Fixando os controladores do Wireless LAN (WLC)

Índice

Introdução

Este documento oferece uma vista geral de diversos aspectos importantes necessários segurar a interação da Segurança entre os controladores do Wireless LAN (WLC) e a rede onde são conectados. Este documento centra-se primeiramente sobre o controle de tráfego, e não se endereça políticas de segurança WLAN, AAA ou WPS.

Os assuntos que afetam o tráfego com destino “ao controlador” são cobertos neste documento, e não relacionados para traficar que é relacionado ao “usuário à rede”.

Nota: Valide mudanças antes de aplicá-las a sua rede, como alguns dos exemplos neste documento podem obstruir o acesso administrativo a seus controladores se aplicados incorretamente.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento de como configurar o WLC e o Access point de pouco peso (REGAÇO) para a operação básica
- Conhecimento básico do modelo osi
- Compreendendo como o Access Control List (ACL) trabalha

Componentes Utilizados

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

- Cisco 2000/2100/4400 Series WLC que executa o firmware 4.2.130.0, 5.2.157.0 ou mais tarde

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

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

Manejo de tráfego nos WLC

Um componente crítico na segurança de rede é controle de tráfego. Em todo o desenvolvimento, é muito importante para os tipos de bloco de tráfego que chegam em dispositivos a fim impedir as edições de segurança potencial (DoS, perda de informação, agravamento do privilégio, etc.).

No WLC, o controle de tráfego é afetado por um fato importante: há dois componentes que seguram o tráfego no dispositivo:

- CPU — Processador principal que toma de toda a atividade do Gerenciamento, de controle RRM, LWAPP, de autenticação, de DHCP, etc.
- NPU — Processador de rede que toma do encaminhamento de tráfego rápido para os clientes autenticados (prendidos ao Sem fio e vice-versa).

Esta arquitetura permite um encaminhamento de tráfego rápido, e reduz a carga no CPU principal, que podem então dedicar todos seus recursos para tarefas de nível elevado.

Esta arquitetura é encontrada nos 4400, em WiSM e em 3750 controladores integrados. Para 2106 e NM-WLC e controladores relacionados, a transmissão é feita no software, também pelo CPU principal. Consequentemente, toma um imposto mais alto no CPU. É por isso estas Plataformas oferecem um apoio mais baixo do usuário e da contagem AP.

Tráfego de controlo

Quando você quer ao filtrar tráfego com relação a um WLC, é importante saber se este é um usuário ao tráfego de rede ou é para o CPU principal.

- Para todo o tráfego ao CPU, por exemplo, os protocolos de gestão tais como o SNMP, o HTTPS, o SSH, o telnet, ou os protocolos dos serviços de rede tais como o raio ou o DHCP, usam um “CPU ACL”.
- Para todo o tráfego a e de um cliente Wireless, incluindo o tráfego que atravessa um túnel de EoIP (acesso do convidado), uma relação ACL, um WLAN ACL, ou a pelo usuário ACL são usados.

O tráfego é definido “ao CPU”, como o tráfego que está entrando no controlador, com o destino ao endereço IP de gerenciamento, a algum das interfaces dinâmica ou ao endereço de porta do serviço. O gerenciador AP não segura nenhum outro tráfego exceto LWAPP/CAPWAP.

Acesso de gerenciamento de controlo

Os WLC têm da “um controle de acesso nivelado sessão” para protocolos de gestão. É importante compreender como trabalham a fim impedir a avaliação incorreta no que é permitido ou não permitido pelo controlador.

Os comandos restringir que protocolos de gestão são permitidos são (em um espaço global):

- **o ssh da rede da configuração permite|desabilitação** — Isto permite ou desabilita o serviço SSH no controlador. Iss está habilitado por padrão. Uma vez deficiente, a porta (TCP 22) não será alcançável.
- **o telnet da rede da configuração permite|desabilitação** — Isto permite ou desabilita o serviço de telnet no controlador. Isto é desabilitado à revelia. Uma vez deficiente, a porta (TCP 23) não será alcançável.
- **o HTTP da rede da configuração permite|desabilitação** — Isto permite ou desabilita o serviço HTTP no controlador. A porta (TCP 80) não é uma alcançável mais longo. Isto é desabilitado à revelia.
- **os https da rede da configuração permitem|desabilitação** — Isto permite ou desabilita o serviço dos https no controlador. Iss está habilitado por padrão. Uma vez deficiente, a porta (TCP 443) não será alcançável.
- **a versão v1|v2|v3 SNMP da configuração permite|desabilitação** — Isto permite ou desabilita versões específicas do serviço SNMP no controlador. Você precisa de desabilitar tudo para impedir o acesso SNMP ao controlador, a menos que usando um ACL.
- **o Mgmt-através-Sem fio da rede da configuração permite|desabilitação** — Isto impede que os clientes associados a este controlador lhe podem protocolos do gerenciamento de acesso (ssh, https, etc.). Isto não impede nem fecha as portas correspondente TCP do ponto de vista do dispositivo Wireless. Isto significa que um dispositivo Wireless, quando este é ajustado para desabilitar, pode abrir uma conexão de SSH, se o protocolo é permitido. O usuário pôde ver uma alerta de nome de usuário gerada pelo demônio SSH, porém a sessão se fecha assim que você tentasse datilografar um username.
- **a Mgmt-através-dinâmico-relação da rede da configuração permite|desabilitação** — Isto impede que os dispositivos no mesmo VLAN que o controlador lhe podem protocolos do gerenciamento de acesso (ssh, https, etc.) ao endereço correspondente da interface dinâmica nesse VLAN. Isto não impede nem fecha as portas correspondente TCP do ponto de vista do dispositivo. Isto significa que um dispositivo, quando este é ajustado para desabilitar, pode

abrir uma conexão de SSH, se o protocolo é permitido. O usuário pôde ver uma alerta de nome de usuário gerada pelo demônio SSH, porém a sessão se fecha assim que você tentasse datilografar um username. Adicionalmente, o endereço de gerenciamento permanecerá sempre acessível de uma interface dinâmica VLAN, a menos que um CPU ACL estiver no lugar.

