Configuração do log do sistema nos roteadores VPN RV016, RV042, RV042G e RV082

Objetivo

Um registro do sistema (Syslog) é usado para registrar dados do computador. Você pode definir as instâncias que gerarão um log. Sempre que uma instância ocorre, a hora e o evento são gravados e enviados para um Servidor syslog ou enviados em um e-mail. O syslog pode então ser usado para analisar e solucionar problemas de uma rede juntamente com o aumento da segurança da rede.

Este documento explica o procedimento para configurar um Servidor Syslog em RV016, RV042, RV042G e RV082 VPN Routers.

Dispositivos aplicáveis

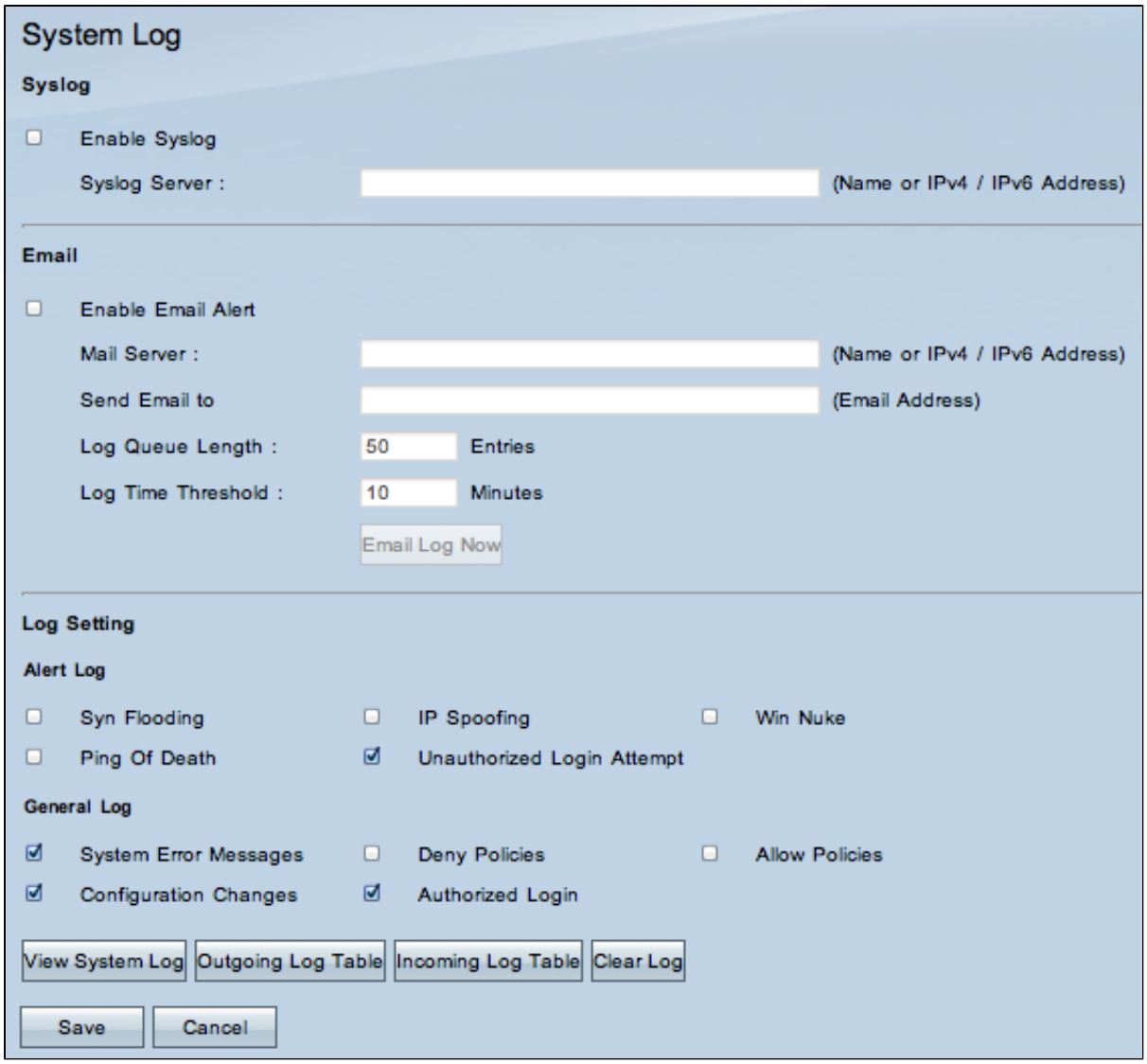
â€¢RV016
â€¢RV042
â€¢RV042G
â€¢RV082

Versão de software

â€¢v4.2.1.02

Configuração de Syslog e Alertas

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Log > System Log**. A página *Log do sistema* será aberta:



Syslog

Esta seção explica como permitir que o roteador envie arquivos de log detalhados ao seu Servidor syslog quando os eventos são registrados.

