Acessar logs do dispositivo da Web seguro

Contents

Introdução

Este documento descreve os métodos para exibir logs do Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SWA físico ou virtual instalado.
- Licença ativada ou instalada.
- Cliente Secure Shell (SSH).
- O assistente de instalação foi concluído.
- Acesso administrativo ao SWA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Tipos de log SWA

O Secure Web Appliance registra suas próprias atividades de gerenciamento de tráfego e sistema gravando-as em arquivos de log. Os administradores podem consultar esses arquivos de log para monitorar e solucionar problemas do equipamento.

Esta tabela descreve os tipos de arquivo de log do Secure Web Appliance.

Tipo de arquivo de log	Descrição	Suporta envio de syslog?	Ativado por padrão?
Logs do mecanismo de controle de acesso	Registra mensagens relacionadas ao mecanismo de avaliação da ACL (lista de controle de acesso) do Web Proxy.	No	No
Logs do Secure EndpointEngine	Registra informações sobre a verificação da reputação do arquivo e a análise do arquivo (Secure Endpoint.)	Yes	Yes
Logs de auditoria	Registra eventos AAA (Authentication, Authorization, and Accounting). Registra toda a interação do usuário com o aplicativo e as interfaces de linha de comando e captura as alterações confirmadas. Alguns dos detalhes do log de auditoria são os seguintes: • Usuário - Logon • Usuário - falha no logon - senha incorreta • Usuário - falha de logon com nome de usuário desconhecido • Usuário - conta com falha de logon expirada • Usuário - Logoff • Usuário - Bloqueio • Usuário - Ativado • Usuário - Alteração de senha • Usuário - Redefinição de senha • Usuário - Configurações de segurança/alteração de perfil	Yes	Yes

Tipo de arquivo de log	Descrição	Suporta envio de syslog?	Ativado por padrão?
	• Usuário - Criado • Usuário - Excluído/modificado • Grupo/Função - Exclusão/Modificado • Grupo /Função - Alteração de permissões		
Logs de acesso	Registra o histórico do cliente do Web Proxy.	Yes	Yes
Logs de estrutura do mecanismo ADC	Registra mensagens relacionadas à comunicação entre o Web Proxy e o mecanismo ADC.	No	No
Logs do mecanismo ADC	Registra mensagens de depuração do mecanismo ADC.	Yes	Yes
Logs de Estrutura de Autenticação	Registra mensagens e histórico de autenticação.	No	Yes
Logs de estrutura do AVC Engine	Registra mensagens relacionadas à comunicação entre o Web Proxy e o mecanismo AVC.	No	No
Logs do AVC Engine	Registra mensagens de depuração do mecanismo AVC.	Yes	Yes
Logs de auditoria CLI	Registra uma auditoria histórica da atividade da interface de linha de comando.	Yes	Yes
Logs de configuração	Registra mensagens relacionadas ao sistema de gerenciamento de configuração do Web Proxy.	No	No
Logs de Gerenciamento de Conexões	Registra mensagens relacionadas ao sistema de gerenciamento de conexões do Web Proxy.	No	No

Tipo de arquivo de log	Descrição	Suporta envio de syslog?	Ativado por padrão?
Logs de segurança de dados	Registra o histórico do cliente para solicitações de upload que são avaliadas pelos Filtros de Segurança de Dados da Cisco.	Yes	Yes
Logs do módulo de segurança de dados	Registra mensagens relacionadas aos Filtros de Segurança de Dados da Cisco.	No	No
Logs de Estrutura do Mecanismo de DCA (Análise de conteúdo dinâmico)	Registra mensagens relacionadas à comunicação entre o Web Proxy e o mecanismo de Análise de Conteúdo Dinâmico dos Controles de Uso da Web da Cisco.	No	No
Logs do mecanismo de DCA (Análise de conteúdo dinâmico)	Registra mensagens relacionadas ao mecanismo de análise de conteúdo dinâmico dos controles de uso da Web da Cisco.	Yes	Yes
Logs de proxy padrão	Registra erros relacionados ao Web Proxy. Este é o mais básico de todos os logs relacionados ao Web Proxy. Para solucionar problemas mais específicos relacionados ao Web Proxy, crie uma assinatura de log para o módulo do Web Proxy aplicável.	Yes	Yes
Logs do Gerenciador de Discos	Registra mensagens do Web Proxy relacionadas à gravação no cache do disco.	No	No
Logs de autenticação externa	Registra mensagens relacionadas ao uso do recurso de autenticação externa, como êxito de comunicação ou falha com o servidor de autenticação externo.	No	Yes