Por exemplo, esta é a configuração usando a informação acima:

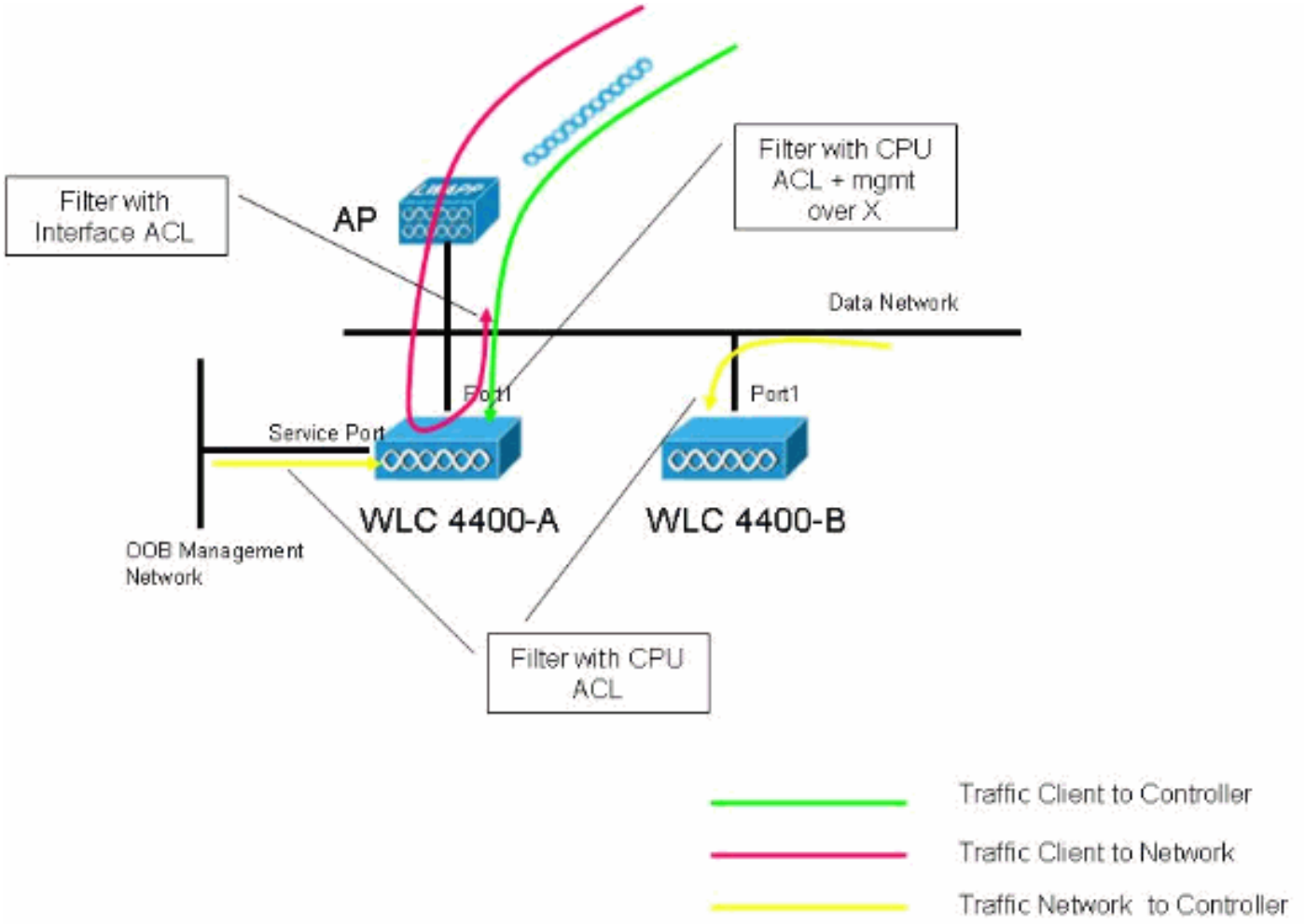
```
(Cisco Controller) >show network summary


RF-Network Name............................. 4400
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Enable
Secure Shell (ssh).......................... Enable
Telnet...................................... Disable
Ethernet Multicast Mode..................... Enable   Mode: Ucast
Ethernet Broadcast Mode..................... Disable
AP Multicast Mode........................... Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority............................ Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Mesh Full Sector DFS........................ Enable
Over The Air Provisioning of AP's........... Enable
Apple Talk ................................. Disable
AP Fallback ................................ Enable
Web Auth Redirect Ports .................... 80
Fast SSID Change ........................... Disabled
802.3 Bridging ............................. Disable
IP/MAC Addr Binding Check .................. Enabled


(Cisco Controller) >show acl cpu

CPU Acl Name................................ NOT CONFIGURED
Wireless Traffic............................ Disabled
Wired Traffic............................... Disabled
```

Você pode concluir aquele:

- O telnet e o HTTP não estarão disponíveis, assim que todo o tráfego de gerenciamento interativo ao controlador será feito com HTTPS/SSH (cifrado).
- Um usuário Wireless associado a este controlador não poderá obter o acesso administrativo.
- Se um usuário Wireless, associado a este controlador, faz uma varredura da porta, mostrará o SSH e o HTTP como aberto, mesmo que nenhum acesso administrativo seja permitido.
- Se um usuário prendido (mesmo VLAN que uma interface dinâmica) faz uma varredura da porta, mostrará o SSH e o HTTP como aberto, mesmo que nenhum acesso administrativo seja permitido.

