Exemplo de configuração de Shunning/Blocking no IPS para ASA/PIX/IOS Router

Contents

Introduction

Este documento descreve como configurar o shunning em um PIX/ASA/Cisco IOS Router com a ajuda do Cisco IPS. O ARC, o aplicativo de bloqueio no sensor, inicia e interrompe blocos em roteadores, Cisco 5000 RSM e Catalyst 6500 Series Switches, PIX Firewalls, FWSM e ASA. O ARC emite um bloco ou um shun para o dispositivo gerenciado para o endereço IP mal-intencionado. O ARC envia o mesmo bloco para todos os dispositivos que o sensor gerencia. Se um sensor de bloqueio primário estiver configurado, o bloco será encaminhado para e emitido a partir deste dispositivo. O ARC monitora o tempo para o bloco e remove o bloco quando o tempo expira.

Quando você usa o IPS 5.1, deve-se ter cuidado especial ao enviar para os firewalls em modo de contexto múltiplo, pois nenhuma informação de VLAN é enviada com a solicitação shun.

Note: O bloqueio não é suportado no contexto admin de um FWSM de contexto múltiplo.

Há três tipos de blocos:

- Host block—Bloqueia todo o tráfego de um determinado endereço IP.
- Bloco de conexão—Bloqueia o tráfego de um determinado endereço IP de origem para um determinado endereço IP de destino e porta de destino. Vários blocos de conexão do mesmo endereço IP de origem para um endereço IP de destino ou uma porta de destino diferente comutam automaticamente o bloco de um bloco de conexão para um bloco de host.**Note**: Os blocos de conexão não são suportados por dispositivos de segurança. Os dispositivos de segurança só suportam blocos de host com informações opcionais de porta e protocolo.
- Bloco de rede—Bloqueia todo o tráfego de uma determinada rede. Você pode iniciar o host e

os blocos de conexão manualmente ou automaticamente quando uma assinatura é disparada. Você só pode iniciar blocos de rede manualmente.

Para blocos automáticos, você deve escolher Solicitar Host de Bloco ou Solicitar Conexão de Bloco como a ação de evento para determinadas assinaturas, de modo que o SensorApp envie uma solicitação de bloco ao ARC quando a assinatura é disparada. Quando o ARC recebe a solicitação de bloqueio do SensorApp, ele atualiza as configurações do dispositivo para bloquear o host ou a conexão. Consulte Atribuindo Ações a Assinaturas, página 5-22 para obter mais informações sobre o procedimento para adicionar as ações de evento Solicitar Host de Bloco ou Solicitar Conexão de Bloco à assinatura. Consulte Configuração de Sobreposições de Ação de Evento, página 7-15 para obter mais informações sobre o procedimento para a configuração de substituições que adicionam as ações de evento Solicitar Host de Bloco ou Solicitar Conexão de Bloco a alarmes de classificações de risco específicas.

Nos roteadores Cisco e nos switches da série Catalyst 6500, o ARC cria blocos aplicando ACLs ou VACLs. As ACLs e VACLs aplicam filtros às interfaces, que incluem direção, e VLANs, respectivamente, para permitir ou negar tráfego. . O PIX Firewall, o FWSM e o ASA não usam ACLs ou VACLs. Os comandos **shun** interno e **no shun** são usados.

Essas informações são necessárias para a configuração do ARC:

- ID do usuário de login, se o dispositivo estiver configurado com AAA
- Senha de login
- Habilitar senha, que não é necessária se o usuário tiver privilégios de habilitação
- Interfaces a serem gerenciadas, por exemplo, ethernet0, vlan100
- Qualquer informação de ACL ou VACL existente que você deseja aplicar no início (ACL de pré-bloco ou VACL) ou final (ACL de pós-bloco ou VACL) da ACL ou da VACL criada. Isso não se aplica a um PIX Firewall, FWSM ou ASA porque eles não usam ACLs ou VACLs para bloquear.
- Se você usa Telnet ou SSH para se comunicar com o dispositivo
- Endereços IP (host ou intervalo de hosts) que você nunca deseja bloquear
- Quanto tempo você quer que os blocos durem

Prerequisites

Requirements

Antes de configurar o ARC para bloqueio ou limitação de taxa, você deve concluir estas tarefas:

- Analise sua topologia de rede para entender quais dispositivos devem ser bloqueados por qual sensor e quais endereços nunca devem ser bloqueados.
- Reúna os nomes de usuário, as senhas do dispositivo, as senhas de ativação e os tipos de conexões (Telnet ou SSH) necessários para fazer login em cada dispositivo.
- Conheça os nomes das interfaces nos dispositivos.
- Conheça os nomes da ACL de pré-bloqueio ou da VACL e da ACL de pós-bloqueio ou da VACL, se necessário.
- Entenda quais interfaces devem e não devem ser bloqueadas e em que direção (entrada ou saída).