Etapa 2. Marque a caixa de seleção **Enable Syslog** para habilitar o serviço syslog no dispositivo.

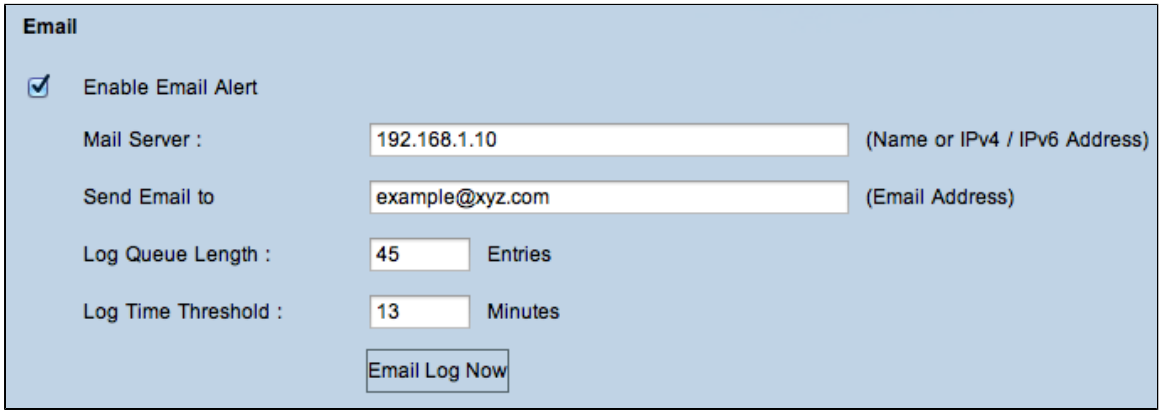
Economizador de tempo: vá para a Etapa 4 se o Syslog precisar ser desabilitado.

Etapa 3. Insira o nome de domínio ou o endereço IP do Servidor syslog no campo Servidor syslog.

E-mail

Esta seção explica como permitir que o roteador envie alertas por e-mail quando os eventos forem

registrados.



Etapa 4. Marque **Ativar alerta por e-mail** para ativar o recurso. Isso permite que o roteador envie alertas de e-mail para o endereço de e-mail especificado pelo usuário.

Economizador de tempo: vá para a Etapa 10 se o alerta por e-mail precisar ser desativado.

Etapa 5. Insira o endereço IPv4 ou IPv6 do servidor SMTP do ISP no campo Mail Server (Servidor de email).

Observação: o ISP pode exigir que você identifique o roteador com um nome de host. Escolha **Setup > Network** para definir o nome do host do roteador.

Etapa 6. Insira o endereço de e-mail para o qual deseja enviar os alertas no campo Enviar e-mail para.

