Verificando a descriptografia de IPS no Cisco Secure Access

Contents

Problema

Ao usar o Cisco Secure Access com RAVPN (Remote Access VPN) através do Secure Client, as organizações precisam verificar se a descriptografia e a inspeção do IPS (Sistema de prevenção de intrusão) estão sendo executadas corretamente para o tráfego para sites específicos. O principal desafio é confirmar que os processos de descriptografia e inspeção de TLS estão funcionando corretamente por meio de métodos diferentes dos logs de IU de gerenciamento padrão, como Pesquisa de atividade. Os requisitos específicos de verificação incluem a identificação de verificações de certificado do lado do cliente ou mecanismos de depuração/relatório que possam suportar a validação de teste e fornecer confirmação adicional da operação do IPS além da interface de gerenciamento.

Ambiente

- Cisco Secure Access (CSA) com funcionalidade RAVPN
- Cisco Secure Client para conexões VPN de acesso remoto
- Recursos de inspeção e descriptografia de IPS habilitados
- Tráfego TLS/SSL que requer descriptografia para inspeção de segurança
- Tráfego da Web de clientes RAVPN para sites externos

Resolução

Há dois métodos para verificar se a descriptografia e a inspeção de IPS estão funcionando corretamente para o tráfego de VPN de acesso remoto no Cisco Secure Access:

Método 1: Pesquisa de Atividade de UI de Gerenciamento (Método Principal)

O recurso Activity Search (Pesquisa de atividade) na interface de gerenciamento do Cisco Secure Access fornece o método mais confiável para confirmar as operações de decodificação e inspeção do IPS. Essa interface exibe logs e análises detalhados que mostram quando o tráfego foi descriptografado e inspecionado pelos serviços de segurança.

Para acessar a Pesquisa de atividades:

Navegue até o painel de gerenciamento do Cisco Secure Access e localize a funcionalidade Activity Search para revisar os logs de inspeção de tráfego e o status de descriptografia para sessões de usuário específicas e sites de destino.

Para habilitar logs de descriptografia, esta configuração pode ser habilitada nas configurações globais:

Painel -> Seguro -> Política de acesso -> Padrões de regra e Configurações globais -> Configurações globais -> Registro de descriptografia.

Método 2: Verificação de certificado do lado do cliente

Como um método de verificação adicional, você pode executar verificações de certificado do lado do cliente para confirmar se a descriptografia do tráfego está ocorrendo.

Quando o Cisco Secure Access descriptografa e inspeciona com sucesso o tráfego TLS, ele apresenta seu próprio certificado ao cliente em vez do certificado original do site.

Para verificar a descriptografia por meio da inspeção de certificado:

1. Verifique o Certificado do Site
Abra os detalhes do certificado no navegador e revise o emissor e o período de validade.

Se o certificado for emitido pela CA raiz de acesso seguro da Cisco com um período de validade de ~10 dias, ele indicará a descriptografia do sistema de prevenção de intrusão no nível do firewall.

Se a validade do certificado for de aproximadamente 5 dias, ela indicará a descriptografia

baseada no Secure Web Gateway.

2. Validar o Emissor do Certificado (Nomeação DC)

Este método de verificação de certificado do lado do cliente serve como uma técnica de confirmação suplementar junto com o método de pesquisa de atividade principal, fornecendo garantia adicional de que os processos de descriptografia de IPS estão funcionando conforme esperado.

Sistema de prevenção de intrusão não descriptografar:

A descriptografia para o sistema de prevenção contra invasões ocorrerá se -

· Está ativado em configurações globais E

· O Sistema de prevenção contra invasões está habilitado para pelo menos uma das regras da política de acesso (acredito que, embora a regra esteja desabilitada, essa condição ainda se aplica)

Desejar ignorar um domínio da descriptografia do Sistema de prevenção contra invasões

Use o sistema fornecido não descriptografar a lista e adicionar o domínio no sistema fornecido não descriptografar a lista.

or

Utilize a descriptografia baseada na origem em Configurações globais no acesso Cisco Secure -

NOTA:Isso funcionará se NÃO houver NAT de saída configurado na configuração do túnel de rede no acesso seguro.

Causa

A necessidade de vários métodos de verificação surge da necessidade de validar a aplicação de políticas de segurança em ambientes corporativos. Embora os logs de UI de gerenciamento

forneçam visibilidade abrangente, os métodos de verificação do lado do cliente oferecem pontos de confirmação adicionais que podem ser úteis para testes de conformidade, solução de problemas e cenários de validação onde o acesso direto às interfaces de gerenciamento pode ser limitado ou quando vários pontos de verificação são necessários para procedimentos de teste completos.

Conteúdo relacionado

- Suporte técnico e downloads da 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.