Autenticação de leap em um servidor Radius local

Índice

Introdução

Este documento fornece uma configuração de exemplo para a autenticação do protocolo lightweight extensible authentication (PULO) em um Access point ®-baseado IO, que serva os clientes Wireless, assim como atua como um servidor Radius local. Isto é aplicável a um Access point IO que execute 12.2(11)JA ou mais tarde.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Familiaridade com a GUI ou CLI do IOS
- Familiaridade com os conceitos por trás de uma autenticação de LEAP

Componentes

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

- Access point da série do Cisco Aironet 1240AG

- Cisco IOS Software Release 12.3(8)JA2
- Adaptador Wireless do 802.11 a/b/g/do Cisco Aironet que executa o utilitário de Desktop de Aironet 3.6.0.122
- Hipótese de haver apenas um VLAN na rede

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.

Vista geral da característica local do servidor Radius

Um servidor de raio externo é usado geralmente para autenticar usuários. Em alguns casos, esta não é uma solução possível. Nestas situações, um Access point pode ser feito para atuar como um servidor Radius. Aqui, os usuários são autenticados contra o base de dados local configurado no Access point. Isto é chamado uma característica local do servidor Radius. Você pode igualmente fazer outros Access point no uso da rede que o servidor Radius local caracteriza em um Access point. Para obter mais informações sobre disto, refira configurar outros Access point para usar o autenticador local.

Configurar

A configuração descreve como configurar o PULO e a característica local do servidor Radius em um Access point. A característica local do servidor Radius foi introduzida no Cisco IOS Software Release 12.2(11)JA. Refira a autenticação de leap com o servidor Radius para a informações de fundo em como configurar o PULO com um servidor de raio externo.

Como a maioria dos algoritmos de autenticação baseados em senha, o LEAP Cisco é vulnerável a ataques de dicionários. Esse não é um novo ataque ou uma nova vulnerabilidade do Cisco LEAP. Você deve criar uma política de senha elaborada para abrandar ataques do dicionário, aquele incluiria senhas elaboradas e frequentaria senhas novas. Refira o ataque do dicionário no PULO de Cisco para obter mais informações sobre dos ataques do dicionário e como impedi-los.

Este documento supõe esta configuração para o CLI e o GUI:

1. O endereço IP de Um ou Mais Servidores Cisco ICM NT do Access point é **10.77.244.194**.
2. O SSID usado é **Cisco**, que é traçado ao **VLAN1.**
3. Os nomes de usuário são **usuário1** e **user2**, que são traçados ao **usuário de teste do** grupo.

