ASA/PIX 7.x e posterior: Atenuação dos ataques à rede

Contents

Introduction

Este documento descreve como reduzir os vários ataques à rede, tais como os Recusa de Serviços (DoS), usando o Cisco Security Appliance (ASA/PIX).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco 5500 Series Adaptive Security Appliance (ASA) que executa o software versão 7.0 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.

Produtos Relacionados

Este documento também pode ser usado com o Cisco 500 Series PIX que executa o software versão 7.0 e posterior.

Conventions

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

Proteção contra ataques SYN

Como você atenua os ataques de sincronização/inicialização (SYN) do Transmission Control Protocol (TCP) no ASA/PIX?

Ataque SYN de TCP

O ataque TCP SYN é um tipo de ataque DoS no qual um remetente transmite um volume de conexões que não podem ser concluídas. Isso faz com que as filas de conexões sejam preenchidas e, conseqüentemente, o atendimento aos usuários TCP legítimos seja recusado.

Quando uma conexão TCP normal é iniciada, um host de destino recebe um pacote SYN de um host de origem e envia de volta uma confirmação de sincronização (SYN ACK). O host de destino deve ouvir um ACK do SYN ACK antes de estabelecer a conexão. Isso é conhecido como handshake triplo do TCP.

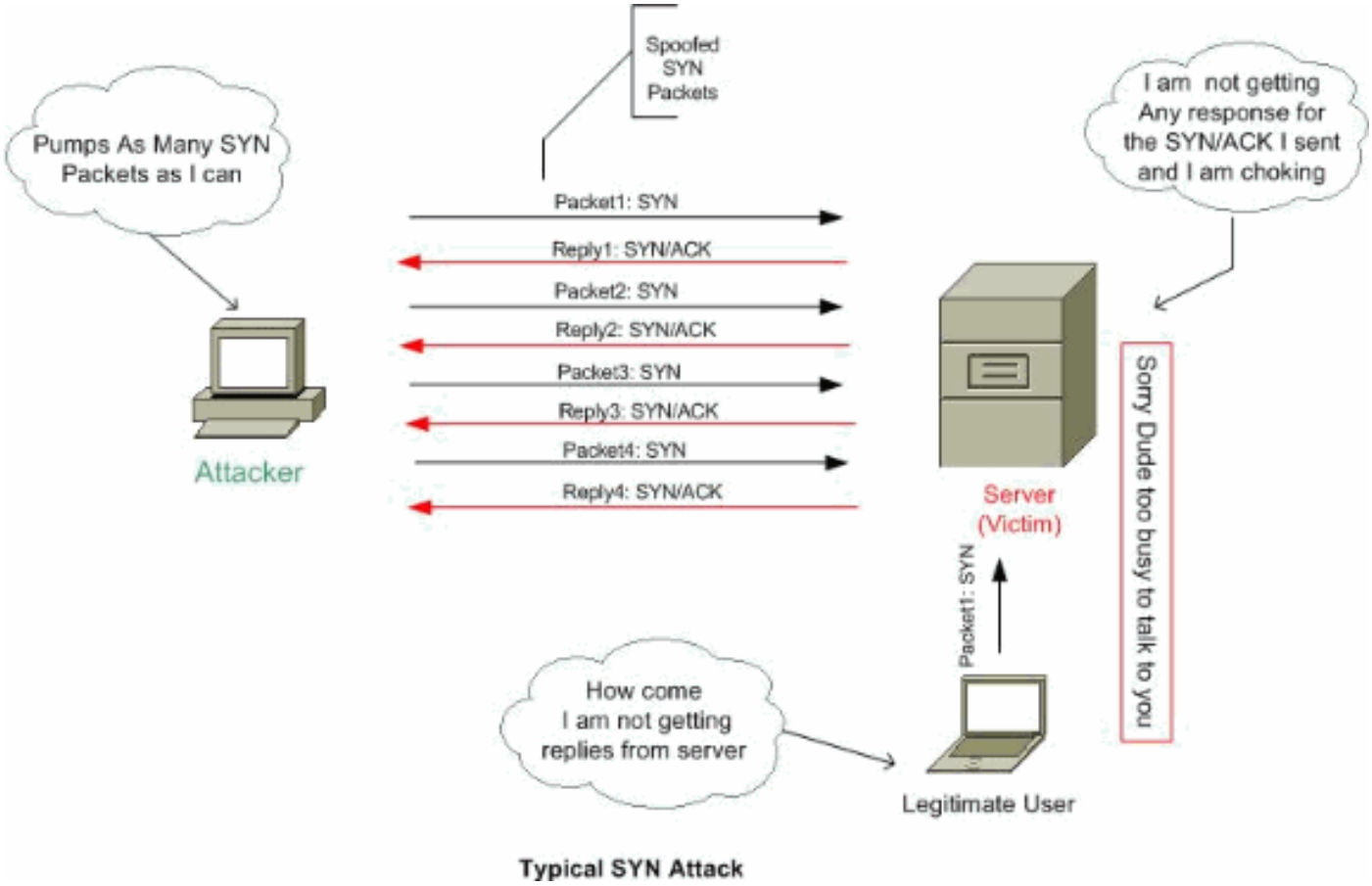
Enquanto aguarda o ACK para o SYN ACK, uma fila de conexão de tamanho finito no host de destino mantém o controle das conexões aguardando conclusão. Essa fila normalmente fica esvaziada rapidamente porque se espera que o ACK chegue alguns milissegundos após o SYN ACK.