Tipo de arquivo de log	Descrição	Suporta envio de syslog?	Ativado por padrão?
	Mesmo com a autenticação externa desabilitada, esse log contém mensagens sobre usuários locais que tiveram êxito ou falharam ao fazer login.		
Logs de feedback	Registra os usuários da Web que relatam páginas mal classificadas.	Yes	Yes
Logs de Proxy FTP	Registra mensagens de erro e de aviso relacionadas ao Proxy FTP.	No	No
Logs do servidor FTP	Registra todos os arquivos carregados e baixados doSecure Web Appliance usando o FTP.	Yes	Yes
Logs de GUI (Interface Gráfica do Usuário)	Registra o histórico de atualizações de página na interface da Web do . Os logs de GUI também incluem informações sobre transações SMTP, por exemplo, informações sobre relatórios agendados enviados por e-mail do dispositivo.	Yes	Yes
Logs Haystack	Os logs Haystack registram o processamento de dados de rastreamento de transação da Web.	Yes	Yes
Logs HTTPS	Registra mensagens do Web Proxy específicas do Proxy HTTPS (quando o Proxy HTTPS está habilitado).	No	No
Logs do servidor ISE	Registra informações operacionais e de conexão do(s) servidor(es) ISE.	Yes	Yes
Logs do módulo de licença	Registra mensagens relacionadas ao sistema de tratamento de chave de recurso e licença do Web Proxy.	No	No
Logs da Estrutura de Log	Registra mensagens relacionadas ao sistema de log do Web Proxy.	No	No
Logs de registro	Registra erros relacionados ao gerenciamento de logs.	Yes	Yes

Tipo de arquivo de log	Descrição	Suporta envio de syslog?	Ativado por padrão?
Logs da Estrutura de Integração da McAfee	Registra mensagens relacionadas à comunicação entre o Web Proxy e o mecanismo de varredura da McAfee.	No	No
Logs McAfee	Registra o status da atividade de varredura antimalware do mecanismo de varredura da McAfee.	Yes	Yes
Logs do gerenciador de memória	Registra mensagens do Web Proxy relacionadas ao gerenciamento de toda a memória, incluindo o cache na memória para o processo do Web Proxy.	No	No
Logs de módulos de proxy diversos	Registra mensagens do Web Proxy que são usadas principalmente por desenvolvedores ou pelo suporte ao cliente.	No	No
Logs do daemon do AnyConnect Secure Mobility	Registra a interação entre oSecure Web Appliance e o cliente AnyConnect, incluindo a verificação de status.	Yes	Yes
Logs NTP (Protocolo de tempo de rede)	Registra as alterações na hora do sistema feitas pelo Network Time Protocol.	Yes	Yes
Logs daemon de hospedagem de arquivo PAC	Registra o uso do arquivo PAC (autoconfig) por clientes.	Yes	Yes
Logs de desvio de proxy	Registra transações que ignoram o Web Proxy.	No	Yes
Logs de relatório	Registra um histórico da geração de relatórios.	Yes	Yes
Logs de Consulta de Relatórios	Registra erros relacionados à geração de relatórios.	Yes	Yes

Tipo de arquivo de log	Descrição	Suporta envio de syslog?	Ativado por padrão?
Solicitar Logs de Depuração	Registra informações de depuração muito detalhadas em uma transação HTTP específica de todos os tipos de log do módulo Web Proxy. É aconselhável criar essa inscrição de log para solucionar um problema de proxy com uma transação específica sem criar todas as outras inscrições de log de proxy. Nota:Você pode criar essa inscrição de log somente na CLI.	No	No
Logs de autenticação	Registra mensagens relacionadas ao recurso Controle de Acesso.	Yes	Yes
Logs SHD (Daemon de Integridade do Sistema)	Registra um histórico da integridade dos serviços do sistema e um histórico de reinicializações inesperadas do daemon.	Yes	Yes
Logs SNMP	Registra mensagens de depuração relacionadas ao mecanismo de gerenciamento de rede SNMP.	Yes	Yes
Logs do módulo SNMP	Registra mensagens do Web Proxy relacionadas à interação com o sistema de monitoramento SNMP.	No	No
Logs de estrutura de integração do Sophos	Registra mensagens relacionadas à comunicação entre o Web Proxy e o mecanismo de verificação Sophos.	No	No
Logs Sophos	Registra o status da atividade de verificação antimalware do mecanismo de verificação Sophos.	Yes	Yes
Logs de status	Registra informações relacionadas ao sistema, como downloads de chave de recurso.	Yes	Yes
Registros de sistema	Registra DNS, erro e atividade de confirmação.	Yes	Yes

