Travando usuários em um grupo do VPN 3000 Concentrator usando um servidor RADIUS

Índice

Introdução

O Cisco VPN 3000 Concentrator tem a capacidade para travar usuários em um grupo de concentrador que cancele o grupo que o usuário configurou no Cisco VPN 3000 Client. Desta maneira, as restrições de acesso podem ser aplicadas aos vários grupos configurados no concentrador VPN com o acreditação que os usuários estão travados nesse grupo com o servidor Radius.

Detalhes deste documento como estabelecer esta característica no Cisco Secure ACS for Windows e Cisco seguro para UNIX (CSUnix).

A configuração no concentrador VPN é similar a uma configuração padrão. A capacidade para travar usuários em um grupo definido no concentrador VPN é permitida definindo um atributo do retorno no perfil de usuário radius. Este atributo contém o nome do grupo do concentrador VPN em que o administrador quer o usuário ser travado. Este atributo é o atributo de classe (atributo de raio de IETF número 25), e tem que ser retornado ao concentrador VPN neste formato:

```
OU=groupname;
```

onde o *nome de grupo* é o nome do grupo no concentrador VPN esse o usuário trava em. *O OU* tem que ser em maiúsculo, e deve haver um ponto-e-vírgula na extremidade.

Neste exemplo, o software do cliente VPN é distribuído a todos os usuários com um perfil da conexão existente usando um *nome do grupo de* “todos” e da senha “qualquer coisa”. Cada usuário tem um nome de usuário discreto/senha (neste exemplo, o username/senha é TEST/TEST). Quando o nome de usuário é enviado ao servidor Radius, o servidor Radius envia abaixo da informação no *grupo real* que o usuário deve estar dentro. No exemplo, é “grupo de

filtros.”

Fazendo isso, você pode completamente controlar a atribuição do grupo no servidor Radius transparente aos usuários. Se o servidor Radius não atribui um grupo ao usuário, o usuário permanece no “todos” grupo. Desde que o “todos” grupo tem muito filtros restritivos, o usuário não pode passar nenhum tráfego. Se o servidor Radius atribui um grupo ao usuário, o usuário herda os atributos, incluindo o filtro menos-restritivo, particular ao grupo. Neste exemplo, você aplica um filtro ao grupo “grupo de filtros” no concentrador VPN para permitir todo o tráfego.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

Nota: Isto foi testado igualmente com sucesso com ACS 3.3, concentrador VPN 4.1.7, e cliente VPN 4.0.5.

- Versão 4.0(1)Rel da Cisco VPN 3000 Concentrator Series
- Versão Cliente VPN Cisco 4.0(1)Rel
- Versões 2.4 à 3.2 do Cisco Secure ACS for Windows
- Cisco seguro para as versões UNIX 2.3, 2.5, e 2.6

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar o Cisco VPN 3000 Concentrator

Nota: Esta configuração supõe que o concentrador VPN já se estabelece com endereços IP de Um ou Mais Servidores Cisco ICM NT, gateway padrão, conjuntos de endereços, e assim por diante. O usuário deve poder autenticar localmente antes de continuar. Se isso não trabalha, a seguir estas mudanças não trabalharão.

1. Sob o **configuração > sistema > servidores > autenticação**, adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius.
2. Uma vez que você adicionou o server, use o **botão Test Button** para verificar que você pode autenticar o usuário com sucesso.Se isto não trabalha, o fechamento do grupo não funciona.
3. Defina um filtro que as gotas alcancem a tudo na rede interna.Isto é aplicado para agrupar

"todos" de modo que mesmo se os usuários podem autenticar neste grupo e ficar nele, elas não pode ainda alcançar qualquer coisa.
4. Sob o **configuração > gerenciamento de política > gerenciamento de tráfego > regras**, adicionar uma regra chamada **Gota Todo** e deixe tudo nos padrões.
5. Sob o **Configuração > Gerenciamento de Política > Gerenciamento de tTáfego > Filtros**, crie um filtro chamado **Gota Todo**, deixe tudo nos padrões, e adicionar-lhe a gota toda a regra.
6. Sob o **configuration > user management** > os **grupos** adicionar um grupo chamado **todos**.Este é o grupo que todos os usuários PRE-configuraram no cliente VPN. Autenticam neste grupo inicialmente, e são travados então em um grupo diferente após a autenticação de usuário. Defina o grupo normalmente. Certifique-se de você adicionar a gota todo o filtro (esse você apenas criou) sob o tab geral. A fim usar a autenticação RADIUS para usuários neste grupo, ajuste o tipo do grupo (sob a aba da identidade) para ser **interno** e a autenticação (sob a aba do IPsec) ao **RAIO**. Certifique-se que a característica do fechamento do grupo não está verificada para ver se há este grupo.**Nota:** Mesmo se você não define uma gota todo o filtro, certifique-se que há pelo menos um filtro definido aqui.
7. Defina o grupo do destino final do usuário (o exemplo é "grupo de filtros"), aplicando um filtro.**Nota:** Você deve definir um filtro aqui. Se você não quer obstruir nenhum tráfego para estes usuários, crie "permitem todo o" filtro e aplicam o "alguns em" e "para fora" ordena-lhe. Você deve definir um filtro de algum amável a fim passar o tráfego. A fim usar a autenticação RADIUS para usuários neste grupo, ajuste o tipo do grupo (sob a aba da identidade) para ser **interno** e a autenticação (sob a aba do IPsec) ao **RAIO**. Certifique-se que a característica do fechamento do grupo não está verificada para ver se há este grupo.