Éimportante notar que nos ambientes com o mais de um controlador no mesmo grupo da mobilidade, o relacionamento do que é um cliente Wireless é somente ao controlador atualmente

associado. Consequentemente, se um cliente é associado ao controlador A, a seguir para um controlador B no mesmo grupo da mobilidade, este cliente é um dispositivo que vem de uma relação VLAN/dynamic. Isto é importante de levar em consideração no Gerenciamento sobre o ajuste wireless. Veja este diagrama para um exemplo de onde pôr uma limitação do tráfego, e que comandos podem afetar cada ponto de ingresso:



CPU ACL

Sempre que você quer controlar que os dispositivos podem falar ao CPU principal, um CPU ACL é usado. É importante mencionar diversas características para estes:

- Filtrar tráfego CPU ACL somente para o CPU, e não nenhum tráfego que retira ou gerado pelo CPU.**Nota:** Para o 5500 Series WLC nas versões 6.0 e mais recente, o CPU ACL é aplicável para o tráfego originado do WLC também. Para as outras Plataformas WLC, este comportamento é executado nas versões 7.0 e mais recente. Também, ao criar campos de sentido CPU ACL não tenha nenhum impacto.
- O apoio total para CPU ACL para todo o gerenciamento IP e endereços dinâmicos do controlador está somente atual em 4.2.130.0 e mais tarde.
- O CPU ACL que obstrui o tráfego da porta do serviço está somente dentro 5.0 atuais e mais atrasado.
- Quando um CPU ACL é projetado, é importante permitir o tráfego de controle entre controladores. O comando **sh das regras** pode oferecer uma ideia rápida do tráfego permitida a CPU ACL em condições normal.
- O controlador tem um grupo de regras de filtragem para os processos internos, que podem

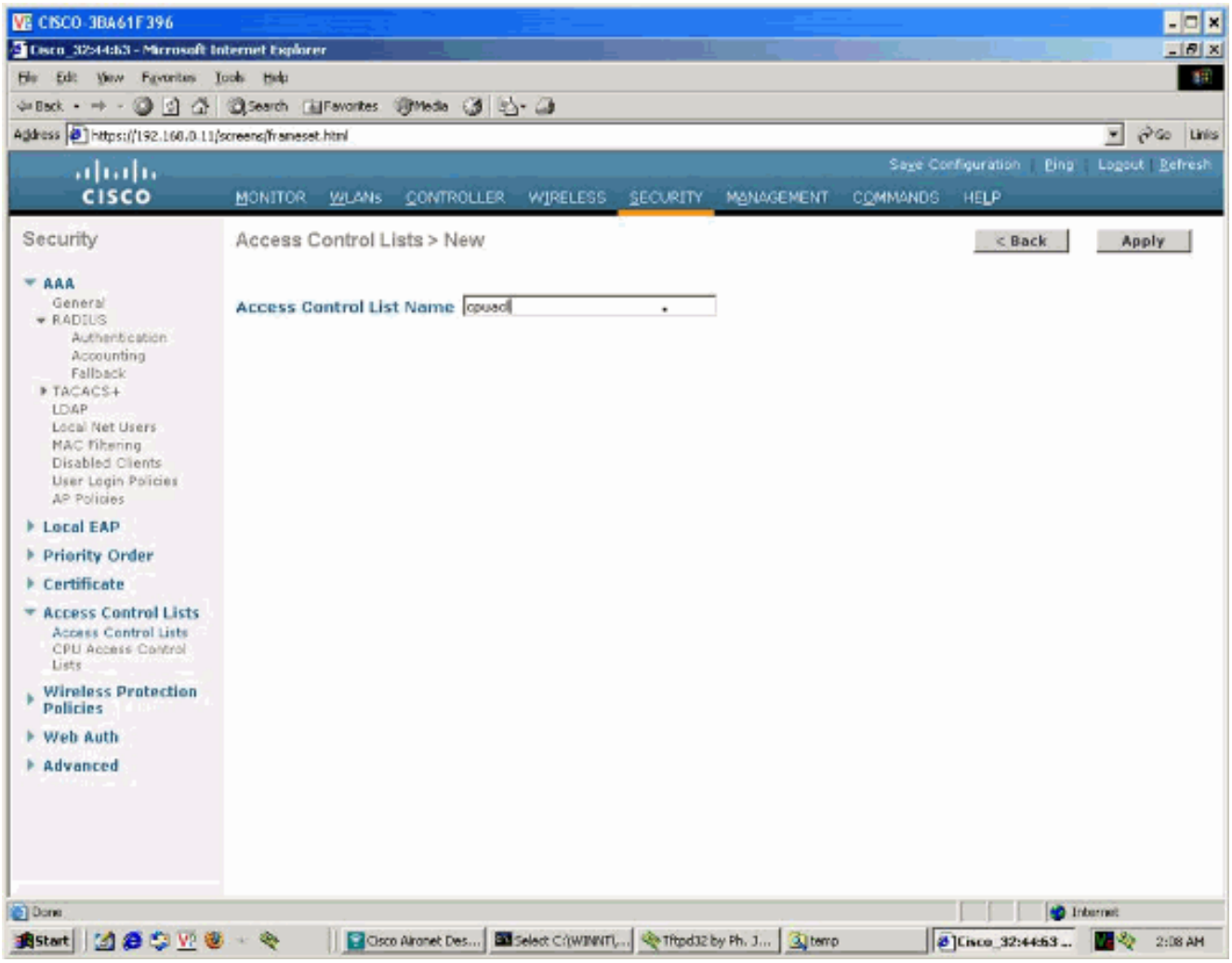
ser verificados com o comando **sh das regras**. Os ACL não afetam estas regras, nem podem estas regras estar ligada - - mosca alterada. O CPU ACL toma a precedência sobre elas.

- O tráfego de dados LWAPP ou CAPWAP não é afetado por regras CPU ACL em 4400 controladores baseados, tráfego de controle é afetado (se fazendo um ACL restrito, você precisa do permitir explicitamente).**Nota:** O tráfego de controle CAPWAP não é afetado por CPU ACL.

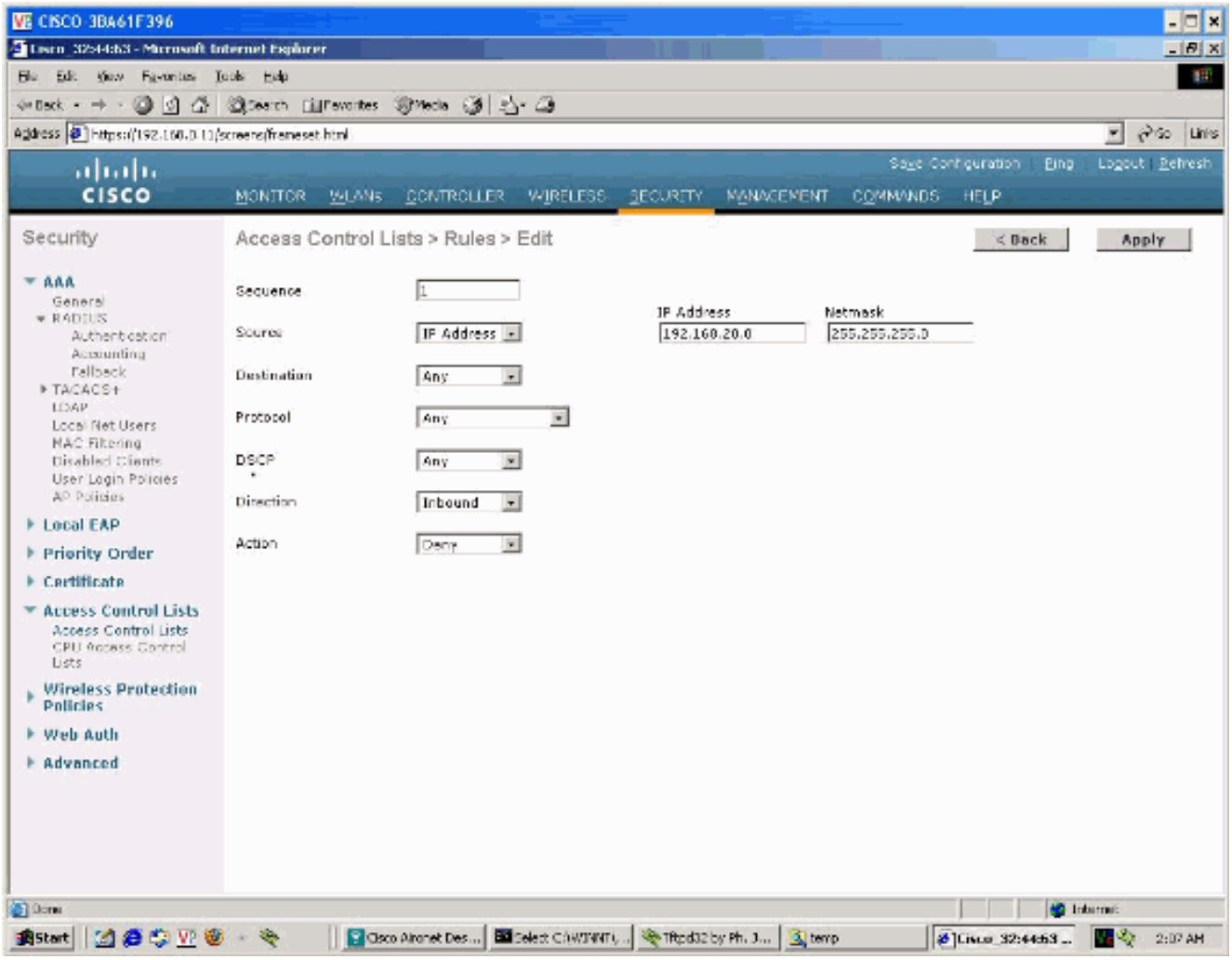
Exemplo

Por exemplo, você pôde querer obstruir todo o tráfego que vem do interface/VLAN dinâmico (192.168.20.0/24) onde os usuários são associados, para o CPU, mas todo o outro tráfego é permitido. Isto não deve impedir clientes Wireless para obter um endereço negociável DHCP.

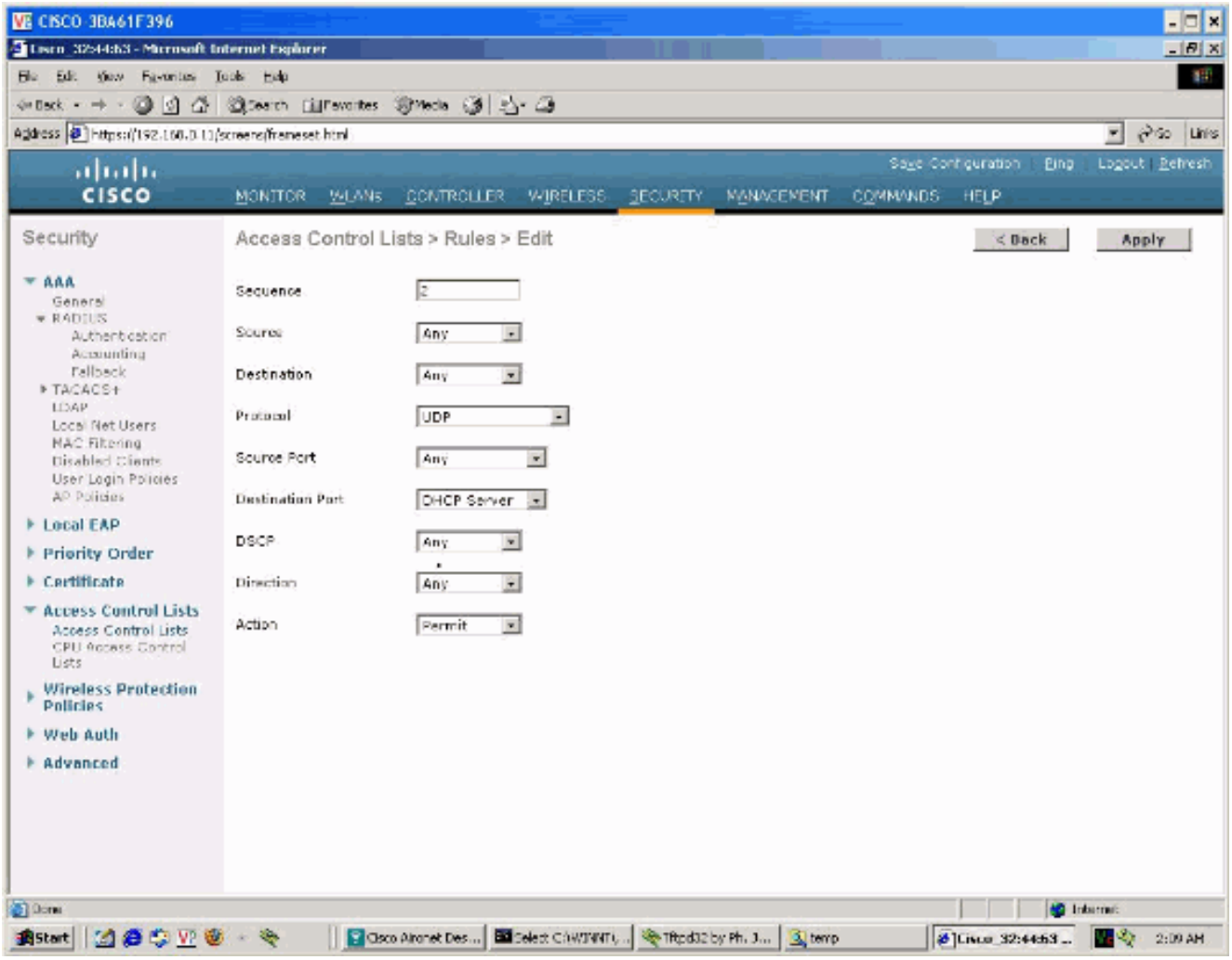
1. Como a primeira etapa, uma lista de acessos é criada:



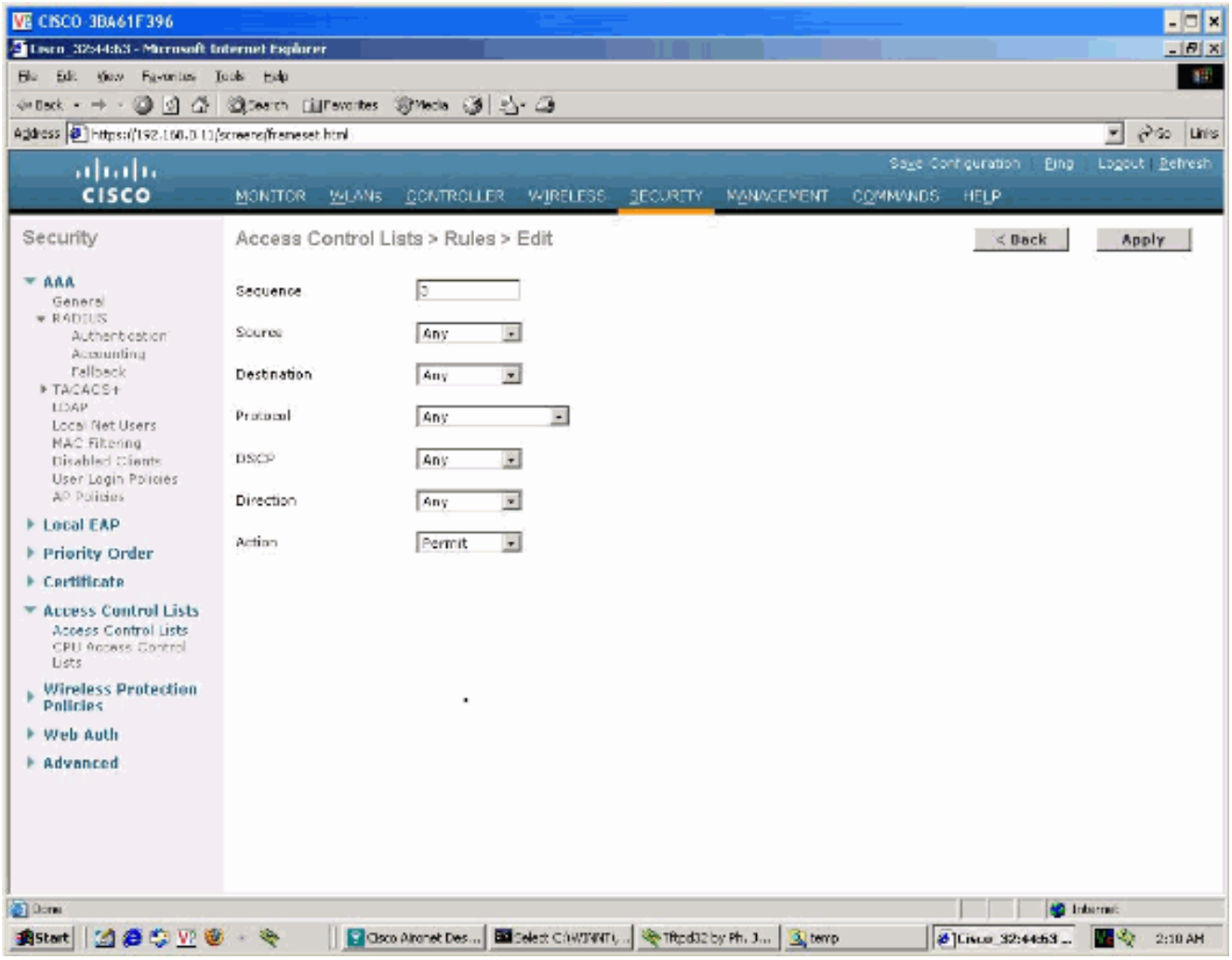
2. Clique **adicionam a regra nova**, e ajustam-na para obstruir todo o tráfego de origem que vem de 192.168.20.0/24 a todo o destino.



3. Adicionar uma segunda regra, para o tráfego DHCP, com porta de servidor de destino, mas com ação da
licença:

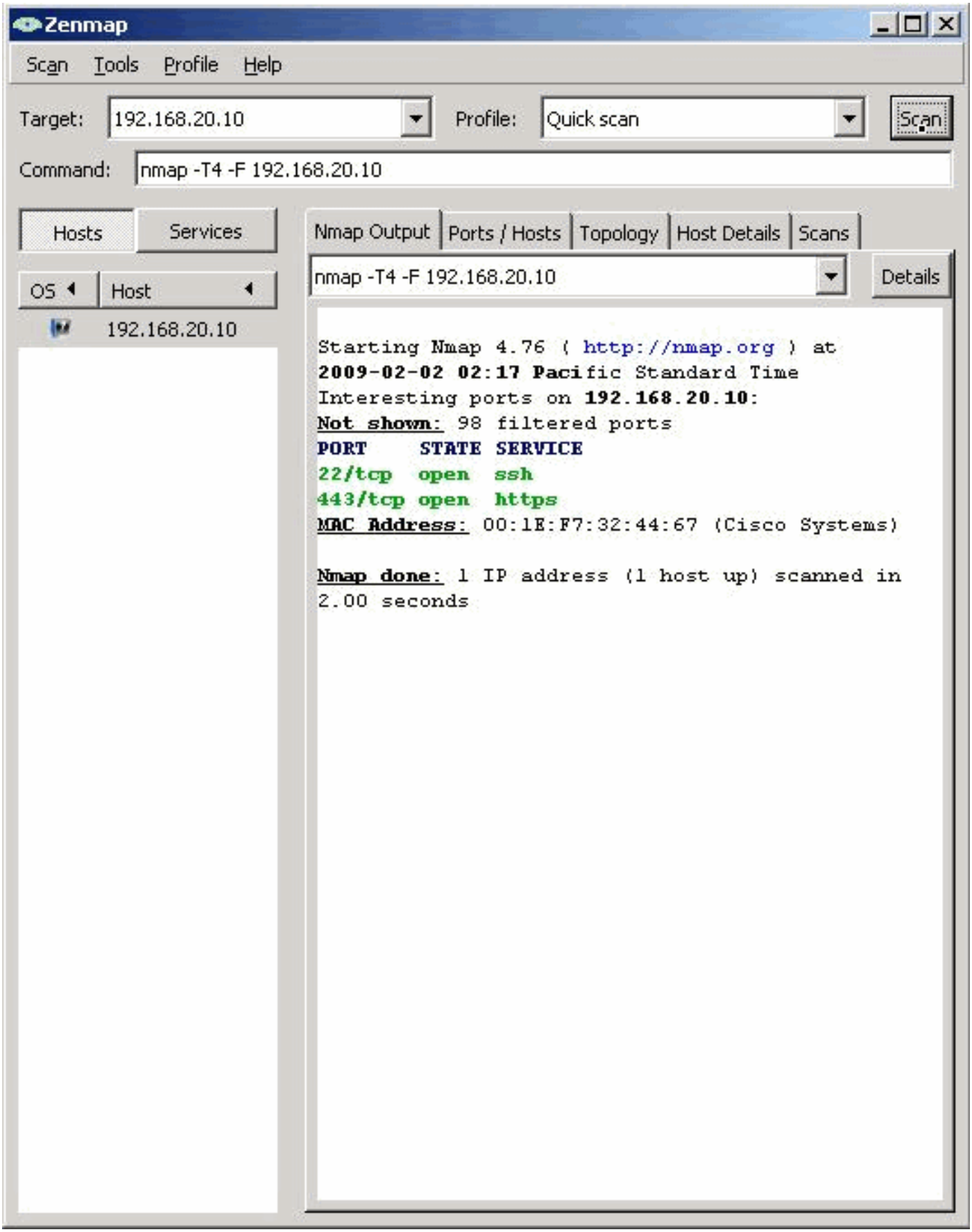


Então, por políticas de segurança da empresa, todo tráfego restante é permitido:



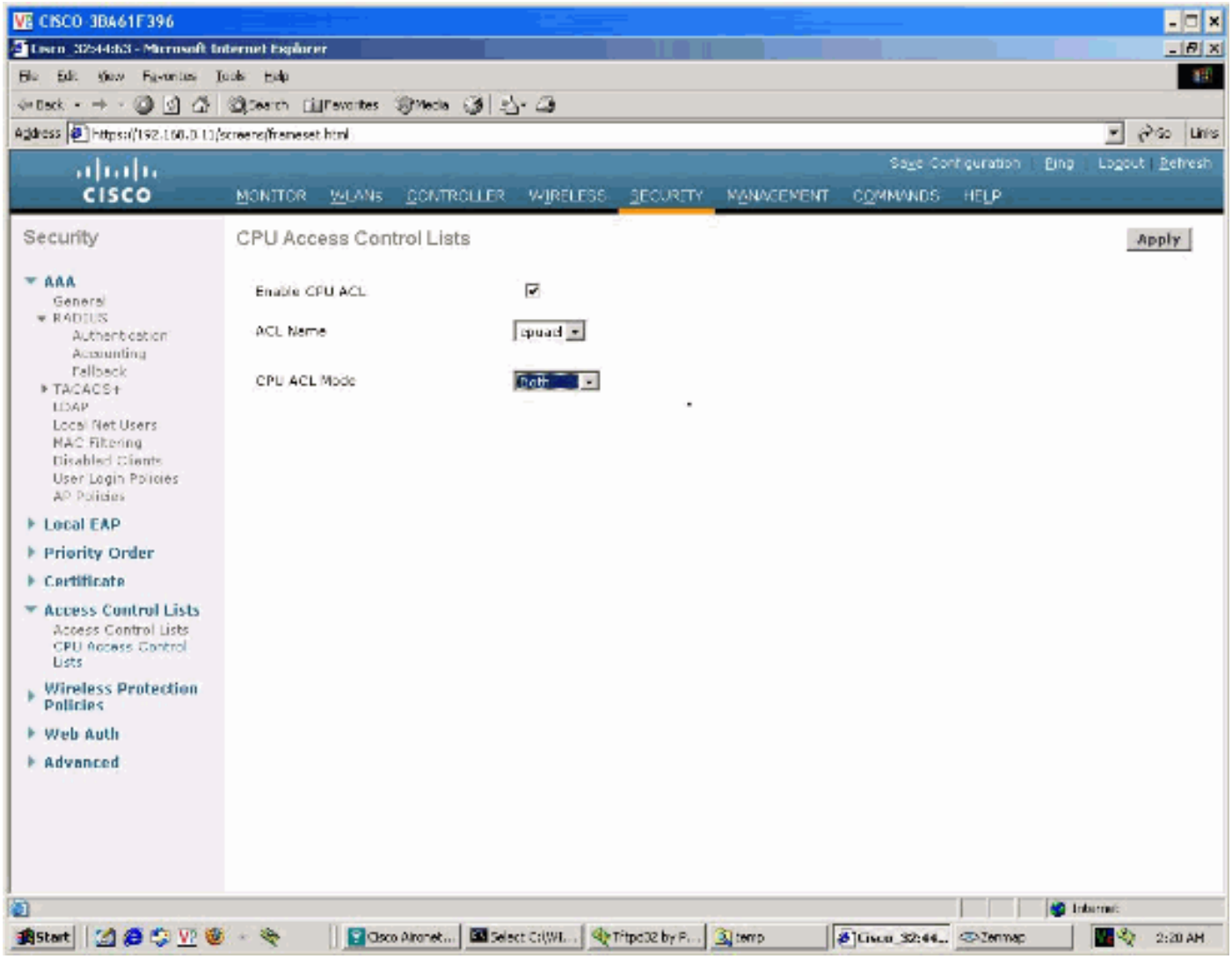
Teste antes de CPU ACL

A fim validar o efeito do CPU ACL, você pode executar uma varredura rápida de um cliente Wireless associado no estado EXECUTADO a fim ver as portas aberta atuais, com base na configuração, antes de aplicar o CPU ACL:



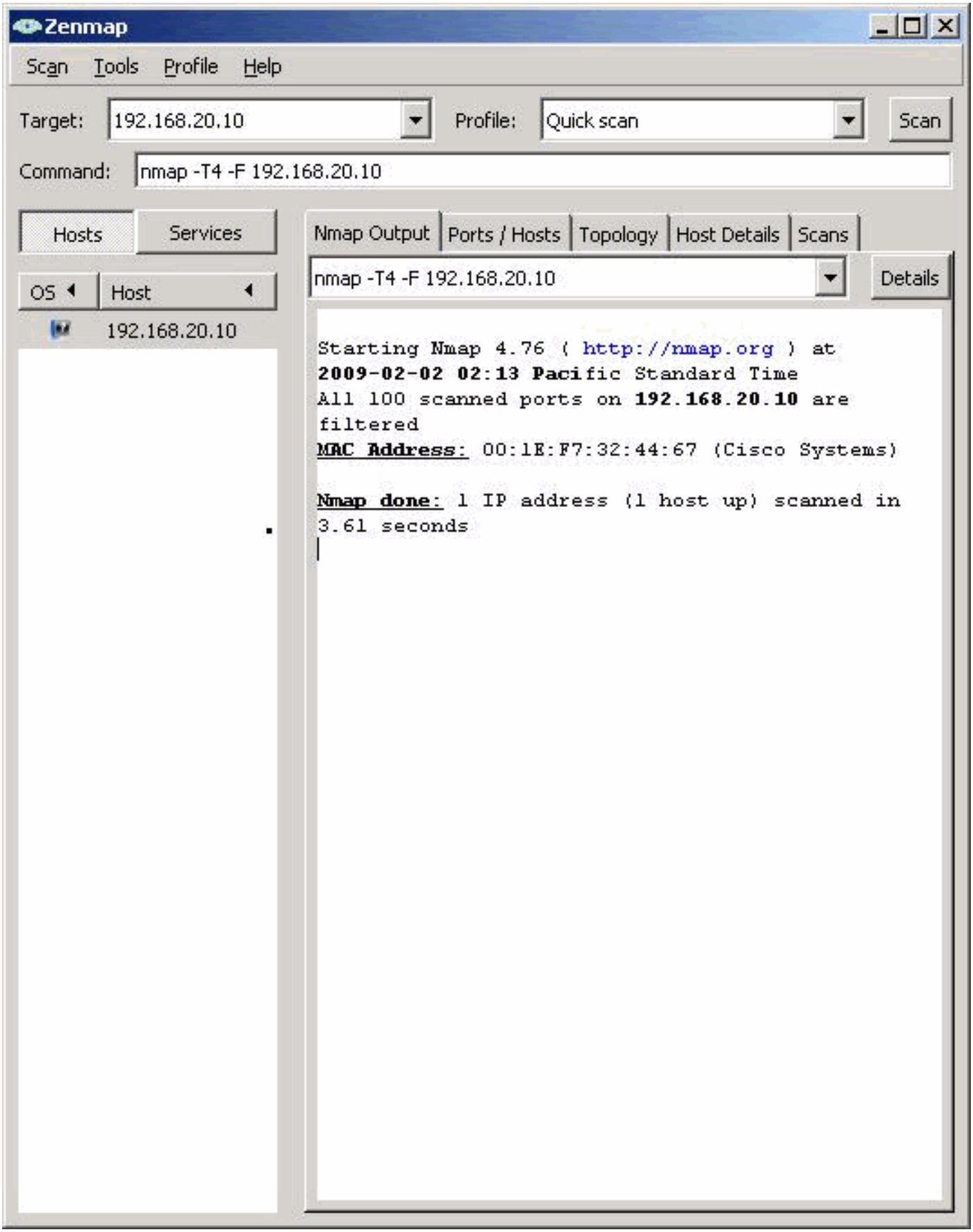
Teste após o CPU ACL

Vá à **Segurança > ao Gerenciamento > ao Access Control List CPU**. O clique **permite CPU ACL**, e seleciona o ACL que foi criado previamente. Então, escolha **ambos** como o sentido a fim segurar isto é aplicado para traficar dos clientes Wireless, e dos outros dispositivos na interface dinâmica VLAN:



Nota: Não há nenhum sentido para o tráfego processador central acl de 7.0 avante para todas as Plataformas WLC e somente para WLC5500 em 6.0.

Agora, se a mesma varredura usada antes é repetida, todas as portas do controlador são mostradas como fechadas:



CPU restrito ACL

Se a procura das políticas de segurança “nega alguma” como por último alinha para uma política, é importante compreender que há diversos tipos de tráfego enviados entre o controlador no mesmo grupo da mobilidade para RRM, a mobilidade e as outras tarefas, e que você pôde ter o tráfego proxied pelo controlador a se para algumas operações, em particular DHCP, onde o

controlador no modo de proxy DHCP (o padrão) pode se gerar o tráfego com destino UDP 1067 para processar.

Para uma lista completa das portas permitidas pelas regras internas da transmissão do padrão, verifique a saída do comando **sh das regras**. A análise da lista completa é além do alcance deste documento.

Você pode verificar que regras ACL estão sendo batidas pelo tráfego com o **comando start do contador acl da configuração**. Os contadores podem ser indicados com o comando **sh do detalhe ACLNAME acl**.

Políticas de plano de controle

Um aspecto de proteger um dispositivo de rede, é certificar-se de que não está oprimido com mais tráfego de gerenciamento que pode processar. Em todos os controladores, após o código 4.1, há uma limitação plana do controle permitida à revelia, que retroceda dentro se o tráfego para o CPU excede o 2 mbps.

Em redes ocupadas, é possível observar a limitação de fato (por exemplo, o monitor deixado cair sibila ao CPU). A característica pode ser controlada com o **comando rate avançado configuração**. Você pode somente permitir ou desabilitar as, mas taxas não ajustadas ou contra que tráfego atuará primeiramente.

Em operações normal, recomenda-se isto é saido permitido.

Criptografia forte para o tráfego HTTP

Àrevelia, o controlador oferece ambas as cifras altos e baixos da força segurar a compatibilidade com navegadores mais velhos durante a instalação HTTPS. O controlador tem disponível de 40 bit RC4, 56 bit DES, até bit AES 256. A seleção da cifra a mais forte é feita pelo navegador.

A fim certificar-se de que somente as cifras fortes estão usadas, você pode permiti-los com o **comando enable alto da cifra-opção do secureweb da rede da configuração**, tão os somente 168 3DES ou o 128 AES e uns comprimentos mais altos da cifra são oferecidos pelo controlador no acesso do gerenciamento HTTPS.

Controle de sessão

Ajustes do telnet/SSH

Àrevelia, o controlador permite um máximo dos usuários simultâneos 5, com um intervalo dos minutos 5. É crítico que estes valores estão configurados adequadamente em seu ambiente, porque os ajustar a ilimitado (zero) pode abrir a porta à recusa de serviço potencial contra controladores, se os usuários deviam tentar um ataque de força bruta contra eles. Este é um exemplo das configurações padrão:

```
(Cisco Controller) >show sessions

CLI Login Timeout (minutes)..... 5
Maximum Number of CLI Sessions..... 5
```

Recorde isso pelo projeto, mesmo se o Gerenciamento sobre o Sem fio ou a interface dinâmica é desabilitado, um dispositivo pode ainda fazer uma conexão de SSH ao controlador. Este é um CPU que taxa a tarefa, e o WLC limita o número de sessões simultâneas, e durante quanto tempo usando estes parâmetros.

Os valores podem ser ajustados com o **comando sessions da configuração**.

Porta de Console

A porta serial tem um valor de timeout separado, que seja ajustado aos minutos 5 à revelia, mas é mudado geralmente a 0 (ilimitado) durante sessões de Troubleshooting.

```
Cisco Controller) >show serial

Serial Port Login Timeout (minutes)......... 5
Baud Rate.................................... 9600
Character Size............................... 8
Flow Control:................................ Disable
Stop Bits.................................... 1
Parity Type:................................. none
```

Éaconselhável usar o padrão dos minutos 5. Isto impede qualquer um que tem o acesso físico ao controlador para ganhar o acesso administrativo, caso que um usuário conectado na porta de Console deixa a sessão aberta. Os valores podem ser ajustados com o **comando serial da configuração**.

Unindo tudo

Após ter verificado o aspecto diferente de fixar um WLC, isto pode ser resumido:

- É importante impedir dispositivos diferentes das estações de gerenciamento recortadas para alcançar o WLC, não somente protocolos NON-usados de desabilitação, mas igualmente limitando o acesso na camada 4/layer 3 com CPU ACL.
- A limitação da taxa deve ser permitida (é à revelia).
- O acesso de controlo através do **Gerenciamento sobre comandos x** não é bastante para as instalações seguras, porque os usuários enlatam ainda protocolos do gerenciamento de acesso que falam diretamente ao endereço IP de gerenciamento, usando o CPU e os recursos de memória.

Práticas da Segurança

Estão aqui algumas das práticas da Segurança:

- Crie o acesso deixando cair CPU ACL de toda a interface dinâmica VLAN ou de sub-redes. Contudo, permita o tráfego DHCP à porta de servidor (67) assim que os clientes podem obter o endereço negociável DHCP se o proxy DHCP é permitido (é à revelia). Se a interface dinâmica tem um endereço IP público, recomenda-se ter a regra ACL que nega todo o tráfego dos origens desconhecida ao endereço da interface dinâmica.
- Ajuste todas as regras ACL como de entrada ou com sentido, e marque-as tão aplicadas quanto **ambos** (opção prendida e wireless).Como validar:`(Cisco Controller) >show acl cpu`

```
CPU Acl Name.............................. acl1
Wireless Traffic.......................... Enabled
Wired Traffic............................. Enabled
```

- Permita a limitação do plano do controle (é permitida à revelia).Como validar:`(Cisco Controller) >show advanced rate`

```
Control Path Rate Limiting.....................  Enabled
```

- Use sempre os protocolos de gestão cifrados (HTTPS, SSH). Esta é a configuração padrão para o Gerenciamento interativo. Para o SNMP você pôde precisar de permitir o V3 de permitir tráfego SNMP cifrado/autenticado. Recorde recarregar o controlador se você faz mudanças à configuração de SNMP.Isto é como validar:`(Cisco Controller) >show network summary`

```
RF-Network Name........................... 4400
Web Mode.................................. Disable
Secure Web Mode........................... Enable
Secure Web Mode Cipher-Option High........ Enable
Secure Web Mode Cipher-Option SSLv2....... Enable
Secure Shell (ssh)........................ Enable
Telnet.................................... Disable
...
```

- Permita a criptografia alta para o HTTPS (isto é desabilitado à revelia).
- É uma boa ideia estabelecer um certificado de servidor validado para o acesso HTTPS a seu controlador (assinado por seu CA confiado), substituindo o certificado assinado do auto instalado à revelia.
- Ajuste o intervalo da sessão e do console aos minutos 5.`(Cisco Controller) >show serial`

```
Serial Port Login Timeout (minutes)......... 5
Baud Rate................................... 9600
Character Size.............................. 8
Flow Control:............................... Disable
Stop Bits................................... 1
Parity Type:................................ none
```

```
(Cisco Controller) >show sessions

CLI Login Timeout (minutes)............ 5
Maximum Number of CLI Sessions......... 5
```

Informações Relacionadas

- Access point de pouco peso FAQ
- Perguntas Frequentes de Troubleshooting de Controladoras Wireless LAN (WLC)
- Cisco Wireless LAN Controller Module - Perguntas e Respostas
- Gerência de recursos de rádio sob redes Wireless unificadas
- Suporte Técnico e Documentação - Cisco Systems