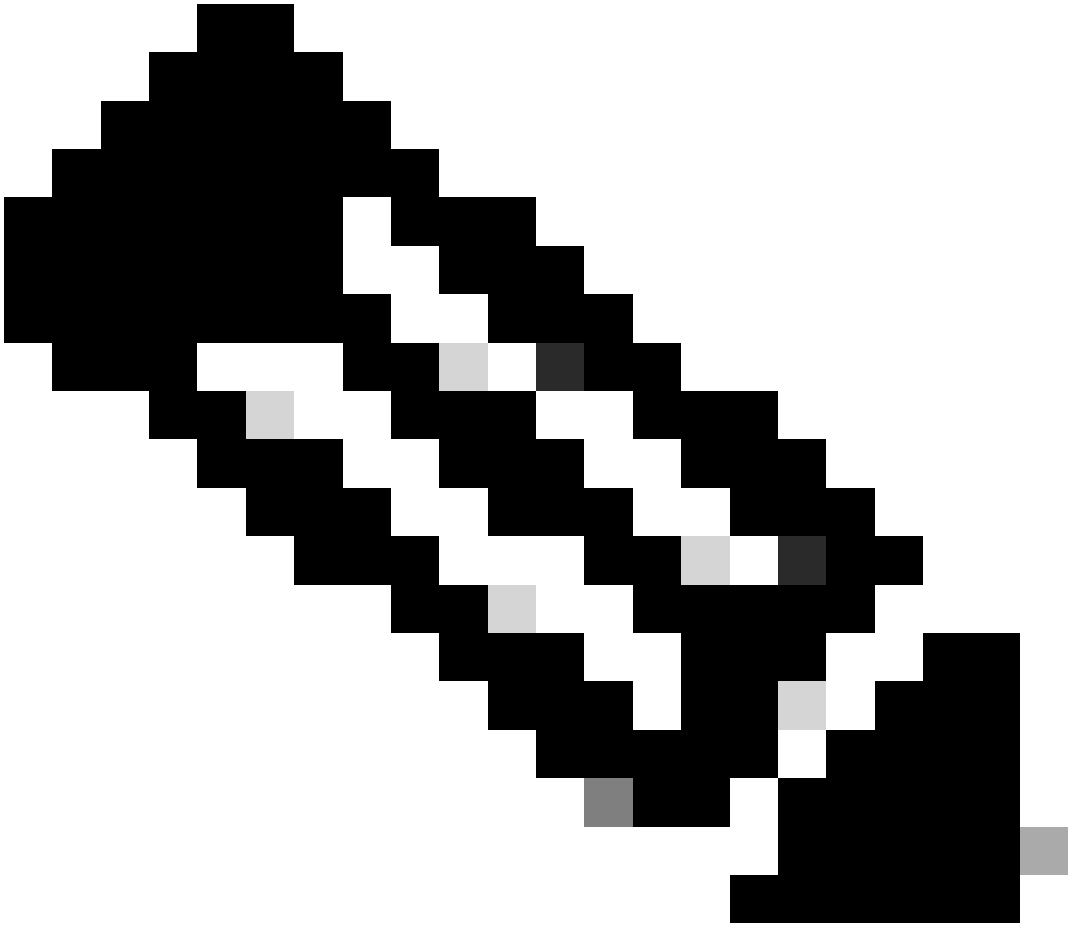
Tipo de arquivo de log	Descrição	Suporta envio de syslog?	Ativado por padrão?
Logs de erro do monitor de tráfego	Registra a interface L4TM e captura erros.	Yes	Yes
Logs do monitor de tráfego	Registra sites adicionados ao bloco L4TM e às listas de permissão.	No	Yes
Logs UDS (Serviço de descoberta de usuário)	Registra dados sobre como o Web Proxy descobre o nome de usuário sem fazer a autenticação real. Ele inclui informações sobre como interagir com o aplicativo de segurança adaptável da Cisco para o Secure Mobility, bem como integrar com o servidor Novell eDirectory para identificação transparente de usuário.	Yes	Yes
Logs do Atualizador	Registra um histórico de WBRS e outras atualizações.	Yes	Yes
Logs W3C	Grava o histórico do cliente Web Proxy em um formato compatível com W3C. Para obter mais informações.	Yes	No
Logs WBNP (Participação de rede SensorBase)	Registra um histórico de uploads de participação da rede Cisco SensorBase para a rede SensorBase.	No	Yes
Logs da Estrutura WBRS (Pontuação do Web Reputation)	Registra mensagens relacionadas à comunicação entre o Web Proxy e os Filtros do Web Reputation.	No	No
Logs do módulo WCCP	Registra mensagens do Web Proxy relacionadas à implementação do WCCP.	No	No
Logs da Estrutura de Integração do	Registra mensagens relacionadas à comunicação entre o Web Proxy e o mecanismo de filtragem de URL	No	No

Tipo de arquivo de log	Descrição	Suporta envio de syslog?	Ativado por padrão?
Webcat	associado aos Controles de uso da Web da Cisco.		
Logs da Estrutura de Integração do Webroot	Registra mensagens relacionadas à comunicação entre o Web Proxy e o mecanismo de varredura do Webroot.	No	No
Logs do Webroot	Registra o status da atividade de varredura antimalware do mecanismo de varredura Webroot.	Yes	Yes
Logs de confirmação da página de boas-vindas	Registra um histórico de clientes da Web que clicam no botão Aceitar na página de reconhecimento do usuário final.	Yes	Yes

Exibir logs

Por padrão, os logs são armazenados localmente no SWA, você pode baixar os arquivos de log armazenados localmente via GUI ou exibir os logs da CLI.

Fazer download de arquivos de log via GUI



Observação: o FTP deve ser habilitado no equipamento. Para habilitar o FTP, consulte Enable FTP on Secure Web Appliance neste artigo.

