

Compreenda o registro do gerente do acesso de rede de AnyConnect

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Permita o registro NAM](#)

[Configurar a captura de pacote de informação NAM](#)

[Registre a coleção](#)

[Lendo logs NAM](#)

[Registre o sumário de uma conexão de rede sem autenticação permitida 802.1x](#)

[Registre o sumário de uma conexão de rede usando o 802.1x e o PEAP sobre a rede ligada com fio](#)

Introdução

Este documento descreve como permitir o gerente do acesso de rede de AnyConnect (NAM) que registra assim como recolher e interpretar os logs. Os exemplos incluídos no documento descrevem as encenações diferentes da autenticação e os logs que refletem as etapas tomadas pelo gerente do acesso de rede para autenticar o cliente.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

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.

Permita o registro NAM

Se uma edição é identificada que possa ser relacionada ao módulo de NAM, a primeira etapa é permitir recursos de registro prolongados. Isto deve ser feito no valor-limite do cliente quando o módulo de NAM for executado.

Etapa 1. Abra o indicador de AnyConnect e certifique-se que está no foco.

Etapa 2. Pressione esta combinação chave, **SHIFT esquerda + saiu Alt + L**. Não há nenhuma resposta.

Etapa 3. Clicar com o botão direito no ícone de AnyConnect na bandeja do sistema Windows. Um menu estala acima.

Etapa 4. Selecione **registro prolongado** assim que tem uma marca de verificação indicada. O NAM registra agora detalhado debuga mensagens.

Configurar a captura de pacote de informação NAM

Quando o registro prolongado é permitido, o NAM igualmente mantém ir do buffer da captura de pacote de informação. O buffer à revelia é limitado aproximadamente a 1MB. Se a captura de pacote de informação é precisada, pode ser benéfico aumentar o tamanho de buffer assim que captura mais atividades. Para estender o buffer, um arquivo do ajuste XML deve manualmente ser alterado.

Etapa 1. No PC Windows, consulte a:

**Cliente da mobilidade de C:\ProgramData\Cisco\Cisco AnyConnect \ gerente \ sistema seguros do acesso de rede **

Etapa 2. Arquivo em aberto **internalConfiguration.xml**.

Etapa 3. Encontre a etiqueta `<packetCaptureFileSize>1</packetCaptureFileSize>` XML e ajuste o valor ao 10 para um tamanho de buffer 10MB, e assim por diante.

Etapa 4. Recarregue o PC cliente para que a mudança tome o efeito.

Registre a coleção

A coleção do log NAM é feita através do diagnóstico e da ferramenta de relatório (DARDO), que é um módulo da série de AnyConnect. No instalador, selecione um módulo e use a instalação completa ISO de AnyConnect para instalar. O instalador da relação dos serviços de Cisco media (MSI) pode igualmente ser encontrado dentro do ISO.

Depois que você permite registro prolongado e executa um teste, executa simplesmente o DARDO e atravessa o diálogo, o pacote do log está ficado situado à revelia na área de trabalho do Windows.

Além do que o pacote do DARDO, o log de mensagens NAM é igualmente útil encontrar os dados relevantes no log NAM. A fim encontrar o log de mensagens NAM, navegue à **história da janela**

de configuração de AnyConnect > do gerente > da mensagem do acesso de rede. O log de mensagens contém o timestamp de cada evento da conexão de rede, que pode ser usado para encontrar os logs relevantes ao evento.

Lendo logs NAM

Os logs NAM, especialmente depois que você permite registro prolongado, contêm uma grande quantidade de dados, mais de que seja irrelevante e possa ser ignorado. Esta seção alista para fora as linhas debugar para demonstrar cada etapa NAM toma para estabelecer uma conexão de rede. Quando você trabalha através de um log, estas frase-chaves podem ser úteis encontrar parte do log relevante à edição.

