Parâmetros de assinatura do IDS do controlador de LAN sem fio

Contents

Introduction

Este documento descreve como configurar assinaturas do Intrusion Detection System (IDS) em um Controlador de LAN Wireless (WLAN) da Cisco (release de software 3.2 ou posteriores).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no software WLAN Controller versão 3.2 e posterior.

Conventions

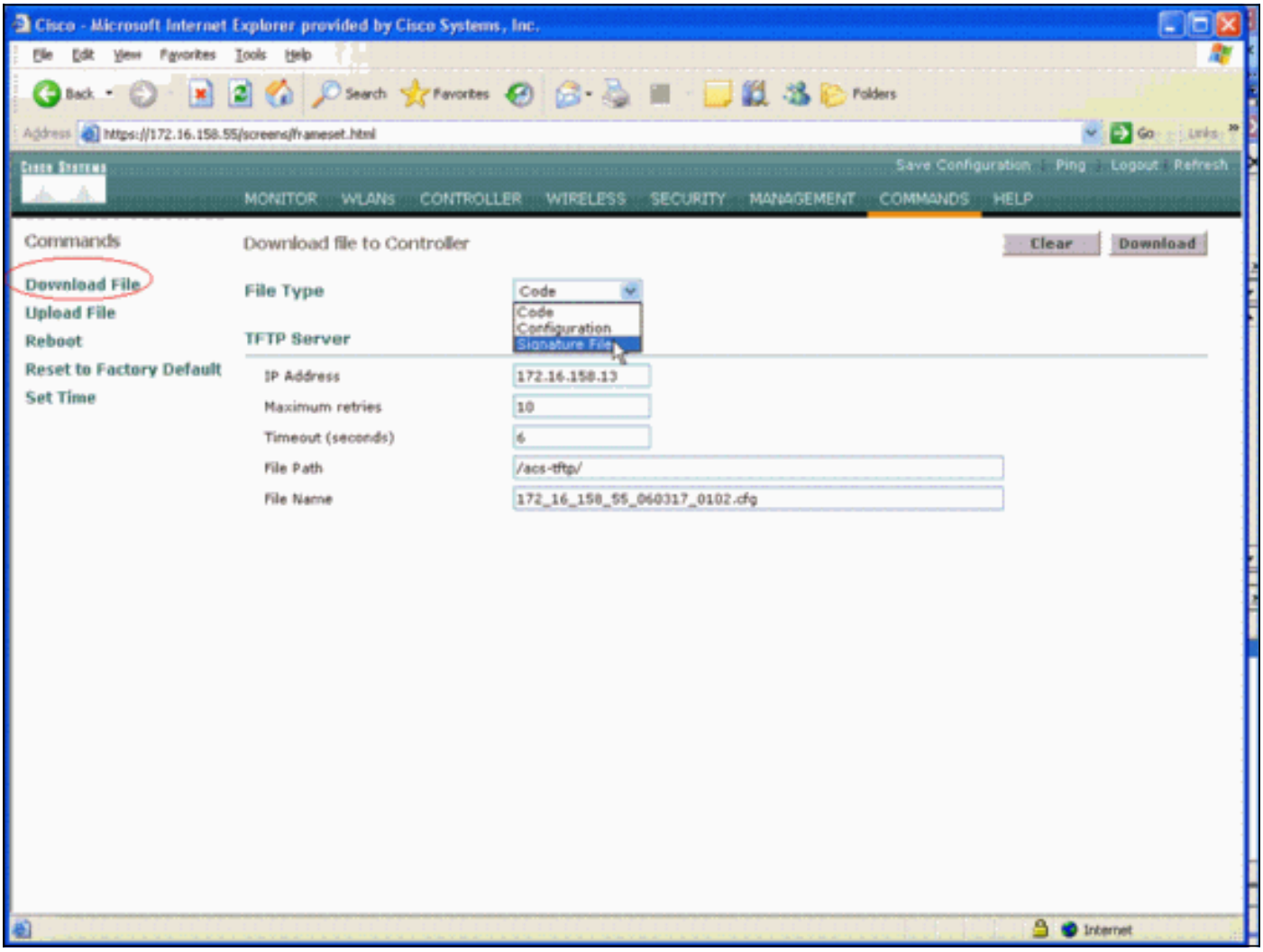
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Você pode carregar o arquivo de assinatura do IDS para edição de assinatura (ou para revisão da documentação). Escolha **Comandos > Carregar arquivo > Arquivo de assinatura**. Para fazer o

download de um arquivo de assinatura IDS modificado, escolha **Commands > Download File > Signature File**. Depois de baixar um arquivo de assinatura para a controladora, todos os access points (APs) conectados à controladora são atualizados em tempo real com os parâmetros de assinatura recém-editados.