O ataque SYN em TCP explora esse projeto ao fazer um host de origem de ataque gerar pacotes SYN no TCP com endereços de origem aleatórios em direção ao host de uma vítima. O host de destino da vítima envia um SYN ACK de volta ao endereço de origem aleatório e adiciona uma entrada à fila de conexão. Como a SYN ACK é destinada a um host incorreto ou inexistente, a última parte do "handshake triplo" nunca é concluída e a entrada permanece na fila de conexão até que um temporizador expire, normalmente por cerca de um minuto. Ao gerar pacotes SYN de TCP falsos de endereços IP aleatórios em uma taxa rápida, é possível preencher a fila de conexão e negar serviços TCP (como e-mail, transferência de arquivos ou WWW) a usuários legítimos.

Não há maneira fácil de rastrear o originador do ataque porque o endereço IP da origem é forjado.

As manifestações externas do problema incluem incapacidade de obter e-mail, incapacidade de aceitar conexões com serviços WWW ou FTP ou um grande número de conexões TCP em seu host no estado SYN_RCVD.

Consulte Defesas contra ataques de inundação TCP SYN para obter mais informações sobre ataques TCP SYN.



Typical SYN Attack

Atenuação

Esta seção descreve como atenuar os ataques SYN definindo o máximo de conexões TCP e User Datagram Protocol (UDP), o máximo de conexões embrionárias, o tempo limite de conexão e como desativar a aleatorização da sequência TCP.

Se o limite de conexão embrionária for atingido, o Security Appliance responderá a cada pacote SYN enviado ao servidor com um SYN+ACK e não passará o pacote SYN para o servidor interno. Se o dispositivo externo responder com um pacote ACK, o Security Appliance saberá que é uma solicitação válida (e não parte de um possível ataque SYN). O Security Appliance estabelece uma conexão com o servidor e une as conexões. Se o Security Appliance não receber um ACK de volta do servidor, ele grava agressivamente essa conexão embrionária.

Cada conexão TCP tem dois Números de Sequência Inicial (ISNs): um gerado pelo cliente e um gerado pelo servidor. O Security Appliance randomiza o ISN do TCP SYN que passa nas direções de entrada e saída.

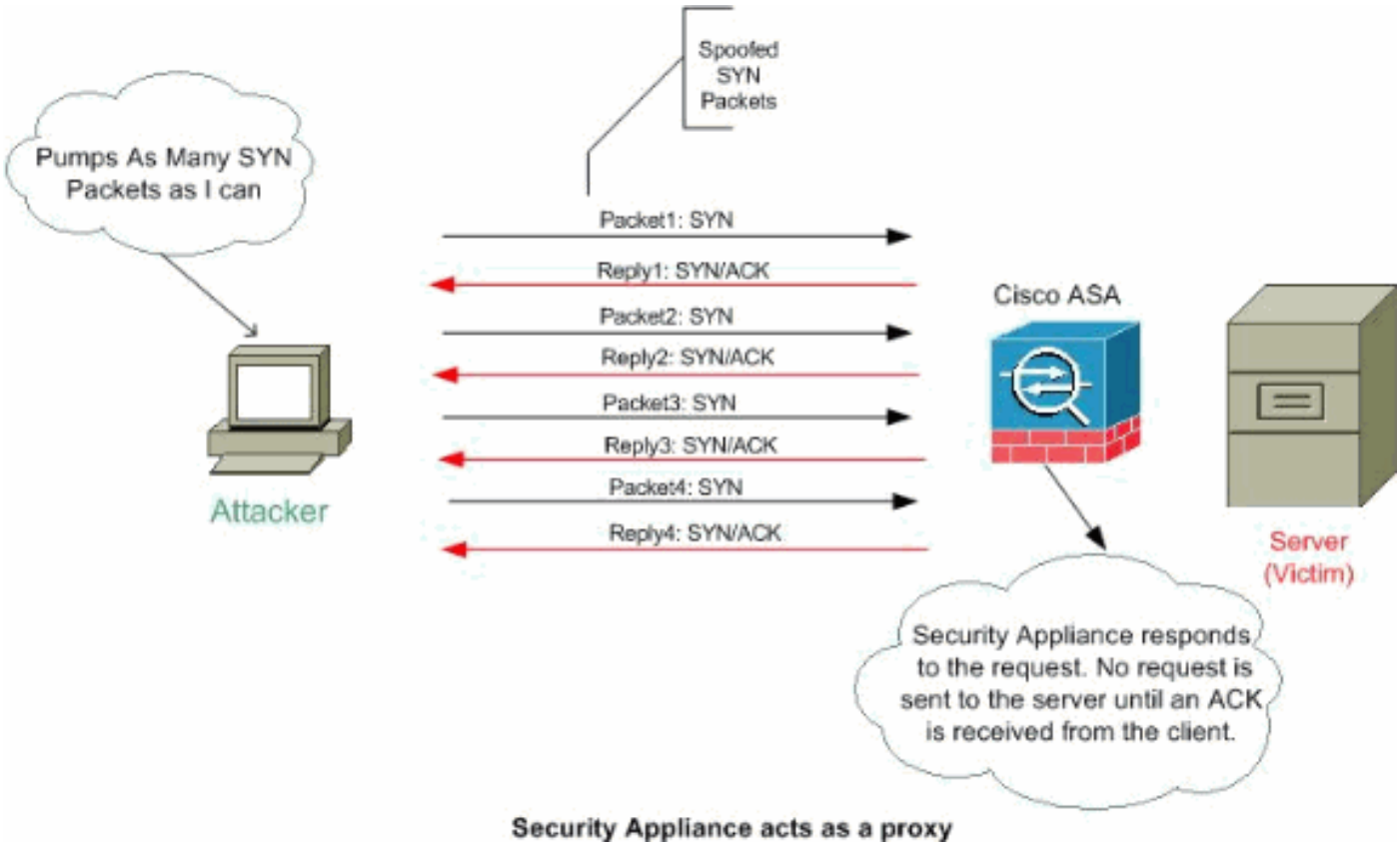
Randomizar o ISN do host protegido evita que um invasor preveja o próximo ISN para uma nova conexão e potencialmente sequestre a nova sessão.