Configurar o servidor Radius

Cisco Secure ACS for Windows

Estas etapas estabelecem seu servidor Radius do Cisco Secure ACS for Windows para travar um usuário em um grupo particular configurado no concentrador VPN. Mantenha na mente que os grupos definiram no servidor Radius não não têm nada fazer com os grupos definidos no concentrador VPN. Você pode usar grupos no servidor Radius para facilitar a administração de seus usuários. Os nomes não têm que combinar o que é configurado no concentrador VPN.

1. Adicionar o concentrador VPN como um servidor do acesso de rede (NAS) no servidor Radius sob a seção de configuração de rede.Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do concentrador VPN na caixa de endereço IP NAS.Adicionar a mesma chave que você definiu mais cedo no concentrador VPN na caixa principal.Da autenticação usando o menu suspenso, selecione o **RAIO (IETF)**.Clique **Submit + Restart**.
2. Sob a configuração da interface, o **RAIO** seleto **(IETF)** e certifica-se que o atributo **25 (classe)** está verificado.Isto permite que você mude-o no grupo/configuração do usuário.
3. Adicionar o usuário.Neste exemplo, o usuário é chamado "TESTE." Este usuário pode estar em qualquer grupo do Cisco Secure ACS for Windows. A não ser a passagem abaixo do atributo 25 para dizer ao concentrador VPN que grupo se usar para o usuário, lá não é nenhuma correlação entre grupos do Cisco Secure ACS for Windows e grupos do concentrador VPN. Este usuário é colocado em "Group_1."
4. Sob a instalação de grupo, edite ajustes no grupo (em nosso exemplo, este é "Group_1").
5. Clique o botão verde do **RADIUS IETF** para tomá-lo aos atributos apropriados.

6. Enrole para baixo e altere o atributo 25.
7. Adicionar o atributo como mostrado aqui. Substitua o nome do grupo que você quer travar os usuários para no grupo de filtros.Certifique-se que o OU é em maiúsculo e aquele lá é um ponto-e-vírgula após o nome do grupo.
8. Clique **Submit + Restart**.

Cisco seguro para UNIX

Estas etapas estabelecem seu server seguro dos RADIUS UNIX de Cisco para travar um usuário em um grupo particular configurado no concentrador VPN. Mantenha na mente que os grupos definiram no servidor Radius não não têm nada fazer com os grupos definidos no concentrador VPN. Você pode usar grupos no servidor Radius para facilitar a administração de seus usuários. Os nomes não têm que combinar o que é configurado no concentrador VPN.

1. Adicionar o concentrador VPN dentro como um NAS no servidor Radius sob a seção avançada.Escolha um dicionário que permita que o atributo 25 seja enviado como um resposta-atributo. Por exemplo, o IETF ou ascensão.
2. Adicionar o usuário.Neste exemplo, o usuário é “TESTE.” Este usuário pode estar em qualquer grupo seguro de Cisco UNIX ou em nenhum grupo. A não ser a passagem abaixo do atributo 25 para dizer ao concentrador VPN que grupo se usar para o usuário, lá não é nenhuma correlação entre grupos seguros de Cisco UNIX e grupos do concentrador VPN.
3. Sob o usuário/perfil de grupo, defina um atributo do retorno do RAIO (IETF).
4. Adicionar o atributo de classe, o número de atributo **25**, e faça seu valor **OU=filtergroup;**. Substitua o grupo definido no concentrador VPN para o grupo de filtros.**Nota:** Em Cisco UNIX seguro, defina o atributo cercado pela cotação - marcas. Estão descascados fora de quando o atributo é enviado ao concentrador VPN. O usuário/perfil de grupo deve olhar similares a este.
5. O clique **submete-se** para salvar cada entrada.As entradas Unix seguras terminadas de Cisco parecem similares a esta saída:

```
# ./ViewProfile -p 9900 -u NAS.172.18.124.132
User Profile Information
user = NAS.172.18.124.132{
profile_id = 68
profile_cycle = 1
NASNAME="172.18.124.132"
SharedSecret="cisco"
RadiusVendor="IETF"
Dictionary="DICTIONARY.IETF"

}

# ./ViewProfile -p 9900 -u TEST
User Profile Information
user = TEST{
profile_id = 70
set server current-failed-logins = 0
profile_cycle = 3
password = clear "********"
radius=IETF {
check_items= {
2="TEST"
}
reply_attributes= {
25="OU=filtergroup"
 !--- The semi-colon does NOT appear !--- after the group name, even though it has to be
included !--- when it defines the attribute via the GUI. } } } # ./ViewProfile -p 9900 -u
```

```
filtergroup User Profile Information user = filtergroup{ profile_id = 80 profile_cycle = 1
radius=IETF { check_items= { 2="filtergroup" } } } # ./ViewProfile -p 9900 -u Everyone User
Profile Information user = Everyone{ profile_id = 67 profile_cycle = 1 radius=IETF {
check_items= { 2="Anything" } } }
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Usuário e processamento de atributo de grupo de Cisco VPN 3000 Client no VPN 3000 concentrator
- Página de suporte de tecnologia dos radius (serviço de usuário de discagem de autenticação remota)
- Páginas de suporte do Concentradores Cisco VPN série 3000
- Páginas de suporte ao Cisco VPN 3000 Client
- Páginas de suporte do produto do protocolo de segurança IP (IPsec)
- Solicitações de Comentários (RFCs)
- Página de suporte do produto do Cisco Secure ACS for Windows
- Field Notice dos produtos de segurança
- Cisco Secure ACS para páginas de suporte do produto de UNIX
- Suporte Técnico - Cisco Systems