Cisco Secure Services Client e Cisco Trust Agent em um ambiente do Cisco Network Admission Control

Índice

Introdução

Este documento descreve como configurar fixa o cliente dos serviços com Cisco Trust Agent (CTA) em um ambiente do Network Admission Control (NAC).

Pré-requisitos

Componentes Utilizados

Esta seção alista as versões de software usadas neste documento.

- Versão 4.0 do Cisco Secure Services ClientO Cisco Secure Services Client está disponível para a transferência do centro de software de Cisco.com (clientes registrados somente).
- Versão 2.0.0.30 ou mais recente do Cisco Trust Agent (sem suplicante)O Cisco Trust Agent está disponível para a transferência do centro do software da Cisco.com (clientes registrados somente).

Convenções

Para obter mais informações sobre das convenções de documento, refira convenções dos dicas técnicas da Cisco.

Configurar o Cisco Secure Services Client com CTA em um ambiente NAC

O ambiente de Cisco NAC é um programa com vários sócios projetado limitar dano causado por vírus e por worms. A fim controlar o acesso de rede, o NAC monitora dispositivos de rede para

assegurar-se de que sigam com as políticas de segurança de rede. O Cisco Secure Services Client e o CTA são componentes centrais do ambiente NAC. Cada dispositivo que procura o acesso de rede contacta um dispositivo do acesso de rede (roteador, interruptor, concentrador VPN, ou Firewall). Estes dispositivos exigem credenciais da Segurança de terminal com o Cisco Secure Services Client e o CTA. Esta informação é retransmitida aos servidores da política a fim permitir ou negar a admissão à rede.

Nota: O CTA deve ser instalado em todos os anfitriões que exigem a validação para o acesso de rede.

O CTA permite o aplicativo NAC determinar se os produtos de software necessários do sócio, tais como o antivírus, são instalados e corrente. O CTA igualmente determina níveis atuais do sistema operacional e da correção de programa.

Os recursos chaves e os benefícios do CTA incluem:

- O agente sem intrusão pequeno que atua como um componente do middleware e firmemente comunica a informação sobre a política do host ao servidor da política do Authentication, Authorization, and Accounting (AAA) com um suplicante do 802.1X tal como o Cisco Secure Services Client. O CTA pode comunicar a Segurança de Cisco, sistema operacional, e versões da correção de programa, assim como a versão de todo o software do sócio.
- Interage diretamente com os aplicativos NAC-permitidos que são executado no host sem intervenção de usuário. O CTA comunica-se com os aplicativos NAC-permitidos através dos canais de comunicação integrados pelos Parceiros NAC dentro de seus aplicativos.

Para estabelecer o ambiente NAC com Cisco Secure Services Client e CTA, termine estas etapas:

1. Transfira e instale o Cisco Secure Services Client e aplicativos CTA.
2. Transfira e instale aplicativos NAC-permitidos dos Parceiros apropriados do software NAC.
3. Use a autenticação Protocolo flexível da autenticação extensível através do Tunelamento seguro (EAP-FAST) a fim configurar o Cisco Secure Services Client para autenticar à rede. Sem validação da postura, os usuários são colocados em um VLAN quarantined.
4. Configurar o CTA como indicado no *guia do administrador do Cisco Trust Agent* (disponível na site da Cisco na Web).
5. Configurar o software do sócio para usar-se com o aplicativo CTA como indicado na documentação do sócio.Uma vez que operacional, o NAC é transparente. As mensagens da postura NAC são indicadas pelo CTA na tela dos usuários.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems