Processamento de atributos de grupo e usuário do Cisco VPN Client no VPN 3000 Concentrator

Contents

Introduction

Este documento descreve como os Cisco VPN Clients são autenticados no VPN Concentrator e como o Cisco VPN 3000 Concentrator usa atributos User e Group.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco VPN 3000 Concentrator.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

O VPN Client se conecta a um VPN 3000 Concentrator

Quando um VPN Client se conecta a um VPN 3000 Concentrator, até quatro autenticações

podem ocorrer.

1. O grupo é autenticado. (Isso é frequentemente chamado de "Grupo de Túneis.")
2. O usuário é autenticado.
3. (Opcional) Se o Usuário fizer parte de outro Grupo, esse Grupo será autenticado em seguida. Se o usuário não pertencer a outro Grupo ou ao Grupo de Túneis, o padrão será o Grupo Base e essa etapa NÃO ocorrerá.
4. O "Grupo de Túneis" da Etapa 1 é autenticado novamente. (Isso é feito caso o recurso "Bloqueio de grupo" seja usado. Este recurso está disponível na versão 2.1 ou posterior.)

Este é um exemplo dos eventos que você vê no Log de Eventos para um VPN Client autenticado através do Banco de Dados Interno ("testuser" faz parte do Grupo "Engineering").

```
1 12/09/1999 11:03:46.470 SEV=6 AUTH/4 RPT=6491 80.50.0.4
Authentication successful: handle = 642, server = Internal, user = Tunnel_Group
2 12/09/1999 11:03:52.100 SEV=6 AUTH/4 RPT=6492 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = testuser
3 12/09/1999 11:03:52.200 SEV=6 AUTH/4 RPT=6493 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Engineering
4 12/09/1999 11:03:52.310 SEV=6 AUTH/4 RPT=6494 80.50.0.4
Authentication successful: handle = 643, server = Internal, user = Tunnel_Group
```

Observação: para ver esses eventos, você deve configurar a Classe de evento de autenticação com gravidade 1-6 em **Configuração > Sistema > Eventos > Classes**.

Group Lock Feature - Se o recurso Group Lock estiver habilitado no Group - Tunnel_Group, o usuário deve fazer parte do Tunnel_Group para se conectar. No exemplo anterior, você vê todos os mesmos Eventos, mas "testuser" não se conecta porque eles fazem parte do Grupo - Engenharia e não fazem parte do Grupo - Tunnel_Group. Este evento também é exibido:

```
5 12/09/1999 11:35:08.760 SEV=4 IKE/60 RPT=1 80.50.0.4
User [ testuser ]
User (testuser) not member of group (Tunnel_Group), authentication failed.
```

Para obter informações adicionais sobre o recurso Group Lock e um exemplo de configuração, consulte Bloqueando Usuários em um Grupo de Concentradores VPN 3000 Usando um Servidor RADIUS.

Autentique grupos e usuários externamente por meio do RADIUS

O VPN 3000 Concentrator também pode ser configurado para autenticar usuários e grupos externamente através de um servidor RADIUS. Isso ainda exige que os nomes dos grupos sejam configurados no VPN Concentrator, mas o tipo de grupo é configurado como "Externo".

- Grupos externos podem retornar atributos da Cisco/Altiga se o servidor RADIUS suportar VSAs (Vendor Specific Attributes, atributos específicos do fornecedor).
- Quaisquer atributos da Cisco/Altiga NÃO retornados por padrão RADIUS aos valores no Grupo base.
- Se o servidor RADIUS NÃO oferecer suporte a VSAs, TODOS os atributos serão padronizados para os atributos do grupo base.

Observação: um servidor RADIUS trata nomes de grupo de maneira não diferente dos nomes de usuário. Um grupo em um servidor RADIUS é configurado como um usuário padrão.

Essas etapas descrevem o que acontece quando um cliente IPSec se conecta ao VPN 3000 Concentrator se os usuários e grupos forem autenticados externamente. Da mesma forma que o caso interno, até quatro autenticações podem ocorrer.

1. O grupo é autenticado via RADIUS. O servidor RADIUS pode retornar muitos atributos para o grupo ou nenhum. No mínimo, o servidor RADIUS precisa retornar o atributo Cisco/Altiga "IPSec Authentication = RADIUS" para informar ao VPN Concentrator como autenticar o usuário. Caso contrário, o método de autenticação IPSec do grupo base precisa ser definido como "RADIUS".
2. O usuário é autenticado via RADIUS. O servidor RADIUS pode retornar muitos atributos para o usuário ou nenhum. Se o servidor RADIUS retornar o atributo CLASS (atributo padrão RADIUS nº 25), o VPN 3000 Concentrator usará esse atributo como nome de grupo e se moverá para a Etapa 3, caso contrário, para a Etapa 4.
3. O grupo do usuário é autenticado em seguida via RADIUS. O servidor RADIUS pode retornar muitos atributos para o grupo ou nenhum.
4. O "Grupo de Túneis" da Etapa 1 é autenticado novamente via RADIUS. O subsistema de autenticação deve autenticar o Grupo de Túneis novamente porque ele não armazenou os atributos (se houver) da autenticação na Etapa 1. Isso é feito caso o recurso "Bloqueio de grupo" seja usado.

Como o VPN 3000 Concentrator utiliza os atributos de usuário e de grupo

Depois que o VPN 3000 Concentrator tiver autenticado o Usuário e o Grupo, ele deverá organizar os atributos que recebeu. O VPN Concentrator usa os atributos nessa ordem de preferência. Não importa se a autenticação foi feita interna ou externamente:

1. **Atributos do usuário** — têm precedência sobre todos os outros.
2. **Atributos do grupo** — Todos os atributos ausentes dos atributos do usuário são preenchidos pelos atributos do grupo. Todos os que forem iguais são substituídos pelos atributos do usuário.
3. **Atributos do Grupo de Túneis** — Todos os atributos ausentes dos atributos do Usuário ou Grupo são preenchidos pelos atributos do Grupo de Túneis. Todos os que forem iguais são substituídos pelos atributos do usuário.
4. **Atributos do grupo base** —Todos os atributos ausentes dos atributos Usuário, Grupo ou Grupo de túnel são preenchidos pelos atributos do grupo base.

Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de Suporte do Cisco VPN Client
- Página de suporte do IPSec
- Página de suporte RADIUS
- Solicitações de Comentários (RFCs)
- Suporte Técnico - Cisco Systems