A aleatorização do número de sequência inicial do TCP pode ser desativada, se necessário. Por exemplo:

- Se outro firewall em linha também estiver randomizando os números de sequência iniciais, não haverá necessidade de ambos os firewalls realizarem essa ação, mesmo que essa ação não afete o tráfego.
- Se você usar o multi-hop BGP externo (eBGP) através do Security Appliance e os peers de eBGP estiverem usando MD5, a aleatorização quebra a soma de verificação MD5.

- Você usa um dispositivo WAAS (Wide Area Application Services) que exige que o Security Appliance não randomize os números de sequência de conexões.

Observação: você também pode configurar conexões máximas, conexões embrionárias máximas e aleatorização da sequência TCP na configuração NAT. Se você definir essas configurações para o mesmo tráfego usando ambos os métodos, o Security Appliance usará o limite inferior. Para a randomização da sequência TCP, se ela for desabilitada usando um dos métodos, o Security Appliance desabilitará a randomização da sequência TCP.



Security Appliance acts as a proxy

Conclua estes passos para definir limites de conexão:

1. Para identificar o tráfego, adicione um mapa de classe usando o comando **class-map** de acordo com Using Modular Policy Framework.
2. Para adicionar ou editar um **mapa de políticas** que defina as ações a serem tomadas com o tráfego do mapa de classes, insira este comando:
   ```
   hostname(config)#policy-map name
   ```
3. Para identificar o mapa de classes (da etapa 1) ao qual você deseja atribuir uma ação, insira este comando:
   ```
   hostname(config-pmap)#class class_map_name
   ```
4. Para definir o máximo de conexões (TCP e UDP), o máximo de conexões embrionárias, por cliente-embrionário-max, por cliente-max ou se desabilitar a aleatorização da sequência TCP, insira este comando:
   ```
   hostname(config-pmap-c)#set connection {[conn-max number]
   [embryonic-conn-max number] [per-client-embryonic-max number]
   [per-client-max number][random-sequence-number {enable |
   disable}}
   ```
   Onde number é um inteiro entre 0 e 65535. O padrão é 0, o que significa que não há limite para conexões.Você pode inserir esse comando tudo em uma linha (em qualquer ordem) ou

pode inserir cada atributo como um comando separado. O comando é combinado em uma linha na configuração atual.

5. Para definir o tempo limite para conexões, conexões embrionárias (meio abertas) e conexões meio fechadas, insira este comando:
   ```
   hostname(config-pmap-c)#set connection {[embryonic hh[:mm[:ss]]]
   [half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]]]}
   ```
   Onde **embrionário** hh[:mm[:ss] é um tempo entre 0:0:5 e 192:59:59. O padrão é 0:0:30. Você também pode definir esse valor como 0, o que significa que a conexão nunca expira.Os valores **half-closed** hh[:mm[:ss] e **tcp** hh[:mm[:ss] são um tempo entre 0:5:0 e 1192:59:59. O padrão para **half-closed** é 0:10:0 e o padrão para **tcp** é 1:0:0. Você também pode definir esses valores como 0, o que significa que a conexão nunca expira.Você pode inserir esse comando tudo em uma linha (em qualquer ordem) ou pode inserir cada atributo como um comando separado. O comando é combinado em uma linha na configuração atual.**Conexão embrionária (meio aberta)** —Uma conexão embrionária é uma solicitação de conexão TCP que não terminou o handshake necessário entre a origem e o destino.**Conexão semifechada** — a conexão semifechada ocorre quando a conexão é fechada apenas em uma direção pelo envio FIN. No entanto, a sessão TCP ainda é mantida por peer.**Por cliente-embrionário-máx** — O número máximo de conexões embrionárias simultâneas permitidas por cliente, entre 0 e 65535. O padrão é 0, que permite conexões ilimitadas.**Por cliente-máx** — O número máximo de conexões simultâneas permitidas por cliente, entre 0 e 65535. O padrão é 0, que permite conexões ilimitadas.
6. Para ativar o mapa de políticas em uma ou mais interfaces, digite este comando:
   ```
   hostname(config)#service-policy policymap_name {global | interface interface_name}
   ```
   Onde **global** aplica o mapa de política a todas as interfaces e **interface** aplica a política a uma interface. Apenas uma política global é permitida. Você pode substituir a política global em uma interface aplicando uma política de serviço a essa interface. Você só pode aplicar um mapa de política a cada interface.

Exemplo:

```
ciscoasa(config)#class-map tcp_syn
ciscoasa(config-cmap)#match port tcp eq 80
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map tcpmap
ciscoasa(config-pmap)#class tcp_syn
ciscoasa(config-pmap-c)#set connection conn-max 100
ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200
ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10
ciscoasa(config-pmap-c)#set connection per-client-max 5
ciscoasa(config-pmap-c)#set connection random-sequence-number enable
ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45
ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0
ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
ciscoasa(config)#service-policy tcpmap global
```

Observação: para verificar o número total de sessões de meia-abertura para qualquer host específico, use este comando:

```
ASA-5510-8x# show local-host all
```

```
Interface dmz: 0 active, 0 maximum active, 0 denied
Interface management: 0 active, 0 maximum active, 0 denied
Interface xx: 0 active, 0 maximum active, 0 denied
Interface inside: 7 active, 18 maximum active, 0 denied

local host: <10.78.167.69>,

    TCP flow count/limit = 2/unlimited

    TCP embryonic count to host = 0

    TCP intercept watermark = unlimited

    UDP flow count/limit = 0/unlimited
```

Observação: a linha, `contagem embrionária TCP para host`, exibe o número de sessões semiabertas.

Proteção contra ataques de falsificação de IP

O PIX/ASA pode bloquear ataques de spoof IP?

Spoofing de IP

Para obter acesso, os invasores criam pacotes com endereços IP de origem falsificados. Isso explora aplicativos que usam autenticação com base em endereços IP e leva a usuários não autorizados e possivelmente ao acesso raiz no sistema de destino. Exemplos são os serviços rsh e rlogin.

Épossível rotear pacotes através de firewalls de roteador de filtragem se eles não estiverem configurados para filtrar pacotes de entrada cujo endereço de origem esteja no domínio local. É importante observar que o ataque descrito é possível mesmo que nenhum pacote de resposta possa alcançar o invasor.

Exemplos de configurações que são potencialmente vulneráveis incluem:

- Firewalls de proxy em que os aplicativos de proxy usam o endereço IP de origem para autenticação
- Roteadores para redes externas que suportam várias interfaces internas
- Roteadores com duas interfaces que suportam sub-redes na rede interna

Atenuação

O Unicast Reverse Path Forwarding (uRPF) protege contra falsificação de IP (um pacote usa um endereço IP de origem incorreto para obscurecer sua verdadeira origem) garantindo que todos os pacotes tenham um endereço IP de origem que corresponda à interface de origem correta de acordo com a tabela de roteamento.

Normalmente, o Security Appliance olha apenas o endereço de destino ao determinar para onde encaminhar o pacote. O unicast RPF instrui o Security Appliance a examinar também o endereço de origem. É por isso que se chama **Reverse Path Forwarding**. Para qualquer tráfego que você queira permitir através do Security Appliance, a tabela de roteamento do Security Appliance deve incluir uma rota de volta ao endereço de origem. Consulte RFC 2267 para obter mais informações.

Nota: O `:- %PIX-1-106021: Negar verificação de caminho reverso do protocolo de src_addr para dest_addr na interface int_name` mensagem de log pode ser vista quando a verificação de caminho reverso está habilitada. Desative a verificação de caminho reverso com o comando **no ip verify reverse-path interface (nome da interface)** para resolver esse problema:

`no ip verify reverse-path interface (interface name)`

Para tráfego externo, por exemplo, o Security Appliance pode usar a rota padrão para satisfazer a proteção de RPF Unicast. Se o tráfego entrar em uma interface externa e o endereço de origem não for conhecido na tabela de roteamento, o Security Appliance usará a rota padrão para identificar corretamente a interface externa como a interface de origem.

Se o tráfego entra na interface externa de um endereço conhecido da tabela de roteamento, mas associado à interface interna, o Security Appliance descarta o pacote. Da mesma forma, se o tráfego entra na interface interna de um endereço de origem desconhecido, o Security Appliance descarta o pacote porque a rota correspondente (a rota padrão) indica a interface externa.

O RPF unicast é implementado conforme mostrado:

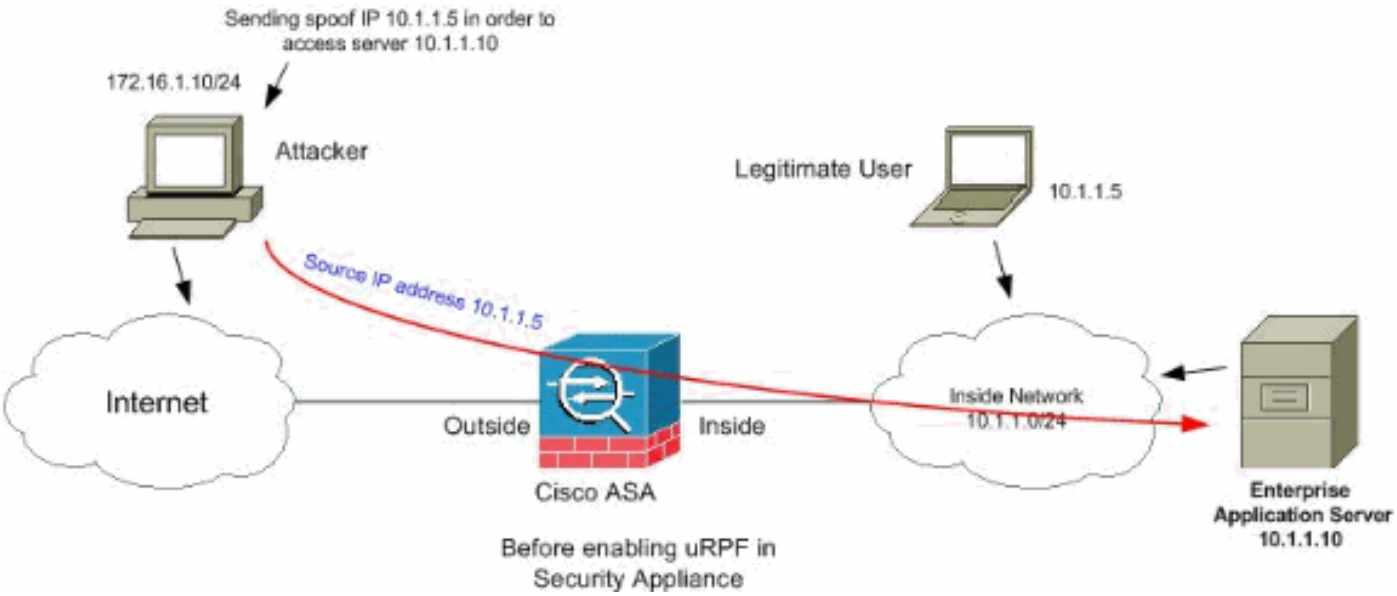
- Os pacotes ICMP não têm sessão, portanto cada pacote é verificado.
- O UDP e o TCP têm sessões, portanto, o pacote inicial requer uma pesquisa de rota reversa. Os pacotes subsequentes que chegam durante a sessão são verificados usando um estado existente mantido como parte da sessão. Os pacotes não iniciais são verificados para garantir que chegaram na mesma interface usada pelo pacote inicial.

Para habilitar o RPF Unicast, insira este comando:

`hostname(config)#`**`ip verify reverse-path interface`** *`interface_name`*

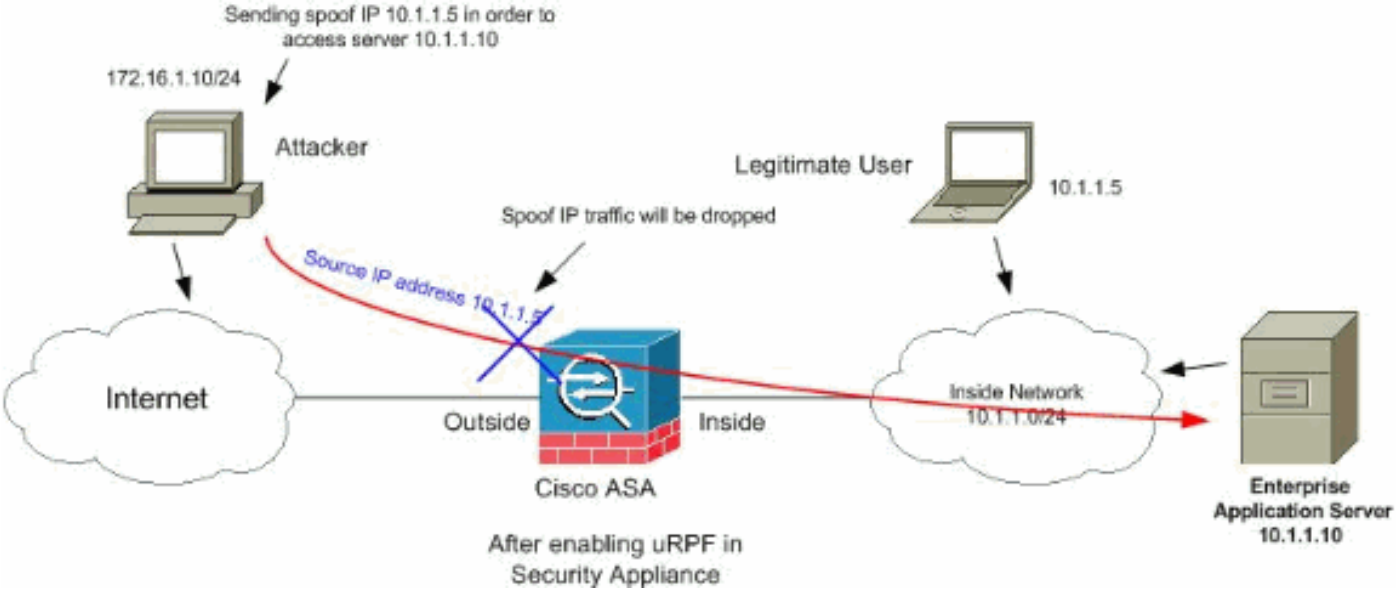
Exemplo:

Como mostrado nesta figura, o PC invasor origina uma solicitação ao servidor de aplicativos 10.1.1.10 enviando um pacote com um endereço IP de origem forjada 10.1.1.5/24, e o servidor envia um pacote ao endereço IP real 10.1.1.5/24 em resposta à solicitação. Esse tipo de pacote ilegal atacará o servidor de aplicativos e o usuário legítimo na rede interna.