Esta janela mostra como baixar o arquivo de assinatura:



O arquivo de texto de assinatura IDS documenta nove parâmetros para cada assinatura IDS. Você pode modificar esses parâmetros de assinatura e gravar novas assinaturas personalizadas. Veja o formato que a seção Parâmetros IDS da Controladora deste documento fornece.

Parâmetros IDS da controladora

Todas as assinaturas *devem* ter este formato:

```
Name = <str>, Ver = <int>, Preced = <int>, FrmType = <frmType-type>, Pattern =
<pattern-format>, Freq = <int>, Interval = <int>, Quiet = <int>, Action = <action-val>,
Desc = <str>
```

O comprimento máximo da linha é de 1000 caracteres. As linhas com mais de 1000 não são analisadas corretamente.

Todas as linhas que começam com `#` no arquivo de texto IDS são consideradas comentários e ignoradas. Também são ignoradas todas as linhas em branco, que são linhas com apenas

espaço em branco ou nova linha. A primeira linha não comentada, não em branco *deve* ter a palavra-chave `Revisão`. Se o arquivo for um arquivo de assinatura fornecido pela Cisco, você não deverá alterar o valor de `Revisão`. A Cisco usa esse valor para gerenciar versões de arquivos de assinatura. Se o arquivo contiver assinaturas criadas pelo usuário final, o valor de `Revisão` *deverá* ser `personalizado` (`Revisão = personalizado`).

Os nove parâmetros de assinatura IDS que você pode modificar são:

- **`Nome`** = nome da assinatura. Esta é uma string exclusiva que identifica a assinatura. O comprimento máximo do nome é 20 caracteres.
- **`Precisa`** = precedência de assinatura. Essa é uma ID exclusiva que indica a precedência da assinatura entre todas as assinaturas definidas no arquivo de assinatura. Deve *haver* um token `preciso` por assinatura.
- **`FrmType`** = tipo de quadro. Este parâmetro pode obter valores da lista `<frmType-val>`. Deve *haver* um token `FrmType` por assinatura. O `<frmType-val>` pode ser apenas uma destas duas palavras-chave:`mgmtdados`O `<frmType-val>` indica se esta assinatura detecta dados ou quadros de gerenciamento.
- **`Padrão`** = padrão de assinatura. O valor do token é usado para detectar pacotes que correspondem à assinatura. Deve *haver* pelo menos um `padrão` token por assinatura. Pode haver até cinco tokens por assinatura. Se a assinatura tiver mais de um token desse tipo, um pacote deverá corresponder aos valores de todos os tokens para que o pacote corresponda à assinatura.Quando o AP recebe um pacote, ele pega o fluxo de bytes que começa em `<offset>`, o faz AND com o `<mask>` e compara o resultado com o `<pattern>`. Se o AP encontrar uma correspondência, o AP considera o pacote uma correspondência com a assinatura. O `<pattern-format>` pode ser precedido pelo operador de negação "`!`". Nesse caso, todos os pacotes que FALHAM na operação de correspondência descrita nesta seção são considerados uma correspondência com a assinatura.
- **`Freq`** = frequência de correspondência de pacotes em pacotes/intervalo. O valor deste token indica quantos pacotes por intervalo de medição devem corresponder a esta assinatura antes que a `ação` de assinatura seja executada. Um valor de 0 indica que a `ação` de assinatura é tomada toda vez que um pacote corresponde à assinatura. O valor máximo para esse token é 65.535. Deve *haver* um token `de freq` por assinatura.
- **`Intervalo`** = intervalo de medição em segundos. O valor desse token indica o período de tempo que o limite (ou seja, o `Freq`) especifica. O valor padrão para este token é 1 segundo. O valor máximo para este token é 3600.
- **`Silencioso`** = tempo de silêncio em segundos. O valor desse token indica a quantidade de tempo que deve passar durante a qual o AP não recebe pacotes que correspondem à assinatura antes que o AP determine que o ataque que a assinatura indica tenha diminuído. Se o valor do token `Freq` for 0, esse token será ignorado. Deve *haver* um token `silencioso` por assinatura.
- **`Ação`** = ação de assinatura. Isso indica o que o AP deve fazer se um pacote corresponder à assinatura. Este parâmetro pode obter valores da lista `<action-val>`. *Deve* haver um token `de ação` por assinatura. O `<action-val>` pode ser apenas uma destas duas palavras-chave:`nenhum` = não fazer nada.`relatório` = informar a correspondência com o switch.
- **`Desc`** = descrição da assinatura. Esta é uma string que descreve a finalidade da assinatura. Quando uma correspondência de assinatura é relatada em uma armadilha de Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol), essa cadeia de caracteres é fornecida à armadilha. O comprimento máximo da descrição é de 100

caracteres. Deve *haver* um token `de descrição` por assinatura.

Assinaturas padrão IDS da controladora

Essas assinaturas IDS são enviadas com a controladora como "assinaturas IDS padrão". Você pode modificar todos esses parâmetros de assinatura, como a seção Parâmetros IDS do controlador descreve.

```
Revision = 1.000
Name = "Bcast deauth", Ver = 0, Preced= 1, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF,
Pattern = 4:0x01:0x01, Freq=30, Quiet = 300, Action = report, Desc="Broadcast
Deauthentication Frame"

Name = "NULL probe resp 1", Ver = 0, Preced = 2, FrmType = mgmt, Pattern =
0:0x0050:0x03FF, Pattern = 36:0x0000:0xFFFF, Freq=1, Quiet = 300, Action = report, Desc =
"NULL Probe Response - Zero length SSID element"

Name = "NULL probe resp 2", Ver = 0, Preced = 3, FrmType = mgmt, Pattern =
0:0x0050:0x03FF, Pattern = !36:0x00:0xFF, Freq=1, Quiet = 300, Action = report, Desc =
"NULL Probe Response - No SSID element"

Name = "Assoc flood", Ver = 0, Preced= 4, FrmType = mgmt, Pattern = 0:0x0000:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Association Request flood"

Name = "Auth Flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0: 0x00b0: 0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Authentication Request flood"

Name = "Reassoc flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0:0x0020:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Reassociation Request flood"

Name = "Broadcast Probe flood", Ver = 0, Preced= 6, FrmType = mgmt, Pattern =
0:0x0040:0x03FF, Pattern = 4:0x01:0x01, Pattern = 24:0x0000:0xFFFF, Freq=50, Quiet = 600,
Action = report, Desc="Broadcast Probe Request flood"

Name = "Disassoc flood", Ver = 0, Preced= 7, FrmType = mgmt, Pattern = 0:0x00A0:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Disassociation flood"

Name = "Deauth flood", Ver = 0, Preced= 8, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Deauthentication flood"

Name = "Res mgmt 6 & 7", Ver = 0, Preced= 9, FrmType = mgmt, Pattern = 0:0x0060:0x03EF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types 6 and 7"

Name = "Res mgmt D", Ver = 0, Preced= 10, FrmType = mgmt, Pattern = 0:0x00D0:0x03FF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-type D"

Name = "Res mgmt E & F", Ver = 0, Preced= 11, FrmType = mgmt, Pattern = 0:0x00E0:0x03EF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types E and F"

Name = "EAPOL flood", Ver = 0, Preced= 12, FrmType = data, Pattern = 0:0x0108:0x03FF,
Pattern = 30:0x888E:0xFFFF, Freq=50, Quiet = 300, Action = report, Desc="EAPOL Flood
Attack"

Name = "NetStumbler 3.2.0", Ver = 0, Preced= 13, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
36:0x466c7572:0xFFFFFFFF, Freq = 1, Quiet = 300, Action = report, Desc="NetStumbler 3.2.0"

Name = "NetStumbler 3.2.3", Ver = 0, Preced= 14, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
36:0x416C6C20:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.2.3"
```

```
Name = "NetStumbler 3.3.0", Ver = 0, Preced= 15, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
36:0x20202020:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.3.0"

Name = "NetStumbler generic", Ver = 0, Preced= 16, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Freq = 1,
Quiet = 600, Action = report, Desc="NetStumbler"

Name = "Wellenreiter", Ver = 0, Preced= 17, FrmType = mgmt, Pattern = 0:0x0040:0x03FF,
Pattern = 24:0x001d746869735f69735f757365645f666f725f77656c6c656e726569:
0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff, Freq = 1, Quiet = 600,
Action = report, Desc="Wellenreiter"
```

Mensagens IDS

Com o Wireless LAN Controller versão 4.0, você pode receber esta mensagem do IDS.

```
Big NAV Dos attack from AP with Base Radio MAC 00:0f:23:xx:xx:xx,
Slot ID 0 and Source MAC 00:00:00:00:00:00
```

Esta mensagem IDS indica que o campo NAV (Network Allocation Vetor) 802.11 no quadro 802.11 sem fio é muito grande e que a rede sem fio pode estar sob um ataque DOS (ou há um cliente com mau comportamento).

Depois de receber esta mensagem IDS, a próxima etapa é rastrear o cliente ofensivo. Você deve localizar o cliente com base na intensidade do sinal com um sniffer sem fio na área ao redor do ponto de acesso ou usar o servidor de localização para localizar sua posição.

O campo NAV é o mecanismo de detecção de portadora virtual usado para atenuar colisões entre terminais ocultos (clientes sem fio que o cliente sem fio atual não consegue detectar quando transmite) em transmissões 802.11. Terminais ocultos criam problemas porque o ponto de acesso pode receber pacotes de dois clientes que podem transmitir ao ponto de acesso, mas não recebem transmissões um do outro. Quando esses clientes transmitem ao mesmo tempo, seus pacotes colidem no ponto de acesso e isso faz com que o ponto de acesso receba nenhum pacote claramente.

Sempre que um cliente sem fio deseja enviar um pacote de dados ao ponto de acesso, ele transmite uma sequência de quatro pacotes chamada sequência de pacote RTS-CTS-DATA-ACK. Cada um dos quatro quadros 802.11 transporta um campo NAV que indica o número de microssegundos para os quais o canal é reservado por um cliente sem fio. Durante o handshake RTS/CTS entre o cliente sem fio e o ponto de acesso, o cliente sem fio envia um pequeno quadro RTS que inclui um intervalo NAV grande o suficiente para completar toda a sequência. Isso inclui o quadro CTS, o quadro de dados e o quadro de confirmação subsequente do ponto de acesso.

Quando o cliente sem fio transmite seu pacote RTS com o NAV definido, o valor transmitido é usado para definir os temporizadores NAV em todos os outros clientes sem fio associados ao ponto de acesso. O ponto de acesso responde ao pacote RTS do cliente com um pacote CTS que contém um novo valor NAV atualizado para contabilizar o tempo já decorrido durante a sequência do pacote. Depois que o pacote CTS é enviado, cada cliente sem fio que pode receber do ponto de acesso atualizou seu temporizador NAV e adia todas as transmissões até que seu temporizador NAV chegue a 0. Isso mantém o canal livre para que o cliente sem fio conclua o processo de transmissão de um pacote ao ponto de acesso.

Um invasor pode explorar esse mecanismo de detecção de portadora virtual ao afirmar um tempo grande no campo NAV. Isso impede que outros clientes transmitam pacotes. O valor máximo para

o NAV é 32767, ou aproximadamente 32 milissegundos em redes 802.11b. Em teoria, um invasor só precisa transmitir aproximadamente 30 pacotes por segundo para obstruir todo o acesso ao canal.

Informações Relacionadas

- Cisco 4400 Series Wireless LAN Controllers
- Cisco 4100 Series Wireless LAN Controllers
- Cisco 2000 Series Wireless LAN Controllers
- Cisco Intrusion Detection System Signature Engines versão 3.1
- Suporte Técnico e Documentação - Cisco Systems