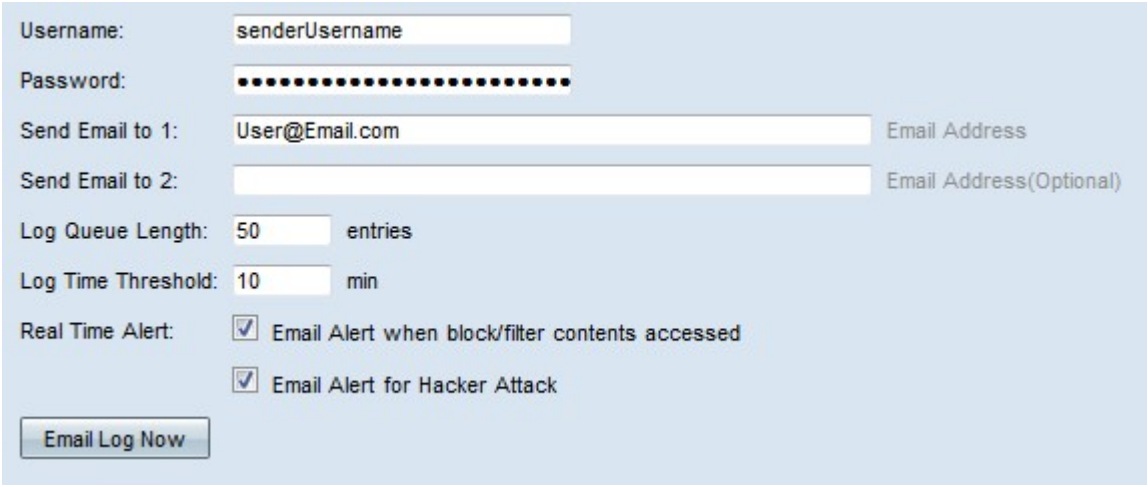
Nenhum — O servidor de e-mail não usa autenticação.

Login Simples — O servidor de e-mail usa a autenticação que está em um formato de texto simples.

TLS — O servidor de e-mail usa TLS (Transport Layer Security) para permitir que o cliente e o servidor troquem informações de autenticação com segurança.

SSL — O servidor de e-mail usa SSL (Secure Sockets Layer) para permitir que o cliente e o servidor troquem informações de autenticação com segurança.

Etapa 4. Insira a porta SMTP (Simple Mail Transfer Protocol) que o servidor de e-mail usa no campo Porta SMTP. O SMTP é um protocolo que permite que emails sejam transmitidos através de redes IP.



Etapa 5. Insira o nome de usuário do remetente do e-mail no campo Nome de usuário.

Etapa 6. Insira a senha do remetente do e-mail no campo Senha.

Passo 7. Insira o endereço de e-mail do destinatário no campo Enviar e-mail para 1.

Etapa 8. (Opcional) Insira um endereço de e-mail adicional para o qual enviar e-mails de log no campo Enviar e-mail para 2.

Etapa 9. Insira o número de entradas de log que devem ser feitas antes que o log seja enviado ao destinatário de e-mail no campo Tamanho da fila de log.

Etapa 10. Insira o intervalo no qual o dispositivo envia o log ao e-mail no campo Limite de tempo de log.

Etapa 11. Marque a primeira caixa de seleção do campo Alerta em tempo real para enviar imediatamente um e-mail quando alguém, que foi bloqueado ou filtrado, tentar acessar o roteador.

Etapa 12. Marque a segunda caixa de seleção do campo Alerta em tempo real para enviar um e-mail imediatamente quando um hacker tentar acessar o roteador por meio de um ataque de negação de serviço (DOS).

Note: Clique em **Log de e-mail agora** para enviar imediatamente o log.

Etapa 13. Click **Save**. O sistema faz login por e-mail configurado.

Configurações de log

Etapa 1. Marque as caixas de seleção dos eventos que dispararão uma entrada de log.

Log de alertas — Esses logs são criados quando um ataque ou tentativa de ataque ocorre.

- Inundação de Sinais — Solicitação SYN são recebidas mais rápido do que o roteador pode processá-las.

- Spoofing de IP — O RV320 recebeu pacotes IP com endereços IP de origem forjada.

- Tentativa de logon não autorizada — Falha na tentativa rejeitada de fazer logon na rede.