Você pode fazer download dos arquivos de log da GUI:

Etapa 1. Fazer login na GUI

Etapa 2. Navegue até Administração do sistema

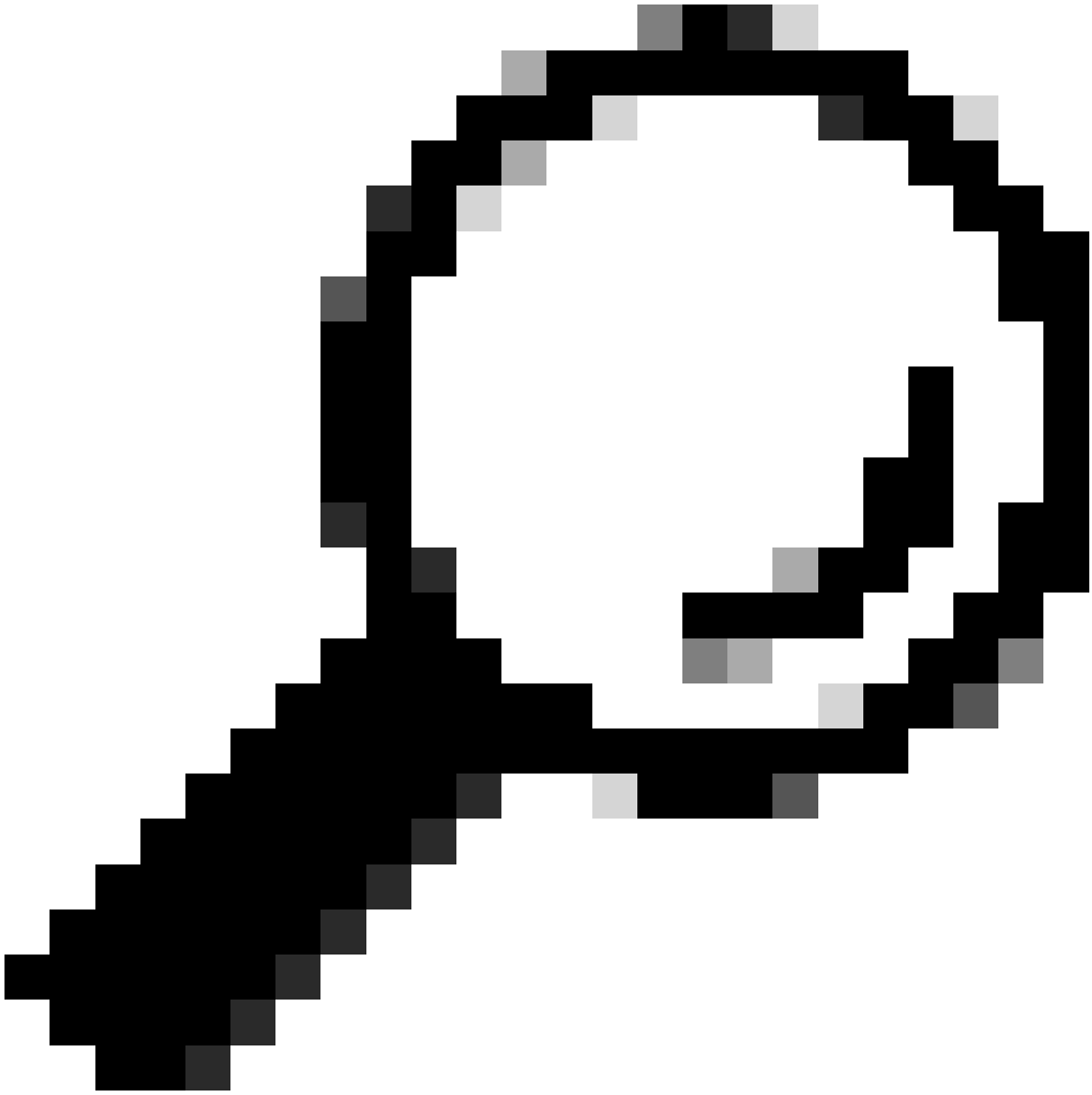
Etapa 3. Escolher Inscrições de Log

Etapa 4.Clique no nome da inscrição de log na coluna Arquivos de log da lista de inscrições de log.

Etapa 5.Quando solicitado, insira o nome de usuário e a senha do administrador para acessar o equipamento.

Etapa 6.Quando estiver conectado, clique em um dos arquivos de log para exibi-lo em seu

navegador ou para salvá-lo em disco.



Dica: atualize o navegador para obter resultados atualizados.