O unicast RPF pode evitar ataques com base na falsificação de endereço de origem. Você precisa configurar o uRPF na interface externa do ASA conforme mostrado aqui:

```
ciscoasa(config)#ip verify reverse-path interface outside
```



Identificação de falsificação usando mensagens de syslog

O Security Appliance continua recebendo mensagens de erro de syslog, conforme mostrado. Isso indica possíveis ataques usando pacotes falsificados ou que podem disparar devido ao roteamento assimétrico.

1.

```
%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port
to IP_address/port flags tcp_flags on interface interface_name
```

ExplicaçãoEsta é uma mensagem relacionada à conexão. Esta mensagem ocorre quando uma tentativa de conexão a um endereço interno é negada pela política de segurança definida para o tipo de tráfego especificado. Os possíveis valores *tcp_flags* correspondem aos flags no cabeçalho TCP que estavam presentes quando a conexão foi negada. Por exemplo, um pacote TCP chegou para o qual não existe um estado de conexão no Security Appliance e ele foi descartado. Os *tcp_flags* neste pacote são FIN e ACK.Os *tcp_flags* são os seguintes:ACK — O número da confirmação foi recebido.FIN — Dados enviados.PSH—O receptor passou dados para o aplicativo.RST—A conexão foi redefinida.SYN—Os números de sequência foram sincronizados para iniciar uma conexão.URG — O ponteiro urgente foi declarado válido.Há muitas razões para a tradução estática falhar no PIX/ASA. Mas, uma razão comum é se a interface de zona desmilitarizada (DMZ) está configurada com o mesmo nível de segurança (0) da interface externa.Para resolver esse problema, atribua um nível de segurança diferente a todas as interfacesConsulte Configurando Parâmetros de Interface para obter mais informações.Essa mensagem de erro também aparece se um dispositivo externo envia um pacote IDENT ao cliente interno, que é descartado pelo PIX Firewall. Consulte Problemas de Desempenho do PIX Causados pelo IDENT Protocol para obter mais informações

2.

```
%PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port
to inside_address/inside_port due to DNS {Response|Query}
```

ExplicaçãoEsta é uma mensagem relacionada à conexão. Essa mensagem será exibida se a conexão especificada falhar devido a um comando **outbound deny**. A variável de protocolo pode ser ICMP, TCP ou UDP.**Ação recomendada:** Use o comando **show outbound** para verificar as listas de saída.

3.
```
%PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst
interface_name: IP_address (type dec, code dec)
```
ExplicaçãoO Security Appliance negou qualquer acesso ao pacote ICMP de entrada. Por padrão, todos os pacotes ICMP têm acesso negado, a menos que especificamente permitido.

4.
```
%PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on
interface interface_name.
```
ExplicaçãoEssa mensagem é gerada quando um pacote chega à interface do Security Appliance que tem um endereço IP de destino de 0.0.0.0 e um endereço MAC de destino da interface do Security Appliance. Além disso, essa mensagem é gerada quando o Security Appliance descartou um pacote com um endereço de origem inválido, que pode incluir um dos seguintes ou algum outro endereço inválido:Rede de loopback (127.0.0.0)Difusão (limitada, direcionada para rede, direcionada para sub-rede e direcionada para todas as sub-redes)O host de destino (land.c)Para aprimorar ainda mais a detecção de pacotes de spoof, use o comando **icmp** para configurar o Security Appliance para descartar pacotes com endereços de origem pertencentes à rede interna. Isso ocorre porque o comando **access-list** foi substituído e não é mais garantido que funcione corretamente.**Ação recomendada:** Determine se um usuário externo está tentando comprometer a rede protegida. Verifique se há clientes configurados incorretamente.

5.
```
%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to
IP_address
```
ExplicaçãoO Security Appliance recebeu um pacote com o endereço IP de origem igual ao destino IP e a porta de destino igual à porta de origem. Essa mensagem indica um pacote falsificado projetado para atacar sistemas. Esse ataque é chamado de ataque à terra.**Ação recomendada:** Se essa mensagem persistir, um ataque pode estar em andamento. O pacote não fornece informações suficientes para determinar a origem do ataque.

6.
```
%PIX|ASA-1-106021: Deny protocol reverse path check from
source_address to dest_address on interface interface_name
```
ExplicaçãoUm ataque está em andamento. Alguém está tentando falsificar um endereço IP em uma conexão de entrada. O unicast RPF, também conhecido como pesquisa de rota reversa, detectou um pacote que não tem um endereço de origem representado por uma rota e supõe que ele faça parte de um ataque em seu dispositivo de segurança.Esta mensagem aparece quando você ativou o unicast RPF com o comando **ip verify reverse-path**. Esse recurso funciona em pacotes de entrada em uma interface. Se estiver configurado no exterior, o Security Appliance verificará os pacotes que chegam do exterior.O Security Appliance procura uma rota com base no endereço de origem. Se uma entrada não for encontrada e uma rota não estiver definida, essa mensagem de registro do sistema será exibida e a conexão será removida.Se houver uma rota, o Security Appliance verificará qual

interface ela corresponde. Se o pacote chegou em outra interface, é uma paródia ou há um ambiente de roteamento assimétrico que tem mais de um caminho até um destino. O Security Appliance não suporta roteamento assimétrico.Se o Security Appliance estiver configurado em uma interface interna, ele verificará as instruções do comando **route** estático ou RIP. Se o endereço de origem não for encontrado, um usuário interno está falsificando seu endereço.**Ação recomendada:** Mesmo que um ataque esteja em andamento, se esse recurso estiver habilitado, nenhuma ação do usuário será necessária. O Security Appliance repele o ataque.**Observação:** o comando **show asp drop** mostra os pacotes ou conexões descartados pelo caminho de segurança acelerado (asp), o que pode ajudá-lo a solucionar um problema. Também indica quando os contadores de queda asp foram removidos pela última vez. Use o comando **show asp drop rpf-violated** no qual o contador é incrementado quando o **ip verify reverse-path** é configurado em uma interface e o Security Appliance recebe um pacote para o qual a pesquisa de rota do IP de origem não produziu a mesma interface em que o pacote foi recebido.

```
ciscoasa#show asp drop frame rpf-violated
  Reverse-path verify failed                         2
```