- Ping of Death - Um ping de tamanho anormal foi enviado a uma interface na tentativa de travar o dispositivo de destino.

- Win Nuke — O DDOS (Distributed Denial of Service Attack, ataque remoto de negação de serviço) conhecido como WinNuke, foi enviado para uma interface na tentativa de travar o dispositivo de destino.

Log geral — Esses logs são criados quando ações gerais de rede ocorrem.

- Negar políticas — O acesso foi negado a um usuário com base nas políticas configuradas do roteador.

- Login autorizado — Um usuário foi autorizado a acessar a rede.

- Mensagens de erro do sistema — Ocorreu um erro no sistema.

- Permitir políticas — O acesso foi concedido a um usuário com base nas políticas configuradas do roteador.

- Kernel — Inclua todas as mensagens do kernel no registro. O kernel é a primeira parte do sistema operacional que é carregada na memória na inicialização. As mensagens do kernel são logs associados ao kernel.

- Alterações na configuração — A configuração do roteador foi modificada.

- IPSEC e PPTP VPN — ocorreu uma negociação, conexão ou desconexão de IPSEC e PPTP VPN.

- VPN SSL — Ocorreu uma negociação, conexão ou desconexão de VPN SSL.

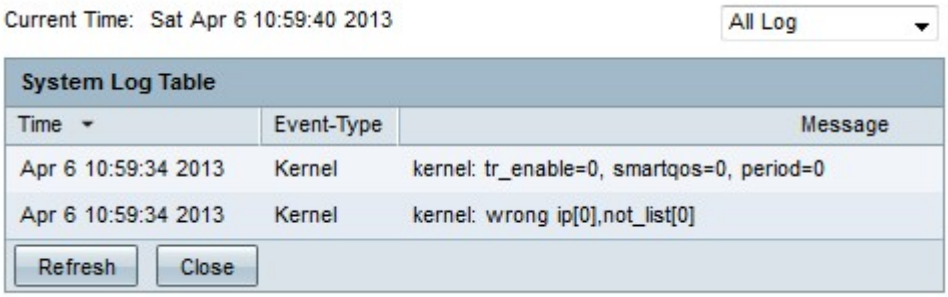
- Rede — Uma conexão física foi feita ou perdida nas interfaces WAN ou DMZ.

Etapa 2. Click **Save**. As Configurações de log estão configuradas.

Note: Clique em **Limpar registro** para limpar o registro atual.

Exibir log do sistema

Etapa 1. Clique em **Exibir log do sistema** para exibir a tabela de log do sistema. A janela *System Log Table (Tabela de log do sistema)* é exibida.



Etapa 2. (Opcional) Na lista suspensa, escolha o tipo de log a ser exibido.

Todos os logs — Inclui todas as mensagens de log.

Log do sistema — Inclui apenas as mensagens de erro do sistema.

Firewall/DoS Log — Inclui apenas os logs de alerta.

Log de VPN — inclui somente os logs de VPN IPSec e PPTP e SSL VPN.

Log de rede — Inclui apenas os logs de rede.

Log do kernel — Inclui apenas mensagens do kernel.

Log do usuário — inclui somente políticas de negação, políticas de permissão, login autorizado e logs de alteração de configuração

Log SSL — Inclui apenas logs de VPN SSL.

A Tabela de log do sistema exibe as seguintes informações.

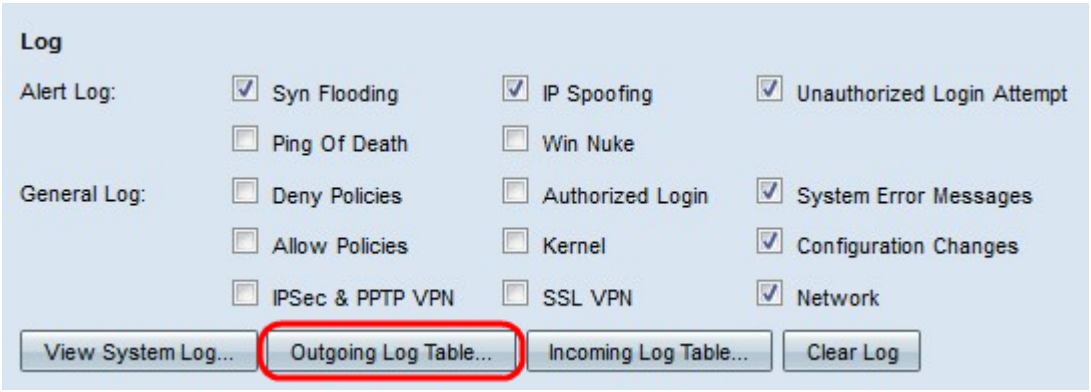
Hora — A hora em que o log foi criado.