Configuração de CLI

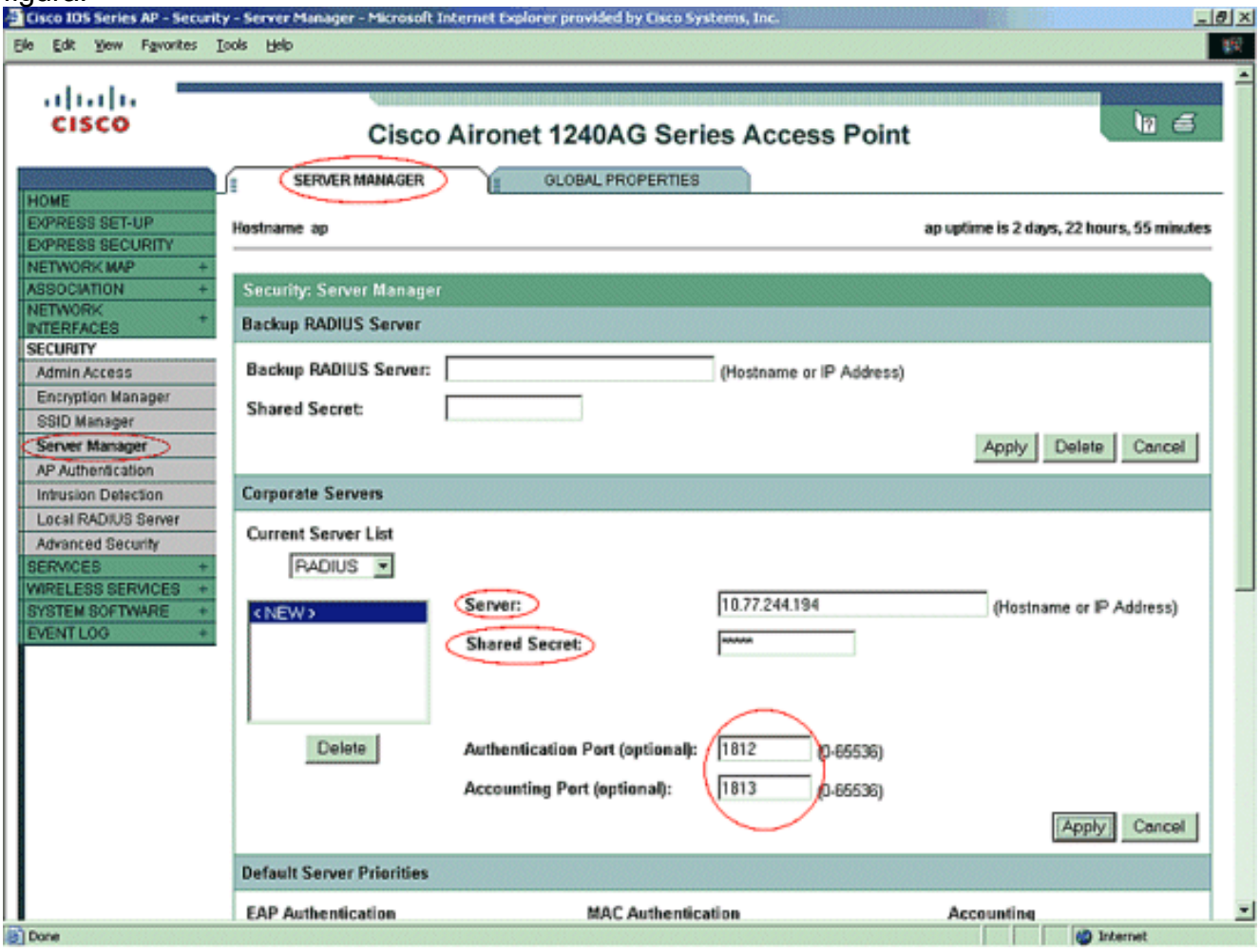
Ponto de acesso
ap#**show running-config** Building configuration... . . . **aaa new-model** *!--- This command reinitializes the authentication, !--- authorization and accounting*

```
functions. ! ! aaa group server radius rad_eap server
10.77.244.194 auth-port 1812 acct-port 1813 !--- A
server group for RADIUS is created called "rad_eap" !---
that uses the server at 10.77.244.194 on ports 1812 and
1813. . . . aaa authentication login eap_methods group
rad_eap !--- Authentication [user validation] is to be
done for !--- users in a group called "eap_methods" who
use server group "rad_eap". . . . ! bridge irb !
interface Dot11Radio0 no ip address no ip route-cache !
encryption vlan 1 key 1 size 128bit
12345678901234567890123456 transmit-key !This step is
optional----!--- This value seeds the initial key for
use with !--- broadcast [255.255.255.255] traffic. If
more than one VLAN is !--- used, then keys must be set
for each VLAN. encryption vlan 1 mode wep mandatory !---
This defines the policy for the use of Wired Equivalent
Privacy (WEP). !--- If more than one VLAN is used, !---
the policy must be set to mandatory for each VLAN.
broadcast-key vlan 1 change 300 !--- You can also enable
Broadcast Key Rotation for each vlan and Specify the
time after which Brodacst key is changed. If it is
disabled Broadcast Key is still used but not changed.
ssid cisco vlan 1 !--- Create a SSID Assign a vlan to
this SSID authentication open eap eap_methods
authentication network-eap eap_methods !--- Expect that
users who attach to SSID "cisco" !--- request
authentication with the type 128 Open EAP and Network
EAP authentication !--- bit set in the headers of those
requests, and group those users into !--- a group called
"eap_methods." ! speed basic-1.0 basic-2.0 basic-5.5
basic-11.0 rts threshold 2312 channel 2437 station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled . . .
interface FastEthernet0 no ip address no ip route-cache
duplex auto speed auto bridge-group 1 no bridge-group 1
source-learning bridge-group 1 spanning-disabled !
interface BVI1 ip address 10.77.244.194 255.255.255.0 !-
-- The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local !--- Engages the Local RADIUS Server
feature. nas 10.77.244.194 key shared_secret !---
Identifies itself as a RADIUS server, reiterates !---
"localness" and defines the key between the server
(itself) and the access point. ! group testuser !---
Groups are optional. ! user user1 nthash password1 group
testuser !--- Individual user user user2 nthash
password2 group testuser !--- Individual user !--- These
individual users comprise the Local Database ! radius-
server host 10.77.244.194 auth-port 1812 acct-port 1813
key shared_secret !--- Defines where the RADIUS server
is and the key between !--- the access point (itself)
and the server. radius-server retransmit 3 radius-server
attribute 32 include-in-access-req format %h radius-
server authorization permit missing Service-Type radius-
server vsa send accounting bridge 1 route ip ! ! line
con 0 line vty 5 15 ! end
```

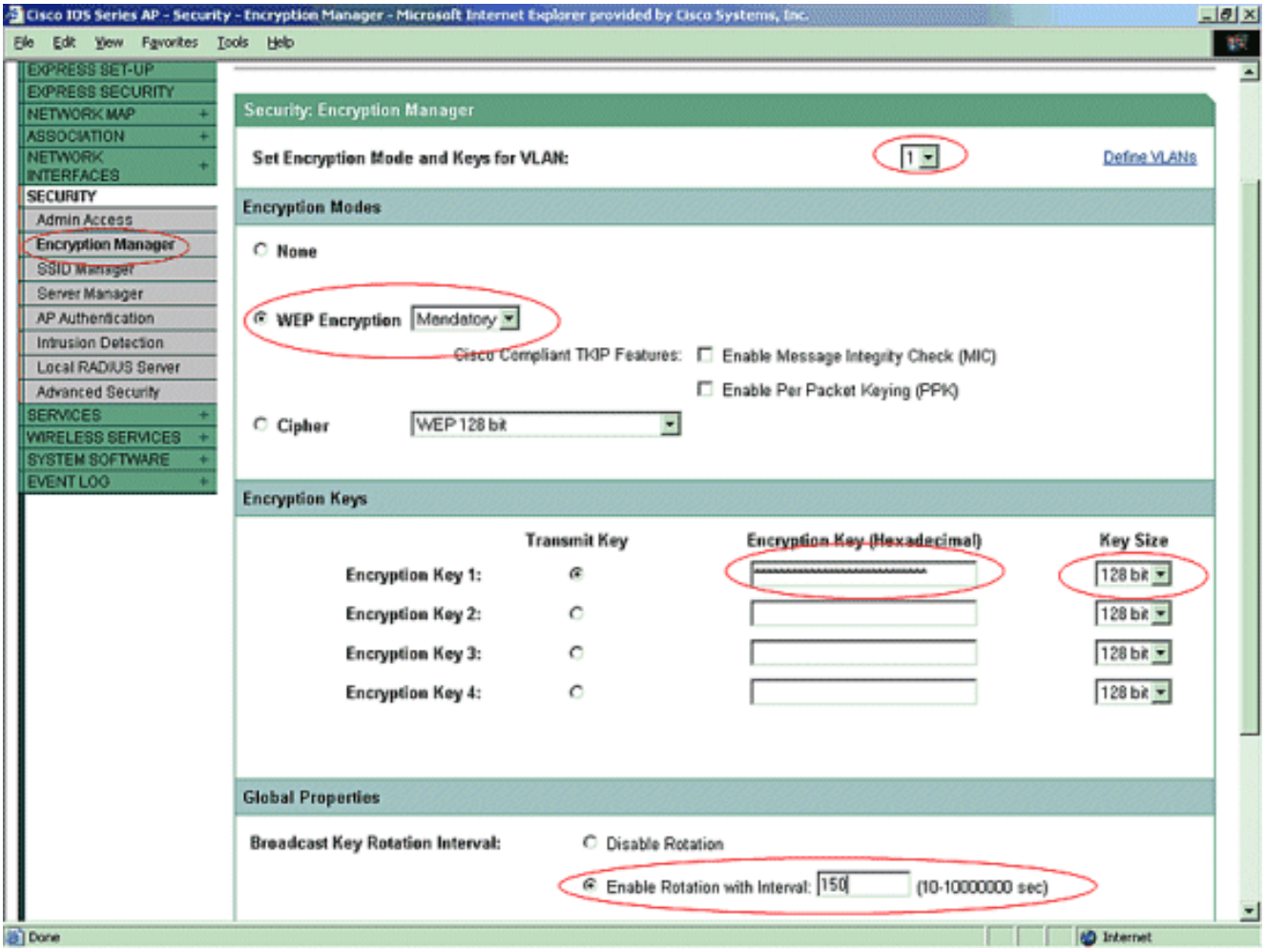
Configuração de GUI

Termine estas etapas a fim configurar a característica local do servidor Radius com o GUI:

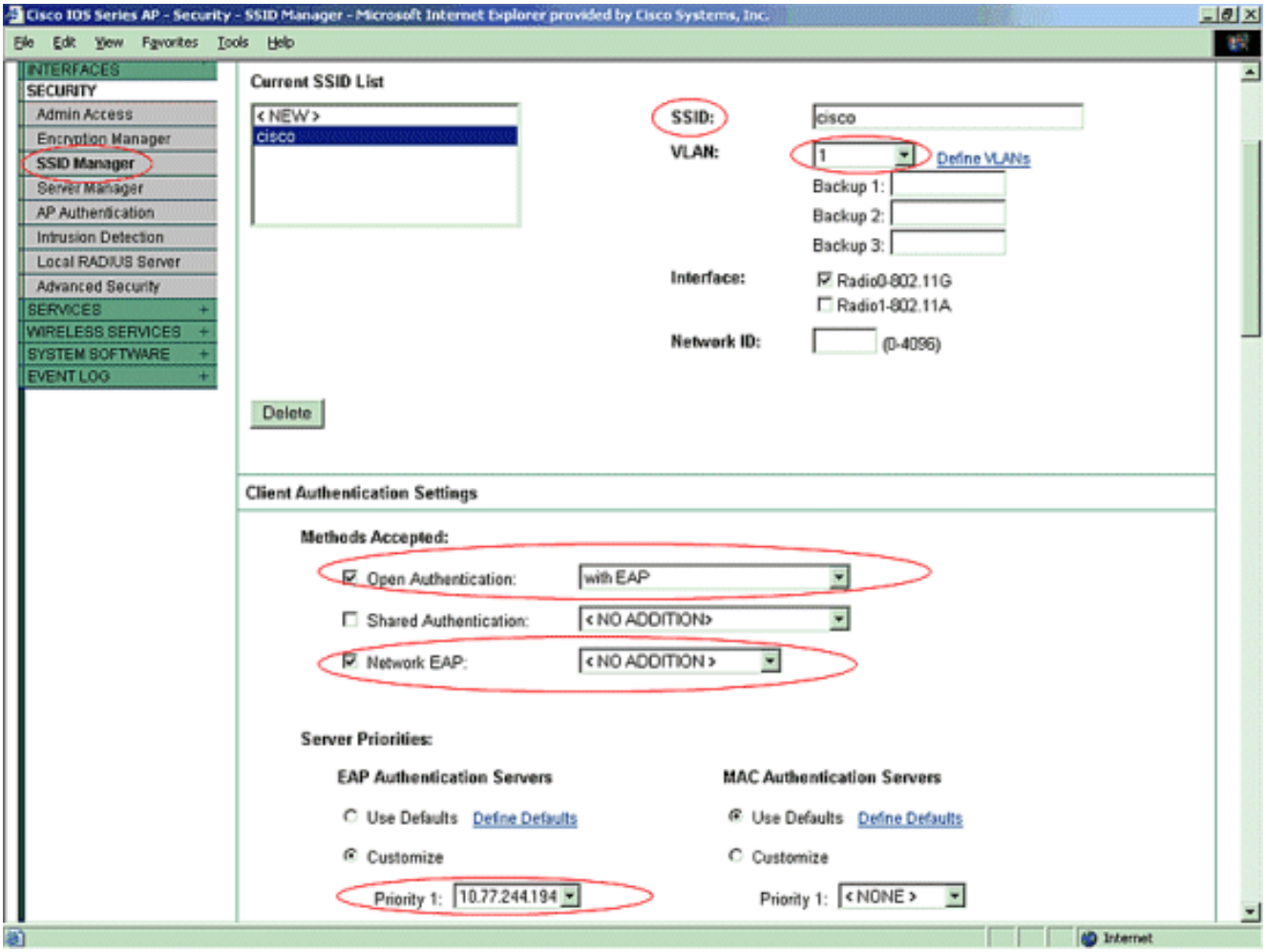
1. Do menu no lado esquerdo, escolha a aba do gerenciador do servidor sob o menu Segurança.Configurar o server e mencione o endereço IP de Um ou Mais Servidores Cisco ICM NT deste Access point, que é 10.77.244.194 neste exemplo.Mencione os números de porta 1812 e 1813 em que o servidor Radius local escuta.Especifique o segredo compartilhado a ser usado com o servidor Radius local segundo as indicações da figura.



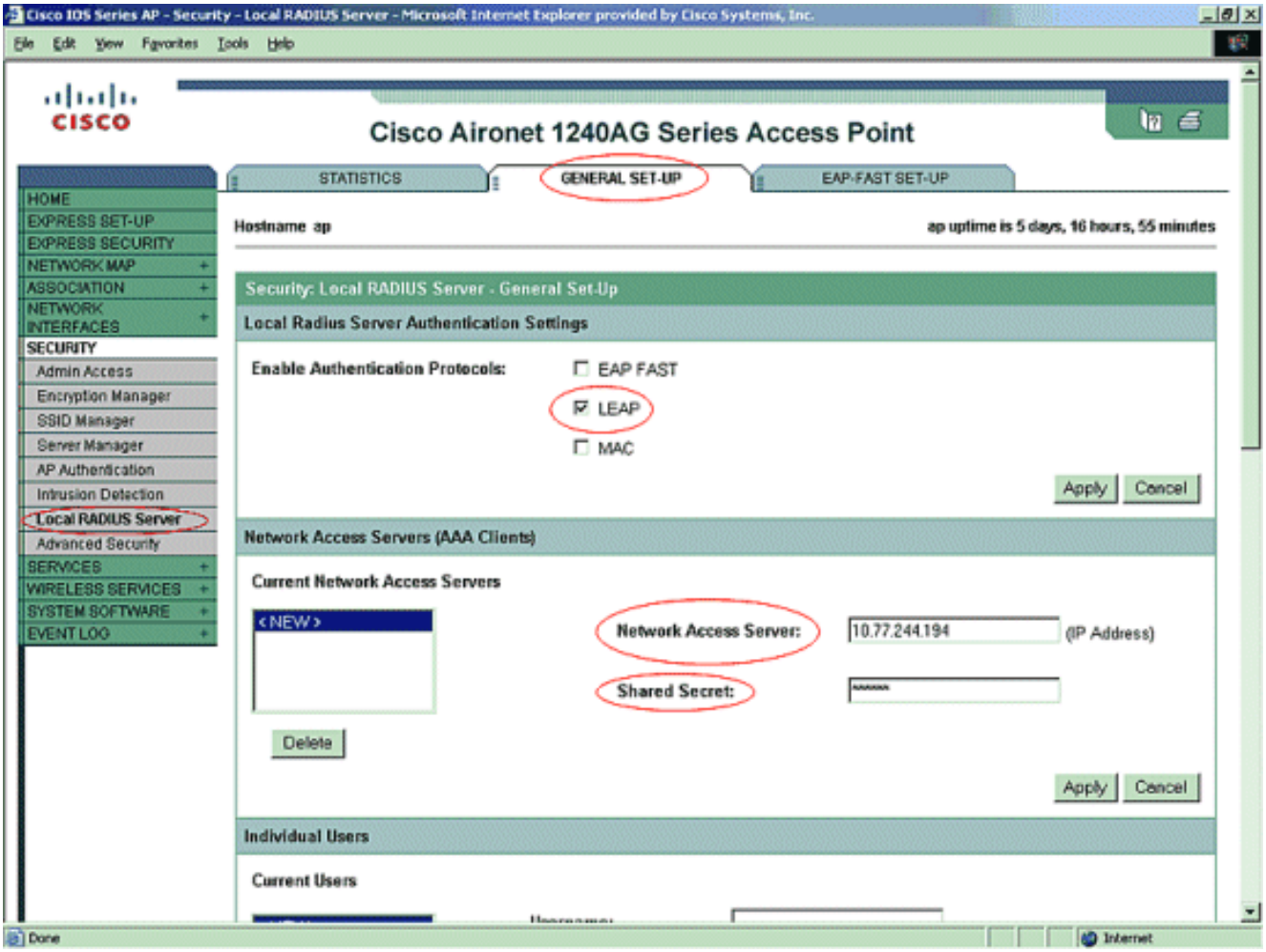
2. Do menu no lado esquerdo, clique a aba do gerenciador de criptografia sob o menu Segurança.Especifique o VLAN a ser aplicado.Especifique a criptografia WEP a ser utilizada.Especifique que seu uso é obrigatório.Inicialize toda a chave de WEP com um caractere hexadecimal 26-digit. Esta chave é usada para cifrar a transmissão e os pacotes de transmissão múltipla. Este passo é opcional.Ajuste o tamanho chave aos bit 128. Você pode igualmente escolher 40 bit. Neste caso, o tamanho da chave de WEP na etapa precedente deve ser um caractere hexadecimal 10-digit. Este passo é opcional.Você pode igualmente permitir a rotação chave da transmissão e especificar o tempo depois do qual a chave da transmissão é mudada. Se é desabilitada, a chave da transmissão ainda está usada mas não mudada. Este passo é opcional.**Nota:** Estas etapas são repetidas para cada VLAN que usa a autenticação de leapClique em
Apply.



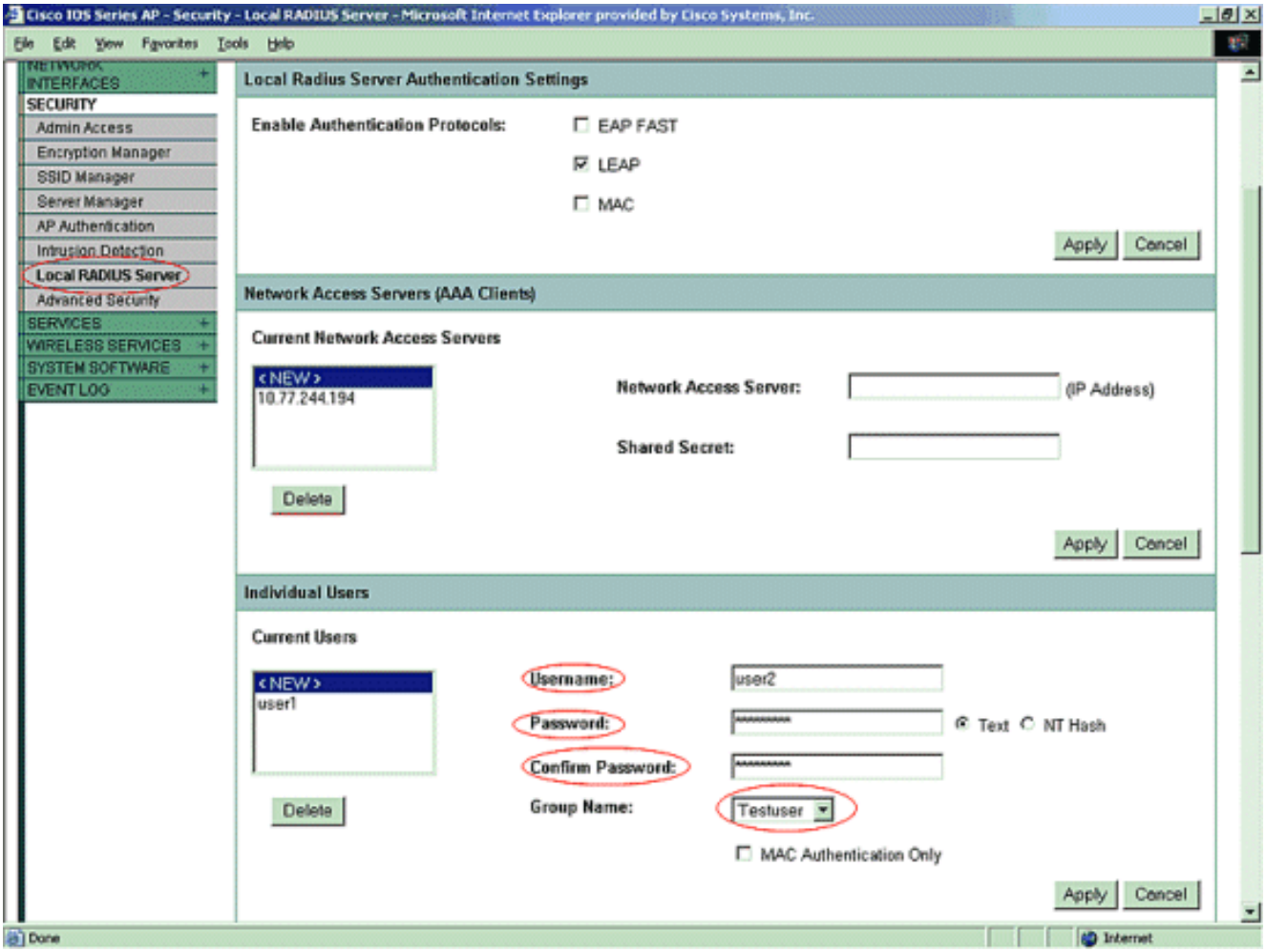
3. Sob o menu Segurança, da aba do gerenciador de SSID, execute estas ações:**Nota:** Você pode adicionar recursos adicionais e gerenciamento chave mais tarde, uma vez que você confirma que a configuração baixa trabalha corretamente.Defina um SSID novo e associe-o com um VLAN. Neste exemplo, o SSID é associado com o VLAN1.Verifique a **autenticação aberta (com EAP)**.Verifique a **rede EAP (nenhuma adição)**.**Dos server das prioridades > da autenticação de EAP do server**, escolha **personalizam**; escolha o endereço IP de Um ou Mais Servidores Cisco ICM NT deste forPriority **1. do** Access point.Clique em Apply.



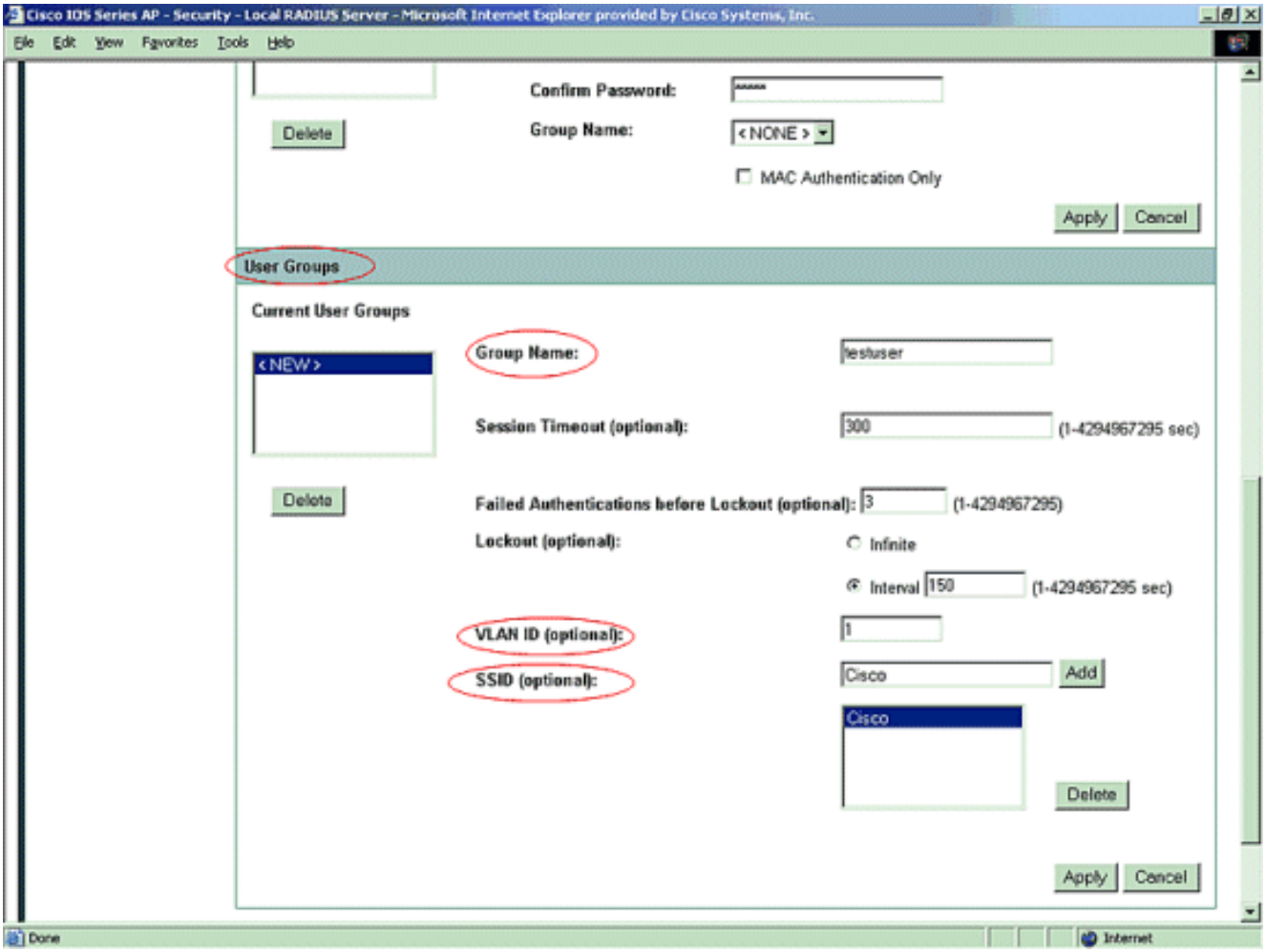
4. Sob a Segurança, clique o servidor Radius local da aba geral da instalaçãoSob ajustes locais da autenticação de servidor Radius, **PULO da** verificação para certificar-se de que os pedidos da autenticação de leap estão aceitados.Defina o endereço IP e o segredo compartilhado do servidor RADIUS. Para o servidor Radius local, este é o endereço IP de Um ou Mais Servidores Cisco ICM NT deste AP (10.77.244.194).Clique em Apply.



5. Enrole para baixo do servidor Radius local sob a aba geral da instalação e defina os usuários individuais com seus nomes de usuário e senha. Opcionalmente, os usuários podem ser associados aos grupos, que é definido na próxima etapa. Isto certifica-se desse somente log de usuários determinados em um SSID.**Nota:** O base de dados RADIUS local é compreendido destes nomes de usuário e senha individuais.



6. Enrole mais para baixo na mesma página, outra vez do servidor Radius local sob a aba geral do sub da instalação grupos de usuário; defina grupos de usuário e associe-os a um VLAN ou a um
SSID.



Nota: Os grupos são opcionais. Os atributos do grupo não passam para o Active Directory e são apenas localmente relevantes. Você pode adicionar grupos mais tarde, uma vez que você confirma que a configuração baixa trabalha corretamente.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

- show radius local-server statistics—Esse comando exibe estatísticas coletadas por um autenticador local.

```
Successes             : 27          Unknown usernames      : 0
Client blocks         : 0           Invalid passwords      : 0
Unknown NAS           : 0           Invalid packet from NAS: 0

NAS : 10.77.244.194
Successes             : 27          Unknown usernames      : 0
Client blocks         : 0           Invalid passwords      : 0
Corrupted packet      : 0           Unknown RADIUS message : 0
No username attribute : 0           Missing auth attribute : 0
Shared key mismatch   : 0           Invalid state attribute: 0
Unknown EAP message   : 0           Unknown EAP auth type  : 0
Auto provision success : 0          Auto provision failure : 0
PAC refresh           : 0           Invalid PAC received   : 0

Username                  Successes  Failures  Blocks
user1                            27         0       0
```

- show radius server-group all—Esse comando exibe uma lista de todos os grupos de servidores RADIUS configurados no ponto de acesso.

Troubleshooting

Procedimento de Troubleshooting

Esta seção fornece a informação de Troubleshooting relevante a esta configuração.

1. A fim eliminar a possibilidade de edições RF que impedem a autenticação bem sucedida, ajuste o método no SSID **para abrir** para desabilitar temporariamente a autenticação.Do GUI — Na página do gerenciador de SSID, desmarcar a **Rede EAP** e verifique **aberto**.Da linha de comando — Não use os comandos authentication open e **nenhum eap_methods da autenticação rede-EAP**.Se o cliente associa com sucesso, o RF não contribui ao problema de associação.
2. Verifique se todas as senhas secretas compartilhadas estão sincronizadas. As linhas `<shared_secret> chave da acct-porta x da autêntico-porta x do host de servidor RADIUS x.x.x.x e <shared_secret> da chave` nas `x.x.x.x devem conter a` mesma senha secundária compartilhada.
3. Remova todos os grupos de usuário e configuração sobre grupos de usuário. Às vezes os conflitos podem ocorrer entre os grupos de usuário definidos pelo Access point, e os grupos de usuário no domínio.

Comandos para Troubleshooting

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **debugar o autenticador todo aaa do dot11** — Isto debuga mostras as várias negociações que um cliente vai completamente enquanto o cliente associa e autentica com o 802.1x ou o processo EAP da perspectiva do autenticador (Access point). Isto debuga foi introduzido no Cisco IOS Software Release 12.2(15)JA. Esse comando torna obsoleto debug dot11 aaa dot1x all nesta versão e em versões posteriores.

```
 *Mar  1 00:26:03.097: dot11_auth_add_client_entry:
   Create new client 0040.96af.3e93 for application 0x1
 *Mar  1 00:26:03.097: dot11_auth_initialize_client:
   0040.96af.3e93 is added to the client list for application 0x1
-----------------------------------------------
   Lines Omitted for simplicity ------------------
*Mar  1 00:26:03.098: dot11_auth_dot1x_start:
   in the dot11_auth_dot1x_start


*Mar  1 00:26:03.132: dot11_auth_dot1x_run_rfsm:
   Executing Action(CLIENT_WAIT,EAP_START) for 0040.96af.3e93
*Mar  1 00:26:03.132: dot11_auth_dot1x_send_id_req_to_client:
   Sending identity request to 0040.96af.3e93(client) *Mar 1 00:26:03.133: *Mar 1
00:26:03.099: dot11_auth_dot1x_send_id_req_to_client: Client 0040.96af.3e93 timer started
for 30 seconds *Mar 1 00:26:03.132: dot11_auth_parse_client_pak: Received EAPOL packet from
0040.96af.3e93 ----------------------------------------------- Lines Omitted---------------
------------------- *Mar 1 00:26:03.138: EAP code: 0x2 id: 0x1 length: 0x000A type: 0x1
01805BF0: 0100000A 0201000A 01757365 7231 .........user1(User Name of the client) *Mar1
00:26:03.146: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,CLIENT_REPLY) for
0040.96af.3e93 *Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server: Sending client
0040.96af.3e93 data to server *Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds ------------------------------------------------
Lines Omitted---------------------------------- *Mar1 00:26:03.150:
```

dot11_auth_dot1x_parse_aaa_resp: **Received server response:GET_CHALLENGE_RESPONSE** *Mar1 00:26:03.150: dot11_auth_dot1x_parse_aaa_resp: found session timeout 10 sec *Mar 1 00:26:03.150: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,SERVER_REPLY) for 0040.96af.3e93 *Mar 1 00:26:03.150: dot11_auth_dot1x_send_response_to_client: **Forwarding server message to client 0040.96af.3e93** ---------- Lines Omitted---------- *Mar 1 00:26:03.151: dot11_auth_send_msg: **Sending EAPOL to requestor** *Mar 1 00:26:03.151: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 10 seconds *Mar 1 00:26:03.166: dot11_auth_parse_client_pak: **Received EAPOL packet*(User Credentials)* from 0040.96af.3e93** *Mar 1 00:26:03.166: EAP code: 0x2 id: 0x11 length: 0x0025 type: 0x11 01805F90: 01000025 02110025...%...%01805FA0: 11010018 7B75E719 C5F3575E EFF64B27 **....{ug.EsW^ovK'** Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96af.3e93 *Mar 1 00:26:03.186: dot11_auth_dot1x_send_response_to_server: **Sending client 0040.96af.3e93 data *(User Credentials)* to server** *Mar 1 00:26:03.186: dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds ---------- ---------- Lines Omitted---------- *Mar 1 00:26:03.196: dot11_auth_dot1x_parse_aaa_resp: **Received server response: PASS** *Mar 1 00:26:03.197: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,SERVER_PASS) for 0040.96af.3e93 *Mar 1 00:26:03.197: dot11_auth_dot1x_send_response_to_client: **Forwarding server message*(Pass Message)* to client** ---------- Lines Omitted---------- *Mar 1 00:26:03.198: dot11_auth_send_msg: Sending EAPOL to requestor *Mar 1 00:26:03.199: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 30 second *Mar 1 00:26:03.199: dot11_auth_send_msg: **client authenticated 0040.96af.3e93,** node_type 64 for application 0x1 *Mar 1 00:26:03.199: dot11_auth_delete_client_entry: 0040.96af.3e93 is deleted for application 0x1 *Mar 1 00:26:03.200: %DOT11-6-ASSOC: **Interface Dot11Radio0, Station *Station Name* 0040.96af.3e93 Associated KEY_MGMT[NONE]**

- debugar a autenticação RADIUS — Isto debuga mostras as negociações de RADIUS entre o server e cliente, ambo, neste caso, é o Access point.
- debugar o cliente do Servidor local do raio — Isto debuga mostras a autenticação do cliente da perspectiva do servidor Radius.