Nota: Recomendação: Rastreie a origem do tráfego com base no IP de origem impresso nessa próxima mensagem do sistema e investigue por que ele está enviando tráfego falsificado.**Nota: Mensagens de log do sistema:** 106021

7.

```
%PIX|ASA-1-106022: Deny protocol connection spoof from source_address
to dest_address on interface interface_name
```

ExplicaçãoUm pacote correspondente a uma conexão chega em uma interface diferente da interface onde a conexão começou.Por exemplo, se um usuário inicia uma conexão na interface interna, mas o Security Appliance detecta a mesma conexão que chega em uma interface de perímetro, o Security Appliance tem mais de um caminho para um destino. Isso é conhecido como roteamento assimétrico e não é suportado no Security Appliance.Um invasor também pode tentar anexar pacotes de uma conexão a outra como forma de invadir o Security Appliance. Em ambos os casos, o Security Appliance exibe essa mensagem e descarta a conexão.**Ação de recomendação:** Esta mensagem aparece quando o comando **ip verify reverse-path** não está configurado. Verifique se o roteamento não é assimétrico.

8.

```
%PIX|ASA-4-106023: Deny protocol src
[interface_name:source_address/source_port] dst
interface_name:dest_address/dest_port [type {string}, code {code}] by
access_group acl_ID
```

ExplicaçãoUm pacote IP foi negado pela ACL. Esta mensagem é exibida mesmo que você não tenha a opção **log** habilitada para uma ACL.**Ação de recomendação:** Se as mensagens persistirem do mesmo endereço de origem, as mensagens podem indicar uma tentativa de impressão a pé ou de verificação de porta. Entre em contato com os administradores do host remoto.

9.

```
%PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet
from sip/sport to dip/dport on interface if_name.
```

10.

```
%ASA-4-419002: Received duplicate TCP SYN from
in_interface:src_address/src_port to out_interface:dest_address/dest_port with
different initial sequence number.
```

ExplicaçãoEssa mensagem de log do sistema indica que estabelecer uma nova conexão através do dispositivo de firewall resultará em exceder pelo menos um dos limites máximos de conexão configurados. A mensagem de log do sistema se aplica tanto aos limites de

conexão configurados usando um comando estático quanto aos configurados usando o Cisco Modular Policy Framework. A nova conexão não será permitida através do dispositivo de firewall até que uma das conexões existentes seja interrompida, reduzindo assim a contagem atual de conexões para um valor inferior ao máximo configurado.*cnt* — Contagem de conexões atuais*limit* — Limite de conexão configurado*dir* — Direção do tráfego, entrada ou saída*sip* — Endereço IP origem*esportivo* — Porta de origem*dip* — Endereço IP de destino*dport* — Porta de destino*if_name* — Nome da interface na qual a unidade de tráfego é recebida, Principal ou Secundário.**Ação de recomendação:** Como os limites de conexão são configurados por um bom motivo, essa mensagem de log do sistema pode indicar um possível ataque de DoS, caso em que a origem do tráfego pode ser um endereço IP falsificado. Se o endereço IP de origem não for totalmente aleatório, identificar a origem e bloqueá-la usando uma lista de acesso pode ajudar. Em outros casos, obter rastreamentos de farejador e analisar a origem do tráfego ajudariam a isolar o tráfego indesejado do tráfego legítimo.

Recurso básico de detecção de ameaças no ASA 8.x

O Cisco Security Appliance ASA/PIX oferece suporte ao recurso chamado de detecção de ameaças do software versão 8.0 e posterior. Usando a detecção básica de ameaças, o Security Appliance monitora a taxa de pacotes descartados e eventos de segurança devido aos seguintes motivos:

- Negar por listas de acesso
- Formato de pacote inválido (como invalid-ip-header ou invalid-tcp-hdr-length)
- Limites de conexão excedidos (limites de recursos em todo o sistema e limites definidos na configuração)
- Ataque DoS detectado (como um SPI inválido, falha de verificação de Firewall Stateful)
- Falha nas verificações básicas de firewall (esta opção é uma taxa combinada que inclui todas as quedas de pacotes relacionadas ao firewall nesta lista com marcadores. Ele não inclui quedas não relacionadas ao firewall, como sobrecarga de interface, falha de pacotes na inspeção de aplicativos e ataque de verificação detectado.)
- Pacotes ICMP suspeitos detectados
- Falha na inspeção do aplicativo de pacotes
- Sobrecarga de interface
- Detectado um ataque de pesquisa (esta opção monitora os ataques de pesquisa; por exemplo, o primeiro pacote TCP não é um pacote SYN ou a conexão TCP falhou no handshake triplo. A detecção completa de ameaças de verificação (consulte Configuração da Detecção de Ameaças de Verificação para obter mais informações) usa essas informações de taxa de ataque de verificação e atua sobre elas classificando hosts como invasores e os desligando automaticamente, por exemplo).
- Detecção de sessão incompleta, como ataque TCP SYN detectado ou nenhum ataque de sessão UDP de dados detectado.