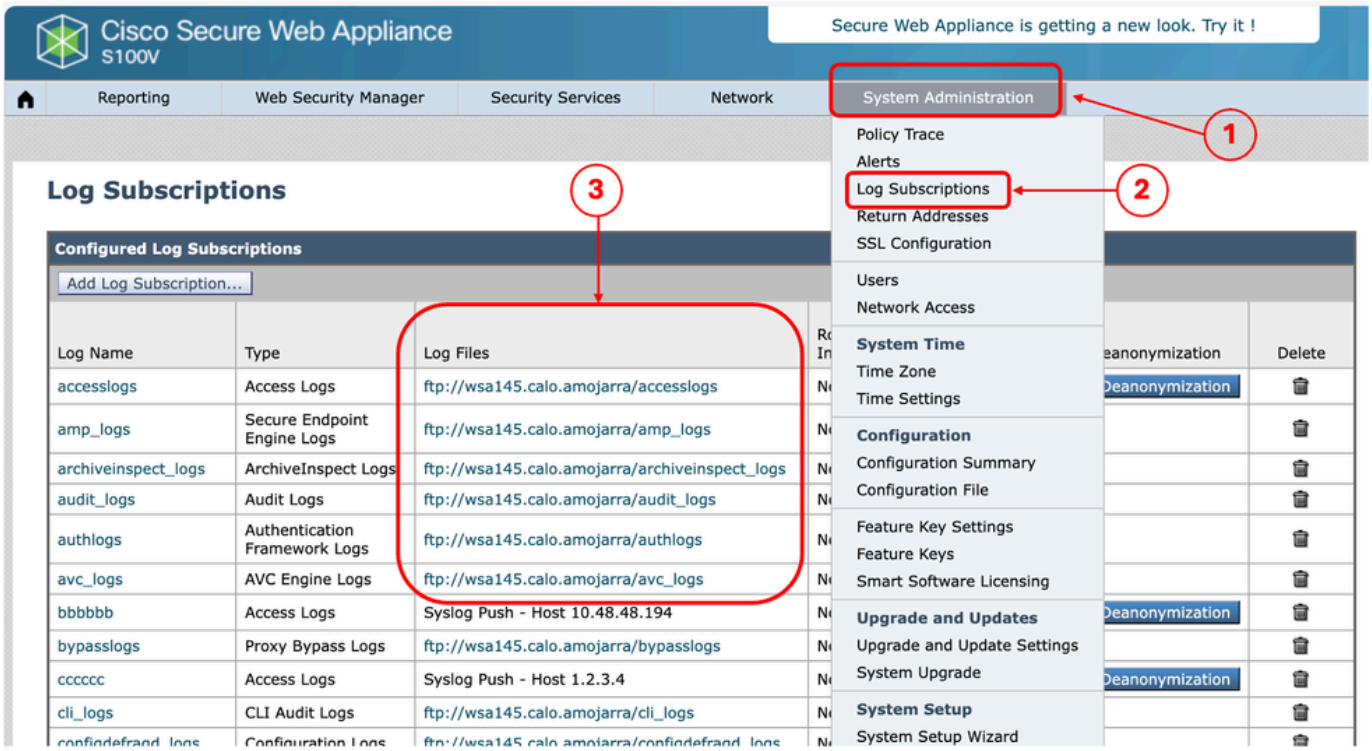
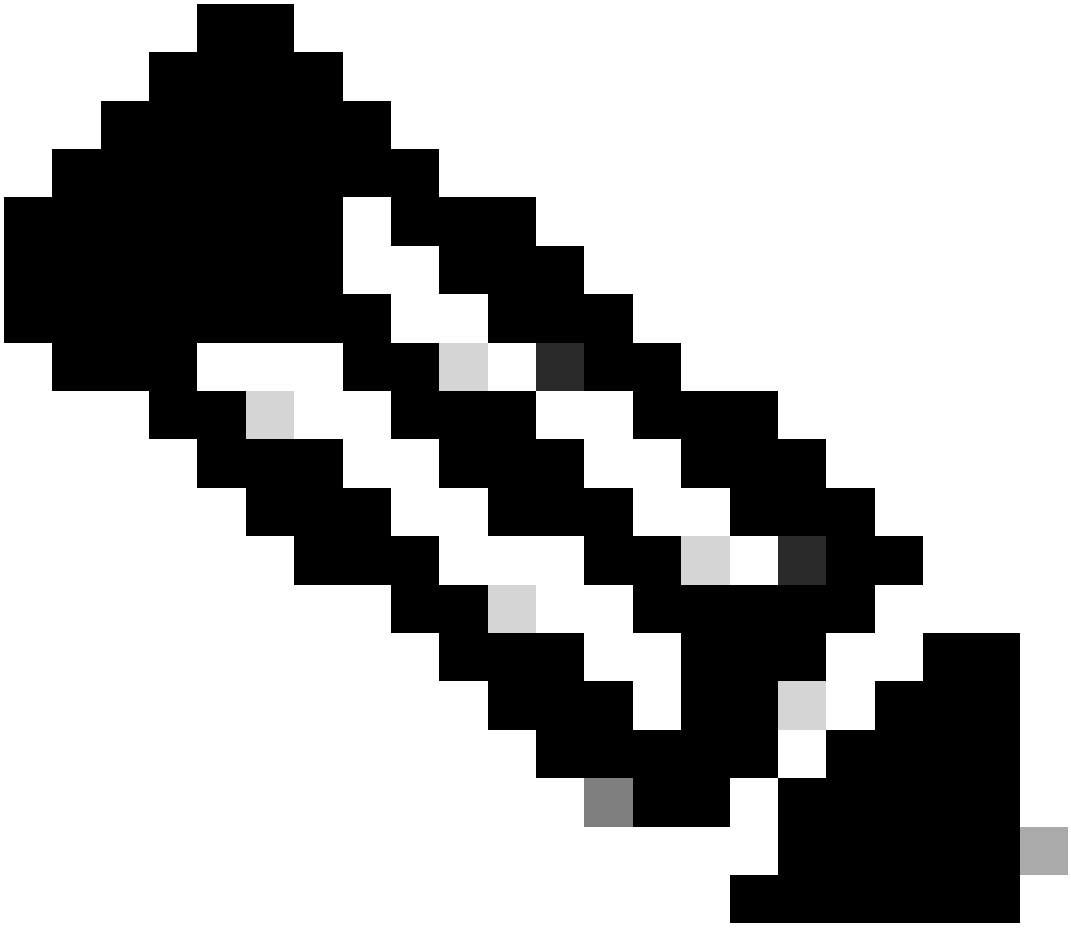