Registre o sumário de uma conexão de rede sem autenticação permitida 802.1x

```
2016 17:20:37.974 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123: AccessStateMachine
current state = ACCESS_STOPPED, received userEvent = START
```

Explicação: Isto indica que o usuário selecionou uma rede do módulo de NAM, e o NAM recebeu um **userEvent** do **COMEÇO**.

```
538: TESTPC: May 16 2016 17:20:37.974 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123:
AccessStateMachine new state = ACCESS_STARTED
```

```
539: TESTPC: May 16 2016 17:20:37.974 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123:
NetworkStateMachine current state USER_T_DISCONNECTED, received access event ACCESS_STARTED
```

Explicação: Alcance a máquina de estado e a máquina de estado da rede foi ligada.

```
545: TESTPC: May 16 2016 17:20:37.974 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Ipv4 {EFDAF0F0-CF25-
4D88-B125-E748CD539DFF}: received Cancel event [state: COMPLETE]
```

Explicação: O exemplo do IPv4 obtido **cancelou** a fim restaurar os estados.

```
547: TESTPC: May 16 2016 17:20:37.974 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: starting
makeMatches...
```

```
549: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-6-INFO_MSG: %[tid=1412]: matching adapter
{484E4FEF-392C-436F-97F0-CD7206CD7D48} and network test123 ...
```

Explicação: O adaptador com ID **484E4FEF-392C-436F-97F0-CD7206CD7D48** foi selecionado para conectar à rede **test123**, que é o nome da conexão de rede configurada no NAM.

```
551: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123:
AccessStateMachine new state = ACCESS_ATTACHED
```

```
557: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123:
AccessStateMachine current state = ACCESS_ATTACHED, received userEvent = CONNECT
```

Explicação: O NAM contratou com sucesso o adaptador para esta rede. Agora o NAM tenta associar (para conectar) a esta rede (que acontece ser wireless):

```
561: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM
current: state(STATE_DISCONNECTED_LINK_DOWN), event(EVENT_CONNECT)
```

```
562: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM
state change: STATE_DISCONNECTED_LINK_DOWN -> STATE_ASSOCIATING
```

```
567: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Starting wifi
connection, trying ssid test123 ...
```

```
568: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Connection Association Started(openNoEncryption)
```

Explicação: o **openNoEncryption** indica que a rede está configurada como aberta. No controlador do Wireless LAN usa o desvio da autenticação de MAC (MAB) para autenticar.

```
234: TESTPC: May 16 2016 17:20:38.020 +0600: %NAMSSO-7-DEBUG_MSG: %[tid=1912]: waiting for cs...
```

Explicação: o **Cs** pode ser visto muito em logs NAM. Estes são logs irrelevantes e devem ser ignorados.

```
575: TESTPC: May 16 2016 17:20:38.020 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123: NetworkStateMachine new state USER_T_DISCONNECTED 236: TESTPC: May 16 2016 17:20:38.020 +0600: %NAMSSO-7-DEBUG_MSG: %[tid=1912]: Tx CP Msg: <?xml version="1.0" encoding="UTF-8"?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ssc="http://www.cisco.com/ssc" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body> <networkStateEvent> <sequenceNumber>16</sequenceNumber> <groupName>Local networks</groupName> <networkName>test123</networkName> <networkState>Associating</networkState> <adapterName>Intel(R) Centrino(R) Ultimate-N 6300 AGN</adapterName> <serverVerifiedName></serverVerifiedName> </networkStateEvent> </SOAP-ENV:Body></SOAP-ENV:Envelope>
```

Explicação: Estas são mensagens do simple object access protocol (SABÃO) usadas para dizer AnyConnect GUI para indicar a mensagem do status de conexão tal como a **associação** neste caso. Todos os Mensagens de Erro indicados no indicador NAM podem ser encontrados em uma das mensagens do SABÃO no log que pode ser usado para encontrar facilmente a edição.

```
582: TESTPC: May 16 2016 17:20:38.020 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: {484E4FEF-392C-436F-97F0-CD7206CD7D48} - Received STATE_AUTHENTICATED
```

```
583: TESTPC: May 16 2016 17:20:38.020 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM current: state(STATE_ASSOCIATING), event(EVENT_AUTH_SUCCESS)
```