Quando o Security Appliance detecta uma ameaça, ele envia imediatamente uma mensagem de registro do sistema (730100).

A detecção básica de ameaças afeta o desempenho somente quando há quedas ou possíveis ameaças. Mesmo nesse cenário, o impacto no desempenho é insignificante.

O comando **show threat-detection rate** é usado para identificar possíveis ataques quando você está conectado ao Security Appliance.

```
ciscoasa#show threat-detection rate
                          Average(eps)    Current(eps) Trigger      Total events
  10-min ACL  drop:                0               0       0                16
  1-hour ACL  drop:                0               0       0               112
  1-hour SYN attck:                5               0       2             21438
  10-min  Scanning:                0               0      29               193
  1-hour  Scanning:              106               0      10            384776
  1-hour Bad  pkts:               76               0       2            274690
  10-min  Firewall:                0               0       3                22
  1-hour  Firewall:               76               0       2            274844
  10-min DoS attck:                0               0       0                 6
  1-hour DoS attck:                0               0       0                42
  10-min Interface:                0               0       0               204
  1-hour Interface:               88               0       0            318225
```

Consulte a seção Configuração da Detecção Básica de Ameaças do guia de configuração do ASA 8.0 para obter mais informações sobre a parte da configuração.

Mensagem Syslog 733100

Mensagem de Erro:

`%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt`

O objeto especificado na mensagem de log do sistema excedeu a taxa de limite de burst especificada ou a taxa de limite média. O objeto pode ser uma atividade de descarte de um host, porta TCP/UDP, protocolo IP ou várias quedas devido a possíveis ataques. Indica que o sistema está sob potencial ataque.

Observação: essas mensagens de erro com resolução se aplicam somente ao ASA 8.0 e posterior.

1. Objeto—A origem geral ou específica de uma contagem de taxa de queda, que pode incluir:FirewallPacotes com problemaLimite de taxaAtaque DoSqueda de ACLLimite de Connataque ICMPDigitalizaçãoataque SYNInspecionarInterface
2. rate_ID—A taxa configurada que está sendo excedida. A maioria dos objetos pode ser configurada com até três taxas diferentes para intervalos diferentes.
3. rate_val—Um valor de taxa específico.
4. total_cnt — A contagem total desde que o objeto foi criado ou limpo.

Estes três exemplos mostram como essas variáveis ocorrem:

- Para uma queda de interface devido a uma limitação de CPU ou barramento:
  ```
  %ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per
      second,
  max configured rate is 8000; Current average rate is 2030 per second,
  max configured rate is 2000; Cumulative total count is 3930654
  ```
- Para uma queda de digitalização devido a possíveis ataques:
  ```
  ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per
      second_
  max configured rate is 10; Current average rate is 245 per second_
  ```

```
max configured rate is 5; Cumulative total count is 147409 (35 instances received)
```

- Para pacotes defeituosos devido a possíveis ataques:

```
%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per
    second,
max configured rate is 400; Current average rate is 760 per second,
max configured rate is 100; Cumulative total count is 1938933
```

Ação recomendada:

Execute estas etapas de acordo com o tipo de objeto especificado que aparece na mensagem:

1. Se o objeto na mensagem syslog for um destes:FirewallPacotes com problemaLimite de taxaataque de DoSqueda de ACLLimite de Connataque ICMPDigitalizaçãoataque SYNInspecionarInterfaceVerifique se a taxa de queda é aceitável para o ambiente em execução.
2. Ajuste a taxa de limite da queda específica para um valor apropriado executando o comando **threat-detection rate *xxx***, onde *xxx* é um destes:acl-dropbad-packet-dropconn-limit-dropdos-dropfw-dropicmp-dropinspect-dropinterface-dropameaça de varreduraataque de SYN
3. Se o objeto na mensagem syslog for uma porta TCP ou UDP, um protocolo IP ou uma queda de host, verifique se a taxa de queda é aceitável para o ambiente em execução.
4. Ajuste a taxa de limite da queda específica para um valor apropriado executando o comando **threat-detection rate bad-packet-drop**. Consulte a seção Configuração da Detecção Básica de Ameaças do Guia de Configuração do ASA 8.0 para obter mais informações.

Observação: se você não quiser que o aviso de taxa de queda seja excedido, você pode desativá-lo executando o comando **no threat-detection basic-threat**.

Informações Relacionadas

- Página de suporte dos dispositivos de segurança adaptável Cisco 5500 Series
- Página de suporte do Cisco 500 Series PIX
- Defesas contra ataques de inundação TCP SYN
- Boletim de mitigação aplicada da Cisco: Identificação e redução da exploração das vulnerabilidades de negação de serviço no módulo de switching de conteúdo
- Boletim de mitigação aplicada da Cisco: Identificação e redução da exploração de várias vulnerabilidades nos dispositivos PIX e ASA da Cisco e no módulo de serviços de firewall
- Spoofing de IP
- Suporte Técnico e Documentação - Cisco Systems