Componentes Utilizados

As informações neste documento são baseadas no Cisco Intrusion Prevention System 5.1 e posterior.

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.

> **Note**: Por padrão, o ARC é configurado para um limite de 250 entradas de bloco. Consulte Dispositivos suportados para obter mais informações sobre a lista de dispositivos de bloqueio suportados pelo ARC.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Use a página de bloqueio para definir as configurações básicas necessárias para ativar o bloqueio e a limitação de taxa.

O ARC controla ações de bloqueio e limitação de taxa em dispositivos gerenciados.

Você deve ajustar seu sensor para identificar hosts e redes que nunca devem ser bloqueados. É possível que o tráfego de um dispositivo confiável dispare uma assinatura. Se essa assinatura estiver configurada para bloquear o invasor, o tráfego legítimo da rede poderá ser afetado. O endereço IP do dispositivo pode ser listado na lista Nunca Bloquear para evitar esse cenário.

Uma máscara de rede especificada em uma entrada Nunca Bloquear é aplicada ao endereço Nunca Bloquear. Se nenhuma máscara de rede for especificada, uma máscara /32 padrão será aplicada.

> **Note**: Por padrão, o sensor não tem permissão para emitir um bloco para seu próprio endereço IP, pois isso interfere na comunicação entre o sensor e o dispositivo de bloqueio. Mas essa opção é configurável pelo usuário.

Quando o ARC é configurado para gerenciar um dispositivo de bloqueio, os shuns e ACLs/VACLs do dispositivo de bloqueio que são usados para bloqueio não devem ser alterados manualmente. Isso pode causar uma interrupção do serviço ARC e fazer com que blocos futuros não sejam emitidos.

> **Note**: Por padrão, somente o bloqueio é suportado em dispositivos Cisco IOS. Você pode substituir o padrão de bloqueio se escolher limite de taxa ou limite de taxa de adição de bloqueio.

Para emitir ou alterar blocos, o usuário do IPS deve ter a função de Administrador ou Operador.

Configure o sensor para gerenciar os roteadores Cisco

Esta seção descreve como configurar o sensor para gerenciar os roteadores Cisco. Ele contém estes tópicos:

- Configurar perfis de usuário
- Roteadores e ACLs
- Configurar roteadores Cisco usando CLI

Configurar perfis de usuário

O sensor gerencia os outros dispositivos com o comando **user-profile** *profile_name* para configurar perfis de usuário. Os perfis de usuário contêm as informações de ID de usuário, senha e senha de ativação. Por exemplo, os roteadores que compartilham as mesmas senhas e nomes de usuário podem estar em um perfil de usuário.

> **Note**: Você **deve** criar um perfil de usuário antes de configurar o dispositivo de bloqueio.

Conclua estes passos para configurar perfis de usuário:

1. Faça login na CLI com uma conta que tenha privilégios de Administrador.
2. Entre no modo de acesso à rede.
```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```
3. Crie o nome do perfil de usuário.
```
sensor(config-net)#user-profiles PROFILE1
```
4. digite o nome de usuário desse perfil de usuário.
```
sensor(config-net-use)#username username
```
5. Especifique a senha para o usuário.
```
sensor(config-net-use)# password
Enter password[]: ********
Re-enter password ********
```
6. Especifique a senha de ativação para o usuário.
```
sensor(config-net-use)# enable-password
Enter enable-password[]: ********
Re-enter enable-password ********
```
7. Verifique as configurações.
```
sensor(config-net-use)#show settings
   profile-name: PROFILE1
   -----------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: jsmith default:
   -----------------------------------------------
sensor(config-net-use)#
```
8. Saia do submodo de acesso à rede.