Imagem - Baixar arquivos de log



Observação: se uma inscrição de log for compactada, baixe, descompacte e abra-a.

Exibir logs do CLI

Você pode exibir os logs na CLI. Nesse caso, você pode ter acesso a logs dinâmicos ou filtrar uma palavra-chave nos logs.

Etapa 1. Conectar-se à CLI

Etapa 2. Digite grep e pressione enter.

Etapa 3. Digite o número do log que deseja exibir

Etapa 4. (Opcional) você pode filtrar a saída definindo uma Expressão Regular ou uma palavra; caso contrário, pressione Enter

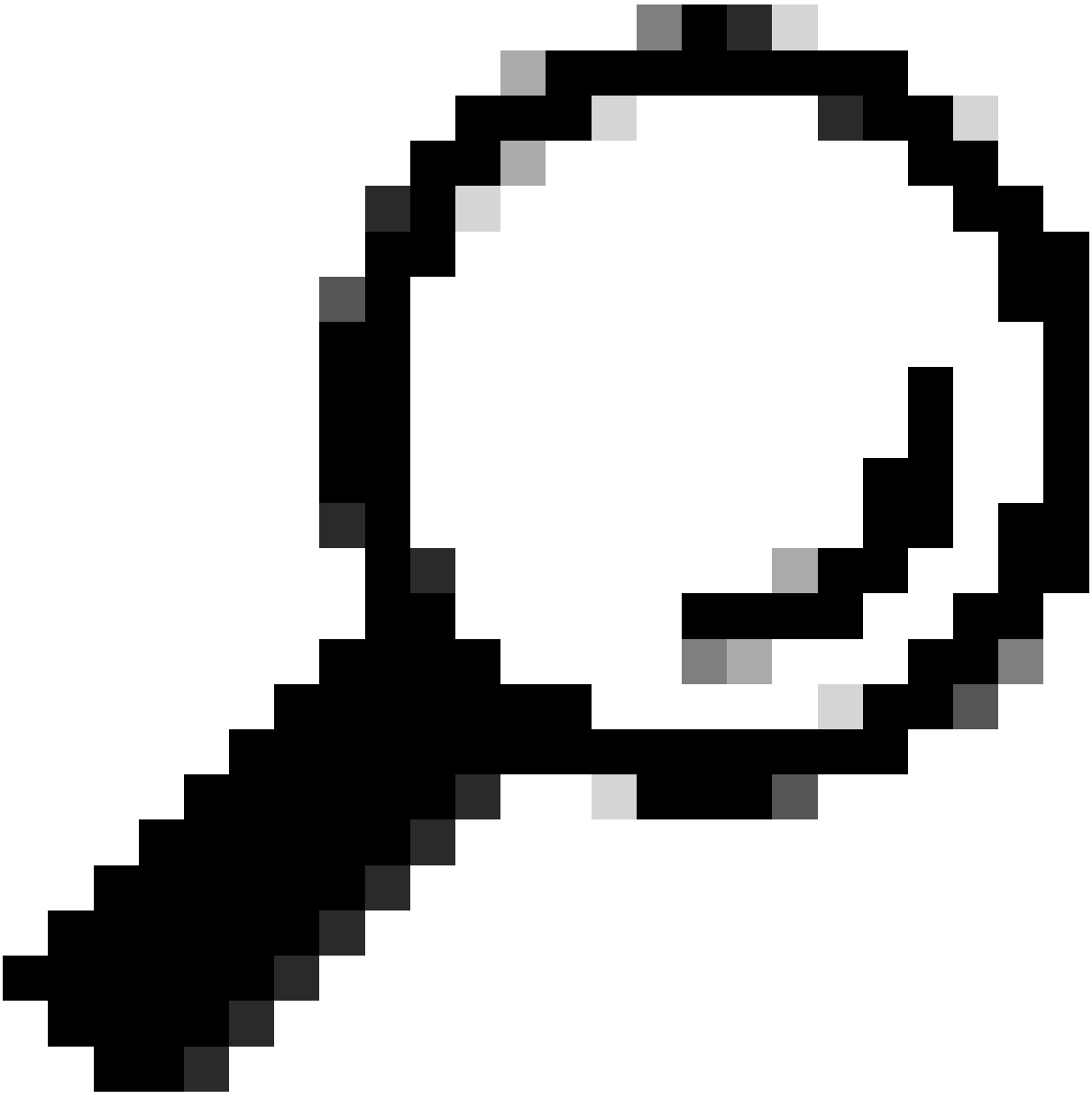
Etapa 5. Se precisar pesquisar a palavra-chave digitada na Etapa 4, para não diferenciar maiúsculas de minúsculas, pressione enter em "Deseja que essa pesquisa não diferencie