*Mar 1 00:30:00.742: RADIUS(0000001A):
Send Access-Request*(Client's User Name)* to 10.77.244.194:1812*(Local Radius Server)* id 1645/65, len 128 *Mar 1 00:30:00.742: RADIUS: **User-Name [1] 7 "user1"** *Mar 1 00:30:00.742: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0" *Mar 1 00:30:00.743: RADIUS: **Calling-Station-Id [31] 16 "0040.96af.3e93" *(Client)*** *Mar 1 00:30:00.743: RADIUS: Service-Type [6] 6 Login [1] *Mar 1 00:30:00.743: RADIUS: Message-Authenticato[80] *Mar 1 00:30:00.743: RADIUS: 23 2E F4 42 A4 A3 72 4B 28 44 6E 7A 58 CA 8F 7B [#.?B??rK(DnzX??{] *Mar 1 00:30:00.743: RADIUS: EAP-Message [79] 12 *Mar 1 00:30:00.743: **RADIUS: 02 02 00 0A 01 75 73 65 72 31 [?????user1]** *Mar 1 00:30:00.744: RADIUS: NAS-Port-Type [61] 6 802.11 wireless ---------- ---------- Lines Omitted For Simplicity---------- *Mar 1 00:30:00.744: RADIUS: **NAS-IP-Address [4] 6 10.77.244.194*(Access Point IP)*** *Mar 1 00:30:00.744: RADIUS: Nas-Identifier [32] 4 "ap" ---------- Lines Omitted---------- ---------- *Mar 1 00:30:00.745: RADIUS: **Received from id 1645/65 10.77.244.194:1812, Access-Challenge**, len 117 *Mar 1 00:30:00.746: RADIUS: 75 73 65 72 31 **[user1]** *Mar 1 00:30:00.746: RADIUS: Session-Timeout [27] 6 10 *Mar 1 00:30:00.747: RADIUS: State [24] 50 *Mar 1 00:30:00.747: RADIUS: BF 2A A0 7C 82 65 76 AA 00 00 00 00 00 00 00 00 [?*?|?ev?????????] ---------- Lines Omitted for simplicity ---------- *Mar 1 00:30:00.756: RADIUS/ENCODE(0000001A):Orig. component type = DOT11 *Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: ssid [264] 5 *Mar 1 00:30:00.756: RADIUS: 63 69 73 [cis] *Mar 1 00:30:00.756: RADIUS: AAA Unsupported Attr: interface [157] 3 *Mar 1 00:30:00.756: RADIUS: 32 [2] *Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194 *Mar 1 00:30:00.757: RADIUS/ENCODE(0000001A): acct_session_id: 26 *Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194 *Mar 1 00:30:00.779: RADIUS(0000001A): **Send Access-Request to 10.77.244.194:1812 id 1645/67, len 189** *Mar 1 00:30:00.779: RADIUS: authenticator B0 15 3C C1 BC F6 31 85 - 66 5D 41 F9 2E B4 48 7F *Mar 1 00:30:00.779: RADIUS: User-Name [1] 7 "user1" *Mar 1 00:30:00.780: RADIUS: Framed-MTU [12] 6 1400 *Mar 1 00:30:00.780: RADIUS: Called-Station-Id [30] 16"0019.a956.55c0" *Mar 1 00:30:00.780: RADIUS: Calling-Station-Id [31] 16"0040.96af.3e93" *Mar 1 00:30:00.758: RADIUS: 92 D4 24 49 04 C2 D2 0A C3 CE E9 00 6B F1 B2 AF [??$I????????k???] *Mar 1 00:30:00.759: RADIUS: EAP-Message [79] 39 *Mar 1 00:30:00.759: RADIUS: 02 17 00 25 11 01 00 18 05 98 8B BE 09 E9 45 E2 **[??????????????E?**] *Mar 1 00:30:00.759: RADIUS: 73 5D 33 1D F0 2F DB 09 50 AF 38 9F F9 3B BD D4 **[s]3??/??P?8??;??]** *Mar 1 00:30:00.759: RADIUS: 75 73 65 72 31

```
[user1] ---------------------------------------- Lines Omitted-------------------------
*Mar 1 00:30:00.781: RADIUS: State [24] 50 RADIUS: NAS-IP-Address [4] 6 10.77.244.194 *Mar 1
00:30:00.783: RADIUS: Nas-Identifier [32] 4 "ap" *Mar 1 00:30:00.822: RADIUS: Received from
id 1645/67 10.77.244.194:1812, Access-Accept, len 214 *Mar 1 00:30:00.822: RADIUS:
authenticator 10 0C B6 EE 7A 96 3A 46 - 36 49 FC D3 7A F4 42 2A ---------------------------
----------- Lines Omitted---------------------------- *Mar 1 00:30:00.823: RADIUS: 75 73 65
72 31 [user1] *Mar 1 00:30:00.823: RADIUS: Vendor, Cisco [26] 59 *Mar 1 00:30:00.823:
RADIUS: Cisco AVpair [1] 53 "leap:session-key=?+*ve=];q,oi[d6|-z." *Mar 1 00:30:00.823:
RADIUS: User-Name [1] 28 "user1 *Mar 1 00:30:00.824: RADIUS: Message-Authenticato[80] 18
*Mar 1 00:30:00.824: RADIUS: 06 2D BA 93 10 C0 91 F8 B4 B8 A4 00 82 0E 11 36 [?-
?????????????6] *Mar 1 00:30:00.826: RADIUS/DECODE: EAP-Message fragments, 37, total 37
bytes *Mar 1 00:30:00.826: found leap session key *Mar 1 00:30:00.830: %DOT11-6-ASSOC:
Interface Dot11Radio0, Station Station Name Associated KEY_MGMT[NONE]
```

- **debugar pacotes do Servidor local do raio** — Isto debuga mostras todos os processos feitos e da perspectiva do servidor Radius.

Informações Relacionadas

- Configurando um ponto de acesso como um autenticador local
- Configurando tipos de autenticação
- Configuração de servidores RADIUS e TACACS+
- Suporte Técnico e Documentação - Cisco Systems