```
sensor(config-net-use)#exit
sensor(config-net)#exit
Apply Changes:?[yes]:
```

9. Pressione **Enter** para aplicar as alterações ou digite não para descartá-las.

Roteadores e ACLs

Quando o ARC é configurado com um dispositivo de bloqueio que usa ACLs, as ACLs são compostas desta maneira:

1. Uma linha de permissão com o endereço IP do sensor ou, se especificado, o endereço NAT do sensor**Note**: Se você permitir que o sensor seja bloqueado, essa linha não aparecerá na ACL.
2. ACL de pré-bloqueio (se especificado): Essa ACL já deve existir no dispositivo.**Note**: O ARC lê as linhas na ACL pré-configurada e copia essas linhas para o início da ACL de bloco.
3. Qualquer bloco ativo
4. **ACL pós-bloco** ou **permit ip any any**:**ACL pós-bloco** (se especificado):Essa ACL já deve existir no dispositivo.**Note**: O ARC lê as linhas na ACL e copia essas linhas até o final da ACL.**Note**: Verifique se a última linha na ACL é permit ip any any se quiser que todos os pacotes não correspondentes sejam permitidos.**permit ip any any** (não usado se uma ACL pós-bloco for especificada)

   Note: As ACLs que o ARC faz nunca devem ser modificadas por você ou por qualquer outro sistema. Essas ACLs são temporárias e novas ACLs são criadas constantemente pelo sensor. As únicas modificações que você pode fazer são as ACLs de pré e pós-bloco.

Se precisar modificar a ACL de pré-bloqueio ou pós-bloqueio, faça o seguinte:

1. Desative o bloqueio no sensor.
2. Faça as alterações na configuração do dispositivo.
3. Reative o bloqueio no sensor.

Quando o bloqueio é reativado, o sensor lê a configuração do novo dispositivo.

Note: Um único sensor pode gerenciar vários dispositivos, mas vários sensores não podem gerenciar um único dispositivo. No caso de os blocos emitidos a partir de vários sensores se destinarem a um único dispositivo de bloqueio, deve ser incorporado no projeto um sensor de bloqueio primário. Um sensor de bloqueio primário recebe solicitações de bloqueio de vários sensores e emite todas as solicitações de bloqueio para o dispositivo de bloqueio.

Você cria e salva ACLs de pré e pós-bloqueio na configuração do roteador. Essas ACLs devem ser ACLs IP estendidas, nomeadas ou numeradas. Consulte a documentação do roteador para obter mais informações sobre como criar ACLs.

Note: As ACLS pré e pós-bloco não se aplicam à limitação de taxa.

As ACLs são avaliadas de cima para baixo e a ação de primeira correspondência é executada. A ACL de pré-bloqueio pode conter uma permissão que teria precedência sobre uma negação resultante de um bloco.

A ACL de pós-bloco é usada para considerar quaisquer condições não tratadas pela ACL de pré-bloco ou blocos. Se você tiver uma ACL existente na interface e na direção em que os blocos são emitidos, essa ACL pode ser usada como a ACL de pós-bloco. Se você não tiver uma ACL de pós-bloco, o sensor insere permit ip any any no final da nova ACL.

Quando o sensor é iniciado, ele lê o conteúdo das duas ACLs. Ele cria uma terceira ACL com estas entradas:

- Uma linha de permissão para o endereço IP do sensor
- Cópias de todas as linhas de configuração da ACL de pré-bloqueio
- Uma linha de negação para cada endereço bloqueado pelo sensor
- Cópias de todas as linhas de configuração da ACL pós-bloqueio

O sensor aplica a nova ACL à interface e direção designadas.

> **Note**: Quando a nova ACL de bloco é aplicada a uma interface do roteador, em uma direção específica, ela substitui qualquer ACL pré-existente nessa interface nessa direção.

Configurar roteadores Cisco usando CLI

Conclua estes passos para configurar um sensor para gerenciar um roteador Cisco para executar bloqueio e limitação de taxa:

1. Faça login na CLI com uma conta que tenha privilégios de Administrador.
2. Entre no submodo de acesso à rede.
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. Especifique o endereço IP do roteador controlado pelo ARC.
   ```
   sensor(config-net)#router-devices ip_address
   ```
4. Insira o nome do dispositivo lógico que você criou ao configurar o perfil de usuário.
   ```
   sensor(config-net-rou)#profile-name user_profile_name
   ```
   Note: O ARC aceita tudo o que você digitar. Não verifica se o perfil de usuário existe.
5. Especifique o método usado para acessar o sensor.
   ```
   sensor(config-net-rou)# communication {telnet | ssh-des | ssh-3des}
   ```

   Se não especificado, SSH 3DES é usado.**Note**: Se você usa DES ou 3DES, deve usar o comando **ssh host-key ip_address** para aceitar a chave SSH do dispositivo.
6. Especifique o endereço NAT do sensor.
   ```
   sensor(config-net-rou)#nat-address nat_address
   ```
   Note: Isso altera o endereço IP na primeira linha da ACL do endereço do sensor para o endereço NAT. O endereço NAT é o endereço do sensor, pós-NAT, traduzido por um dispositivo intermediário, localizado entre o sensor e o dispositivo de bloqueio.
7. Especifique se o roteador executa bloqueio, limitação de taxa ou ambos.**Note**: O padrão é bloquear. Você não precisa configurar os recursos de resposta se quiser que o roteador execute o bloqueio apenas.Limitação de taxa somente
   ```
   sensor(config-net-rou)#response-capabilities rate-limit
   ```

   Bloqueio e limitação de taxa
   ```
   sensor(config-net-rou)#response-capabilities block|rate-limit
   ```

8. Especifique o nome e a direção da interface.
```
sensor(config-net-rou)#block-interfaces interface_name {in | out}
```

   Note: O nome da interface deve ser uma abreviação que o roteador reconhece quando usado após o comando **interface**.
9. (Opcional) Adicione o nome pré-ACL (somente bloqueio).
```
sensor(config-net-rou-blo)#pre-acl-name pre_acl_name
```
10. (Opcional) Adicione o nome pós-ACL (somente bloqueio).
```
sensor(config-net-rou-blo)#post-acl-name post_acl_name
```
11. Verifique as configurações.
```
sensor(config-net-rou-blo)#exit