maiúsculas de minúsculas? [Y]>" digite "N" e pressione Enter.

Etapa 6. Se você precisar isentar sua palavra-chave da pesquisa, digite "Y" em "Deseja procurar linhas não correspondentes? [N]>" ou pressione Enter.

Passo 7. Se precisar exibir logs dinâmicos, digite "Y" em "Deseja encerrar os logs? [N]>", ou pressione Enter.

Etapa 8. Se quiser paginar os logs para exibi-los página por página, digite "Y" em "Deseja paginar a saída? [N]>", ou pressione Enter.



Dica: se você optar por paginar, poderá sair dos logs pressionando "q"

Aqui está um exemplo de saída que mostra todas as linhas com "Aviso":

```
SWA_CLI> grep

Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "Secure Endpoint Engine Logs" Retrieval: FTP Poll
3. "archiveinspect_logs" Type: "ArchiveInspect Logs" Retrieval: FTP Poll
4. "audit_logs" Type: "Audit Logs" Retrieval: FTP Poll
5. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
6. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
7. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
8. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
...
45. "upgrade_logs" Type: "Upgrade Logs" Retrieval: FTP Poll
46. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
47. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
48. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
49. "webtapd_logs" Type: "Webtapd Logs" Retrieval: FTP Poll
50. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 40

Enter the regular expression to grep.
[]> Warning

Do you want this search to be case insensitive? [Y]>

Do you want to search for non-matching lines? [N]>

Do you want to tail the logs? [N]>

Do you want to paginate the output? [N]>
```

Habilitar FTP no aplicativo da Web seguro

Por padrão, o FTP não está habilitado no SWA. Para ativar o FTP:

Etapa 1. Fazer login na GUI

Etapa 2. Navegue até Rede

Etapa 3. Escolher interfaces

Etapa 4. Clique em Edit Settings.