Event-Type — O tipo de log.

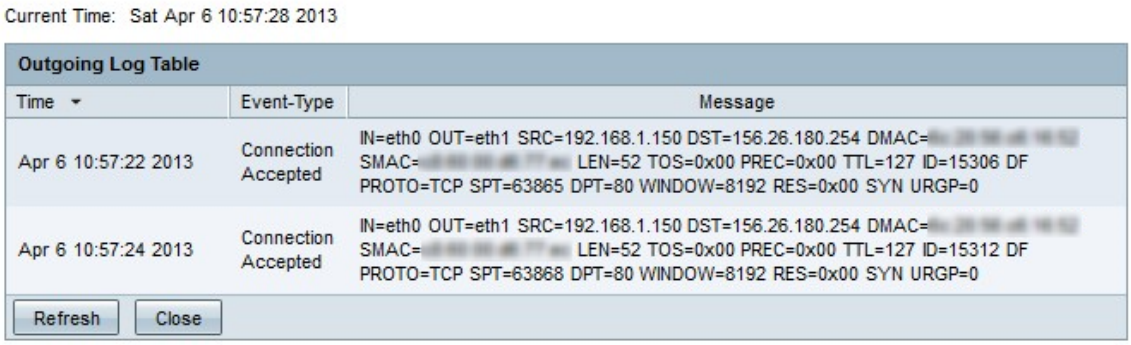
Mensagem — Informações que correspondem ao registro. Isso inclui o tipo de política, o endereço IP origem e o endereço MAC origem.

Note: Clique em **Atualizar** para atualizar a tabela de log.

Exibir tabela de log de saída



Etapa 1. Clique em **Tabela de log de saída** para exibir a tabela de log que se relaciona somente a pacotes de saída. A janela *Outgoing Log Table* é exibida.



A Tabela de log de saída exibe as seguintes informações.

Hora — A hora em que o log foi criado.

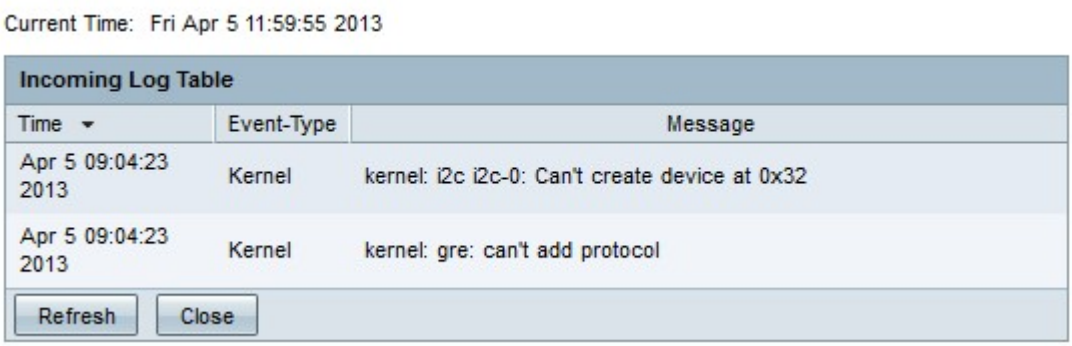
Event-Type — O tipo de log.

Mensagem — Informações que correspondem ao registro. Isso inclui o tipo de política, o endereço IP origem e o endereço MAC origem.

Note: Clique em **Atualizar** para atualizar a tabela de log.

Exibir tabela de log de entrada

Etapa 1. Clique em **Tabela de log de entrada** para exibir a tabela de log que se relaciona somente a pacotes de entrada. A janela *Tabela de log de entrada* é exibida.



A tabela de log de entrada exibe as seguintes informações.

Hora — A hora em que o log foi criado.

Event-Type — O tipo de log.

Mensagem — Informações que correspondem ao registro. Isso inclui o tipo de política, o endereço IP origem e o endereço MAC origem.

Note: Clique em **Atualizar** para atualizar a tabela de log.