Explicação: O NAM recebe um evento **AUTH_SUCCESS**, que se engane porque não há nenhuma autenticação que aconteceu atualmente. Você é obtém este evento simplesmente porque você conecta a uma rede aberta, tão à revelia autenticação é bem sucedido.

```
595: TESTPC: May 16 2016 17:20:38.738 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123: AccessStateMachine current state = ACCESS_ASSOCIATING, received adapterState = associated
```

Explicação: A associação ao Service Set Identifier (SSID) é bem sucedida, cronometra para segurar a autenticação.

```
603: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-6-INFO_MSG: %[tid=1412][mac=1,6,3c:a9:f4:33:ab:50]: Authentication not required.
```

```
604: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM current: state(STATE_ASSOCIATED), event(EVENT_AUTH_SUCCESS)
```

```
605: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM state change: STATE_ASSOCIATED -> STATE_AUTHENTICATED
```

Explicação: Desde que esta é uma rede aberta, à revelia é autenticado. Neste momento, o NAM é conectado à rede e começa agora o processo DHCP:

```
610: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: {484E4FEF-392C-436F-97F0-CD7206CD7D48} creating a new DHCP work
612: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-6-INFO_MSG:
%[tid=1412][mac=1,6,3c:a9:f4:33:ab:50]: {484E4FEF-392C-436F-97F0-CD7206CD7D48}: DHCP: Sending
DHCP request
613: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: queueing DHCP work
642: TESTPC: May 16 2016 17:20:40.830 +0600: %NAM-7-DEBUG_MSG: %[tid=1448]: Ipv4 {484E4FEF-392C-436F-97F0-CD7206CD7D48}: connectivity test[03]: IP:10.201.230.196(255.255.255.224)
GW:10.201.230.193 [Success]
643: TESTPC: May 16 2016 17:20:40.830 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Ipv4 {484E4FEF-392C-436F-97F0-CD7206CD7D48}: received Success event [state: WAIT_FOR_CONNECTIVITY]
645: TESTPC: May 16 2016 17:20:40.845 +0600: %NAM-6-INFO_MSG:
%[tid=1412][mac=1,6,3c:a9:f4:33:ab:50]: {484E4FEF-392C-436F-97F0-CD7206CD7D48}: IP Address
Received: 10.201.230.196
646: TESTPC: May 16 2016 17:20:40.845 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Ipv4 Connectivity
Result: SUCCESS
```

Explicação: O NAM adquire com sucesso um endereço IP de Um ou Mais Servidores Cisco ICM NT.

```
648: TESTPC: May 16 2016 17:20:40.845 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM
current: state(STATE_AUTHENTICATED), event(EVENT_IP_CONNECTIVITY)
649: TESTPC: May 16 2016 17:20:40.845 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM
state change: STATE_AUTHENTICATED -> STATE_CONNECTED
```

Explicação: Uma vez que um endereço IP de Um ou Mais Servidores Cisco ICM NT é recebido o NAM enviará o pedido ARP (protocolo Protocolo de resolução de la dirección (ARP)) ao gateway (GET-**Conectividade**). Uma vez que a reação ARP é recebida o cliente está conectado.

Registre o sumário de uma conexão de rede usando o 802.1x e o PEAP sobre a rede ligada com fio

```
1286: TESTPC: May 16 2016 17:55:17.138 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network WiredPEAP:
AccessStateMachine new state = ACCESS_STARTED
```

Explicação: O NAM começou conectar à rede **WiredPEAP**.

```
1300: TESTPC: May 16 2016 17:55:17.138 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Binding adapter
Intel(R) 82579LM Gigabit Network Connection and user auth for network WiredPEAP
1303: TESTPC: May 16 2016 17:55:17.138 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network WiredPEAP:
AccessStateMachine new state = ACCESS_ATTACHED
```