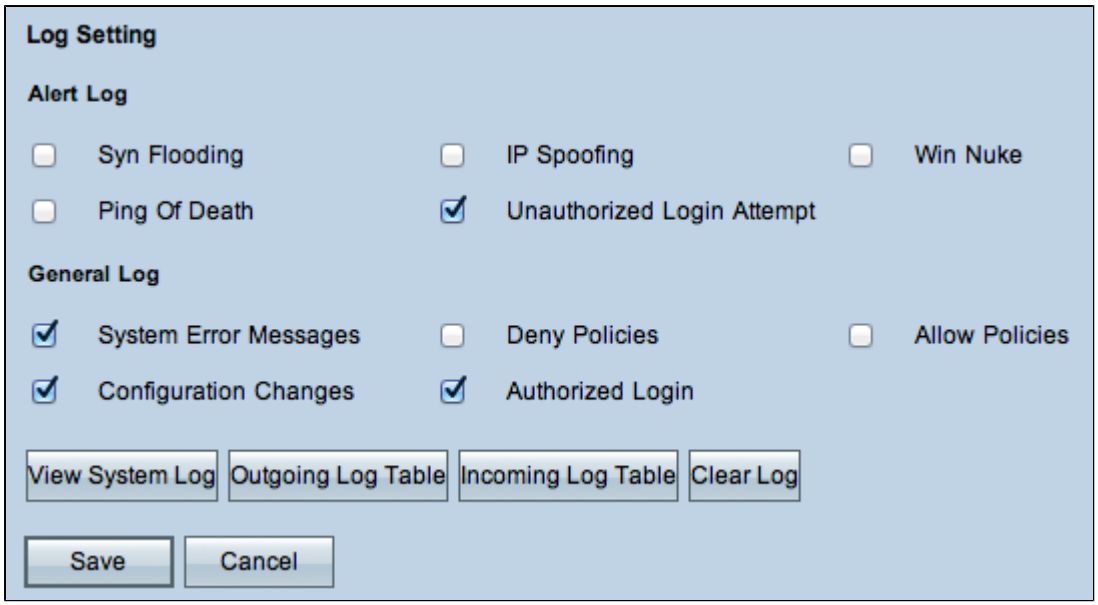
Passo 7. Digite o número de entradas de log a serem incluídas no e-mail no campo Comprimento da fila de log. O padrão é 50.

Etapa 8. Insira o número de minutos para coletar dados antes de enviar o log no campo Limite de tempo de log. O limite de tempo de log é o tempo máximo de espera antes que uma mensagem de log de e-mail seja enviada. Quando o limite de tempo de log expira, um e-mail é enviado independentemente de o buffer de log de e-mail estar cheio ou não. O padrão é 10 minutos

Etapa 9. (Opcional) Clique em **Email Log Now** para enviar instantaneamente uma mensagem para o endereço de e-mail especificado para testar as configurações.

Configuração de Log

Esta seção explica a variedade de eventos que podem ser relatados nos logs:



Etapa 10. A área Registro de alertas contém tipos comuns de ataques e tentativas de login não autenticado. Marque as caixas de seleção de qualquer tipo de ataque desejado para incluí-los no registro de eventos ou desmarque-as para omiti-los do registro de eventos.

· Inundação de SYN â€" O invasor envia vários pacotes SYNC continuamente, o que faz com que o roteador abra várias sessões para que o tráfego fique muito lotado e resulte na negação de tráfego legítimo pelo roteador.

· Falsificação de IP â€" O invasor envia pacotes de um endereço IP de origem falso para fazer com que o ataque pareça tráfego legítimo.

· Win Nuke â€" O invasor envia uma mensagem Fora de Banda a uma máquina Windows para provocar o travamento do computador de destino.

· Ping of Death â€" O invasor envia um grande pacote IP para causar um travamento no computador de destino.

· Tentativa de logon não autorizada â€" Alguém tentou fazer logon no Router Configuration Utility sem a autenticação adequada.

Etapa 11. A área Log geral inclui as ações que são executadas para aplicar políticas configuradas, bem como eventos de rotina, como logins autorizados e alterações de configuração. Marque a caixa de seleção de qualquer evento desejado para incluí-lo no Log geral. Desmarque a caixa de seleção para omiti-la do Log geral.

· Mensagens de erro do sistema â€" Todas as mensagens de erro do sistema.

· Políticas de negação â€" Instâncias em que o roteador negou acesso com base em suas Regras de Acesso.