sensor(config-net-rou)#show settings

   ip-address: 10.89.127.97
   ------------------------------------------------
      communication: ssh-3des default: ssh-3des
      nat-address: 19.89.149.219 default: 0.0.0.0
      profile-name: PROFILE1
      block-interfaces (min: 0, max: 100, current: 1)
      ------------------------------------------------
         interface-name: GigabitEthernet0/1
         direction: in
         ------------------------------------------------
            pre-acl-name: <defaulted>
            post-acl-name: <defaulted>
         ------------------------------------------------
      ------------------------------------------------
      response-capabilities: block|rate-limit default: block
   ------------------------------------------------
sensor(config-net-rou)#
```
12. Saia do submodo de acesso à rede.
```
sensor(config-net-rou)#exit
sensor(config-net)#exit
sensor(config)#exit
Apply Changes:?[yes]:
```
13. Pressione **Enter** para aplicar as alterações ou digite **no** para descartá-las.

Configurar o sensor para gerenciar os firewalls da Cisco

Conclua estes passos para configurar o sensor para gerenciar os firewalls da Cisco:

1. Faça login na CLI com uma conta que tenha privilégios de Administrador.
2. Entre no submodo de acesso à rede.
```
sensor#configure terminal
sensor(config)#service network-access
sensor(config-net)#
```
3. Especifique o endereço IP do firewall controlado pelo ARC.
```
sensor(config-net)#firewall-devices ip_address
```
4. Insira o nome do perfil de usuário que você criou ao configurar o perfil de usuário.
```
sensor(config-net-fir)#profile-name user_profile_name
```
   Note: O ARC aceita qualquer coisa que você digitar. Ele não verifica se o dispositivo lógico existe.
5. Especifique o método usado para acessar o sensor.
```
sensor(config-net-fir)#communication {telnet | ssh-des | ssh-3des}
```

Se não especificado, SSH 3DES é usado.**Note**: Se você usa DES ou 3DES, deve usar o **comando ssh host-key ip_address** para aceitar a chave ou o ARC não pode se conectar ao dispositivo.

6. Especifique o endereço NAT do sensor.
   ```
   sensor(config-net-fir)#nat-address nat_address
   ```
   Note: Isso altera o endereço IP na primeira linha da ACL do endereço IP do sensor para o endereço NAT. O endereço NAT é o endereço do sensor, pós-NAT, traduzido por um dispositivo intermediário, localizado entre o sensor e o dispositivo de bloqueio.
7. Saia do submodo de acesso à rede.
   ```
   sensor(config-net-fir)#exit
   sensor(config-net)#exit
   sensor(config)#exit
   Apply Changes:?[yes]:
   ```
8. Pressione **Enter** para aplicar as alterações ou digite **no** para descartá-las.

Bloquear com SHUN no PIX/ASA

A emissão do comando **shun** bloqueia conexões de um host de ataque. Os pacotes que correspondem aos valores no comando são descartados e registrados até que a função de bloqueio seja removida. O **shun** é aplicado independentemente de uma conexão com o endereço de host especificado estar atualmente ativa.

Se você especificar o endereço de destino, as portas de origem e de destino e o protocolo, você restringirá o shun às conexões que correspondem a esses parâmetros. Você pode ter apenas um comando **shun** para cada endereço IP de origem.

Como o comando **shun** é usado para bloquear ataques dinamicamente, ele não é exibido na configuração do Security Appliance.

Sempre que uma interface é removida, todos os shuns conectados a essa interface também são removidos.

Este exemplo mostra que o host ofensivo (10.1.1.27) faz uma conexão com a vítima (10.2.2.89) com o TCP. A conexão na tabela de conexão do Security Appliance diz o seguinte:

```
TCP outside:10.1.1.27/555 inside:10.2.2.89/666
```

Para bloquear conexões de um host de ataque, use o comando **shun** no modo EXEC privilegiado. Aplique o comando **shun** com estas opções:

```
hostname#shun 10.1.1.27 10.2.2.89 555 666 tcp
```

O comando exclui a conexão da tabela de conexão do Security Appliance e também impede que os pacotes de 10.1.1.27:555 a 10.2.2.89:666 (TCP) passem pelo Security Appliance.

Informações Relacionadas

- Configurando o sensor para gerenciar os switches Catalyst 6500 Series e os roteadores

Cisco 7600 Series

- Suporte Técnico e Documentação - Cisco Systems