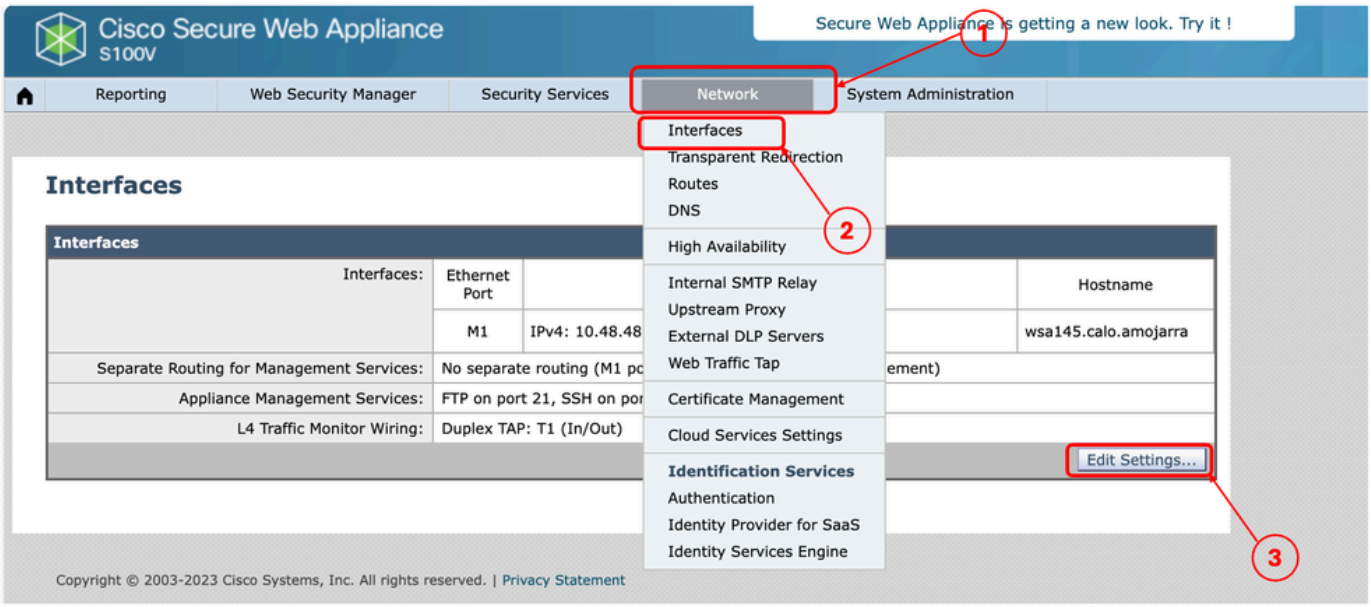


Imagem - Habilitar FTP em SWA

Etapa 5. Marque a caixa de seleção para FTP

Etapa 6. Forneça o número da porta TCP para FTP (a porta FTP padrão é 21)

Passo 7. Enviar e confirmar alterações

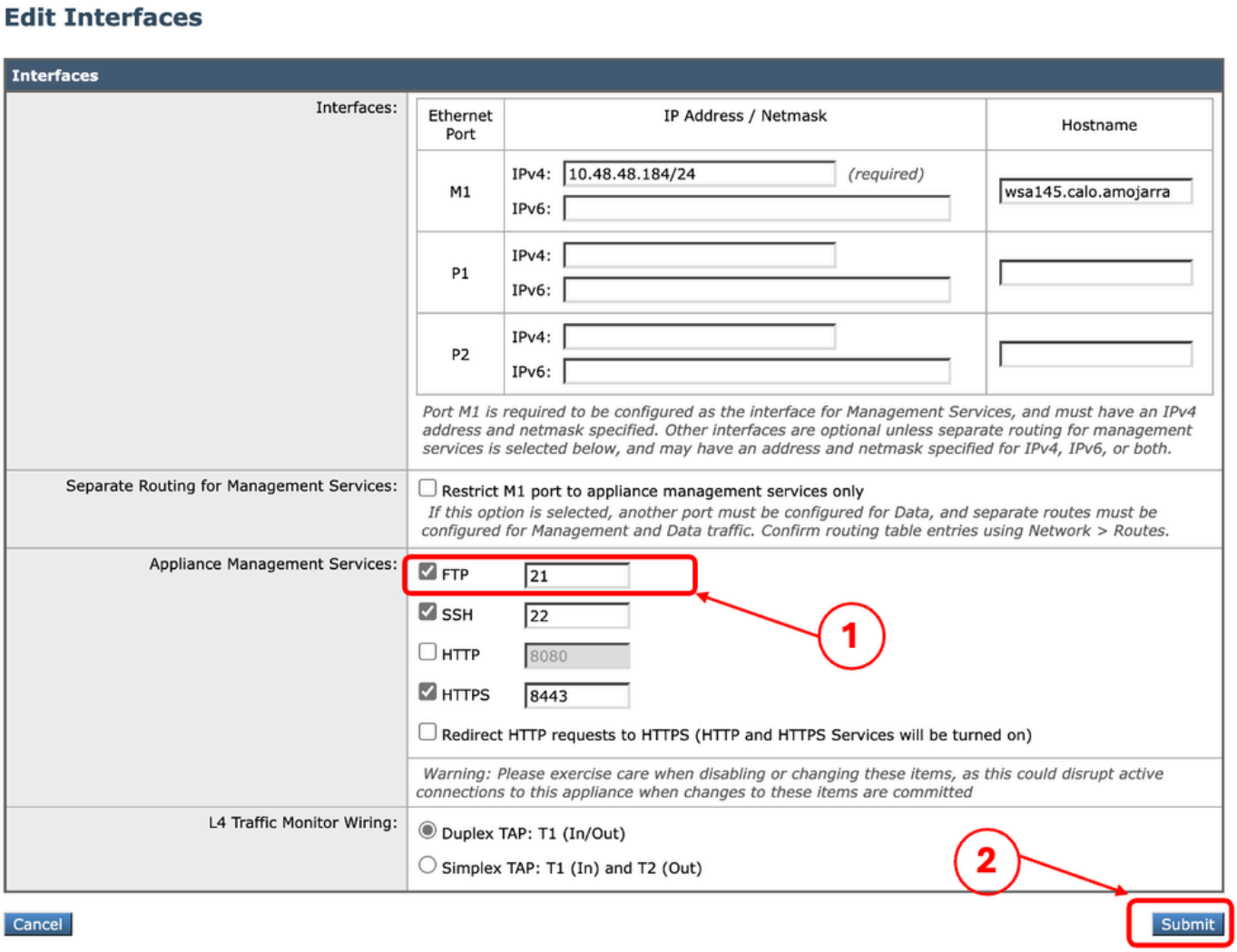


Imagem - Configurar parâmetro FTP em SWA

Informações Relacionadas

- Guia do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance - LD (implantação limitada) - Solução de problemas...
- Configurar logs de envio de SCP no Secure Web Appliance com o Microsoft Server - Cisco

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.