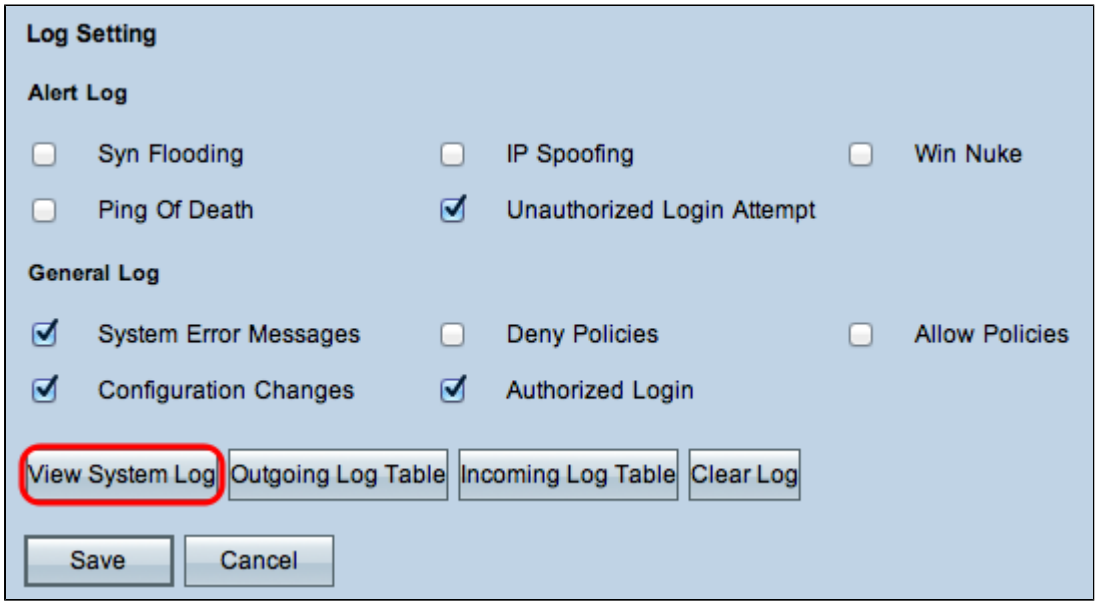
· Allow Policies (Permitir regras) â€" Instâncias em que o roteador permitiu o acesso com base em suas regras de acesso.

· Alterações de configuração â€" Instâncias em que alguém salvou alterações na configuração.

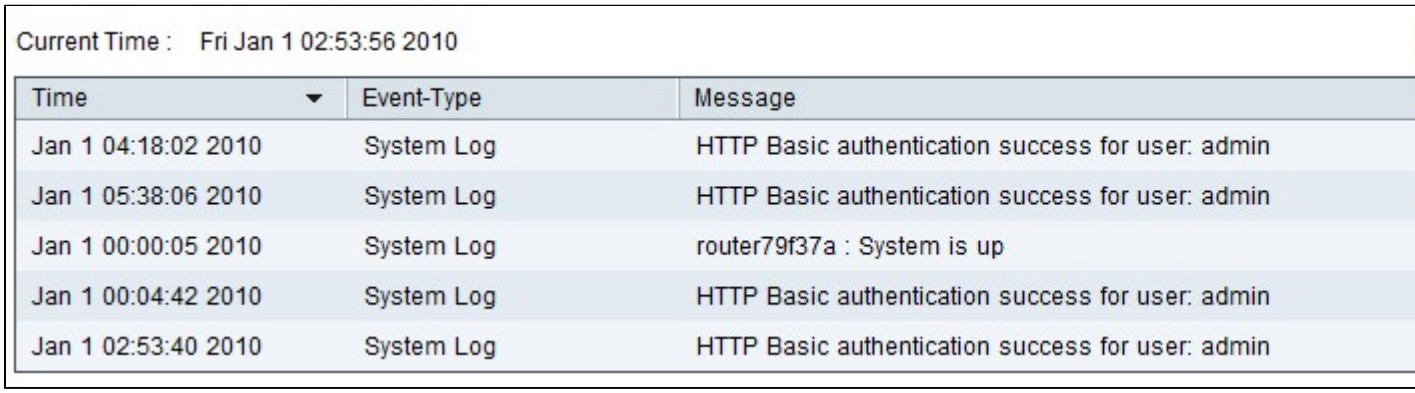
· Login autorizado â€" instâncias em que alguém efetuou login com êxito no utilitário de configuração do roteador após inserir o nome de usuário e a senha corretos.

· Evento de bloqueio de saída â€” instâncias em que há um evento na reputação da Web do ProtectLink ou na filtragem de URLs.

Observação: o evento de bloqueio de saída está disponível somente nos roteadores VPN RV082.



Etapa 12. (Opcional) Para exibir o log do sistema, clique em **Exibir log do sistema**. A janela *Log do sistema* é exibida:



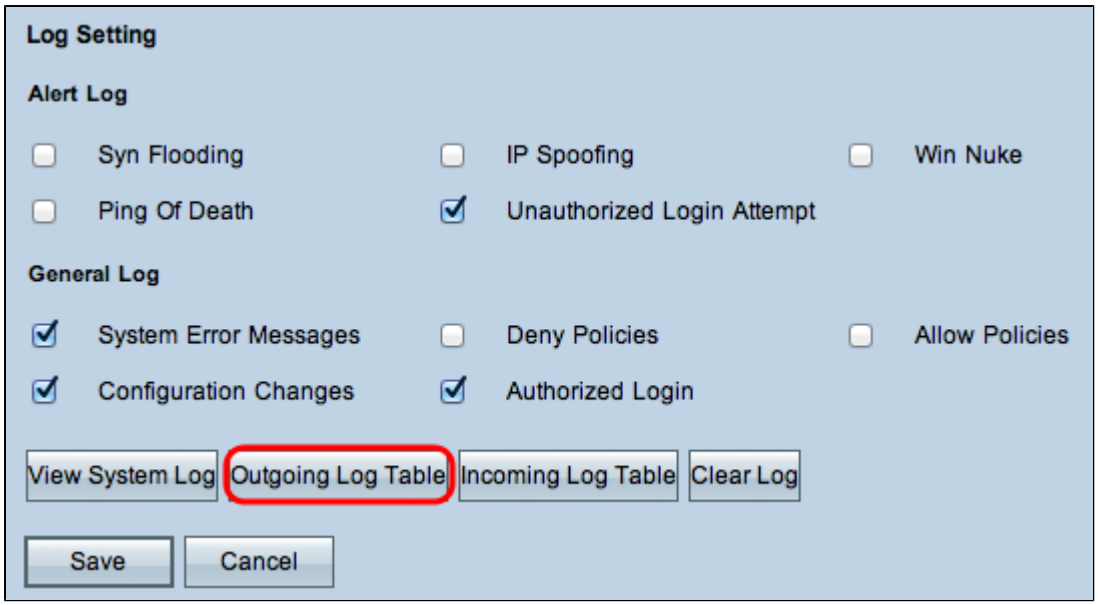
Observação: as entradas de log fornecem a data e a hora do tipo de evento e uma mensagem. Essa mensagem indica o tipo de política, como a regra de acesso, o endereço IP LAN da origem e o endereço MAC.

Etapa 13. Escolha um log específico na lista suspensa.

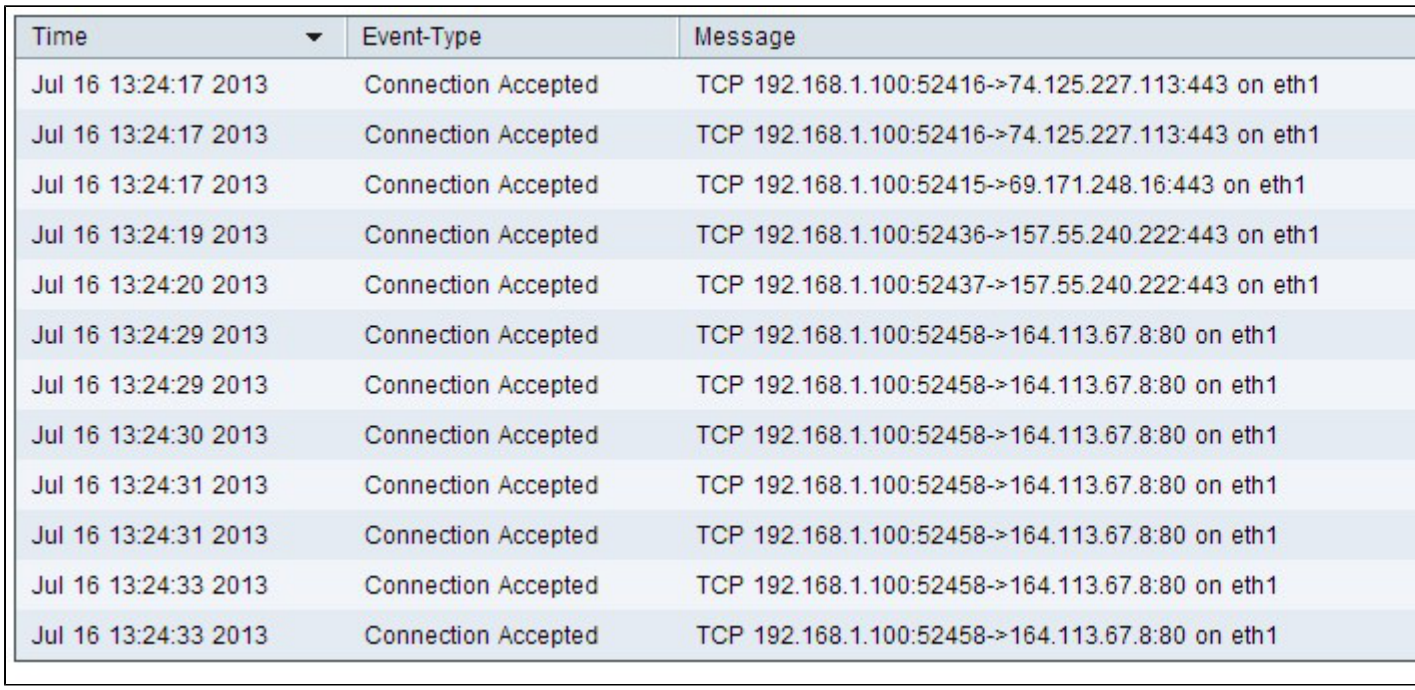
Etapa 14. (Opcional) Para atualizar os dados, clique em **Atualizar**.

Etapa 15. (Opcional) Para apagar todas as informações exibidas, clique em **Limpar**.

Etapa 16. Clique em **Fechar** para fechar a janela.



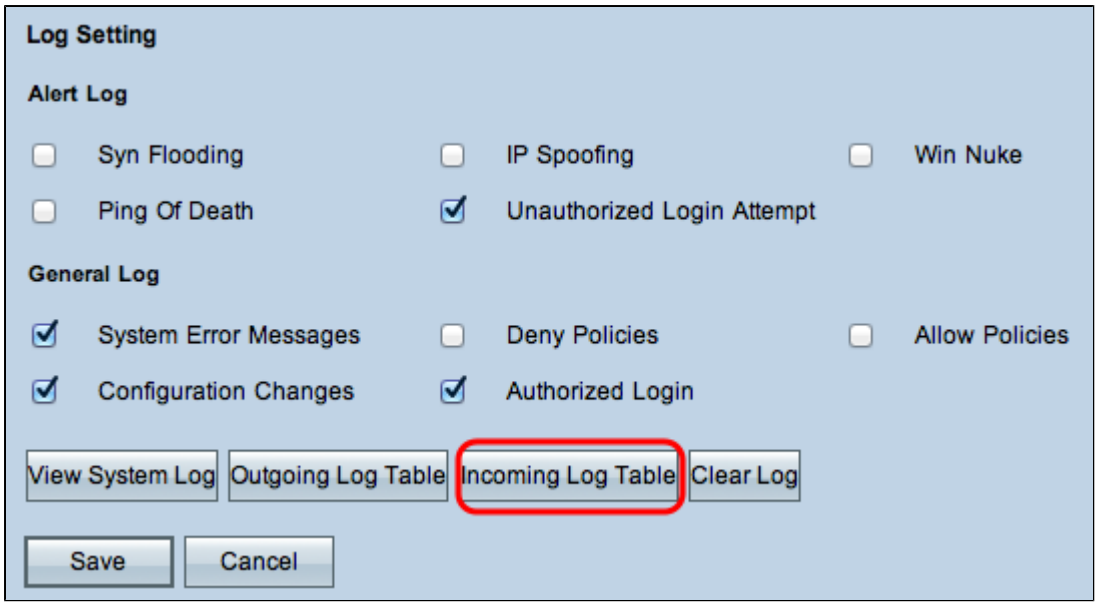
Etapa 17. (Opcional) Para exibir as informações sobre os pacotes de saída, clique em **Outgoing Log Table**. As informações são exibidas em uma nova janela.



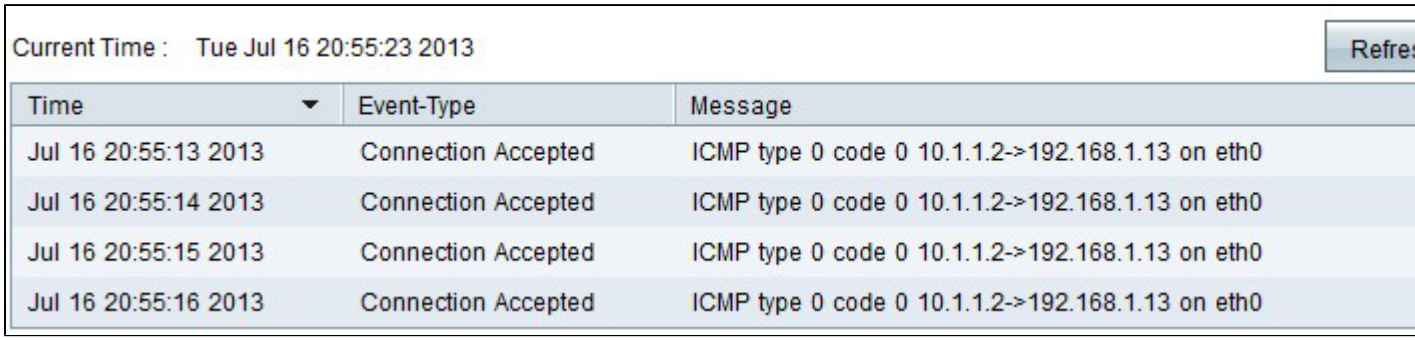
Time	Event-Type	Message
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52415->69.171.248.16:443 on eth1
Jul 16 13:24:19 2013	Connection Accepted	TCP 192.168.1.100:52436->157.55.240.222:443 on eth1
Jul 16 13:24:20 2013	Connection Accepted	TCP 192.168.1.100:52437->157.55.240.222:443 on eth1
Jul 16 13:24:29 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:29 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:30 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:31 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:31 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:33 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:33 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1

Etapa 18. (Opcional) Para atualizar os dados, clique em **Atualizar**.

Etapa 19. Clique em **Fechar** para fechar a janela.

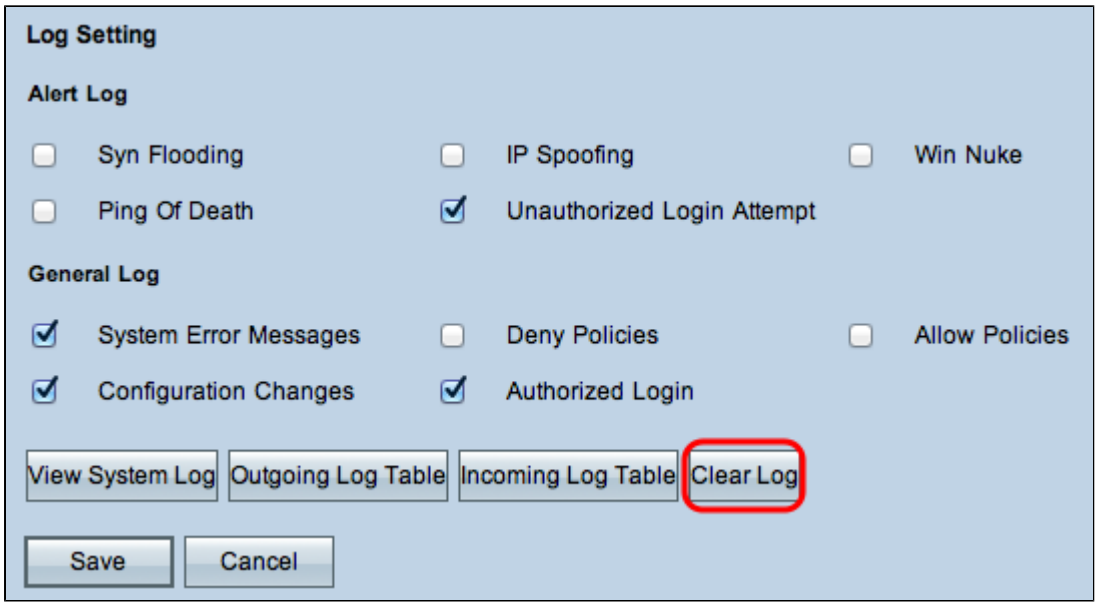


Etapa 20. (Opcional) Clique em **Incoming Log Table** para exibir as informações sobre os pacotes de entrada. As informações são abertas em uma nova janela. Se aparecer um aviso sobre a janela pop-up, permita o conteúdo bloqueado.



Etapa 21. (Opcional) Para atualizar os dados, clique em **Atualizar**.

Etapa 22. Clique em **Fechar** para fechar a janela.



Etapa 23. (Opcional) Para limpar o log, clique em **Clear Log Now**. Clique nesse botão somente se as

informações não precisarem ser exibidas novamente no futuro.

Etapa 24. Clique em **Save** para salvar a configuração.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.