Explicação: O NAM combinou um adaptador a esta rede.

```
1309: TESTPC: May 16 2016 17:55:17.138 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network WiredPEAP:
AccessStateMachine current state = ACCESS_ATTACHED, received userEvent = CONNECT
1342: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: STATE (4)
S_enterStateAux called with state = CONNECTING (dot1x_sm.c 142)
```

Explicação: Conexão começada NAM a esta rede ligada com fio.

```
1351: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: 8021X (4)
Sent start frame (dot1x_sm.c 117)
```

Explicação: O cliente envia **EAPOL_START**.

```
1388: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: PORT (3)
net: RECV (status: UP, AUTO) (portMsg.c 658)
1389: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: 8021X (4)
recvd EAP IDENTITY frame (dot1x_util.c 264)
1397: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
EAP State: EAP_STATE_IDENTITY (eap_auth_client.c 940)
```

Explicação: O cliente recebe o pedido da identidade do interruptor, ele procura agora umas credenciais para enviar para trás.

```
1406: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1464]: EAP-CB: credential
requested: sync=8, session-id=1, handle=00AE1FFC, type=AC_CRED_SESSION_START
1426: TESTPC: May 16 2016 17:55:17.169 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: EAP: processing
credential request: sync=8, session-id=1, eap-handle=00AE1FFC, eap-level=0, auth-level=0,
protected=0, type=CRED_REQ_SESSION_START
1458: TESTPC: May 16 2016 17:55:17.169 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Trying fast
reauthentication for unprotected identity anonymous
1464: TESTPC: May 16 2016 17:55:17.169 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: EAP: credential
request completed, response sent: sync=9
```

Explicação: À revelia, Anyconnect envia **anônimo** como identidade desprotegida (**identidade exterior**), tão aqui ele tenta **anônimo** e vê se o server é **APROVADO** com ele. O fato de que a identidade é **anônima** ao contrário do **host/anônima** indica que é uma autenticação de usuário, um pouco do que a autenticação da máquina.

```
1492: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: 8021X (4)
recvd EAP TLS frame (dot1x_util.c 293)
```

Explicação: O servidor Radius envia um quadro da Segurança da camada do Protocolo-transporte da autenticação extensível (EAP-TLS) sem nenhum índice. Sua finalidade é negociar o protocolo do EAP-TLS com o cliente.

```
1516: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-6-INFO_MSG: %[tid=1412]: EAP: EAP suggested
by server: eapTls
1517: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-6-INFO_MSG: %[tid=1412]: EAP: EAP requested
by client: eapPeap
1518: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: EAP: EAP methods
sent: sync=10
1519: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: EAP: credential
```

request 10: state transition: PENDING -> RESPONDED

Explicação: O NAM reconhece o pedido do server usar o EAP-TLS mas o cliente é configurado para usar o protocolo extensible authentication protegido (PEAP). Esta é a razão que o NAM envia para trás uma contraoferta para o PEAP.

```
1520: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
Auth[WiredPEAP:user-auth]: Authentication state transition:
AUTH_STATE_UNPROTECTED_IDENTITY_SENT_FOR_FAST_REAUTHENTICATION ->
AUTH_STATE_UNPROTECTED_IDENTITY_ACCEPTED
```

Explicação: O servidor Radius aceita identidade exterior/desprotegida.

```
1551: TESTPC: May 16 2016 17:55:17.200 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: 8021X (4)
recvd EAP PEAP frame (dotlx_util.c 305)
1563: TESTPC: May 16 2016 17:55:17.200 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
EAP-PEAP: SSL handshake start (eap_auth_tls_p.c 409)
```

Explicação: A parcela **protegida de** começos PEAP (para estabelecer um túnel seguro para trocar credenciais internas), depois que o cliente recebe uma confirmação do servidor Radius para continuar o uso do PEAP.

```
1565: TESTPC: May 16 2016 17:55:17.200 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
SSL STATE: SSLv3 write client hello A (eap_auth_tls_p.c 394)
1566: TESTPC: May 16 2016 17:55:17.200 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
SSL STATE: SSLv3 read server hello A (eap_auth_tls_p.c 394)
```

Explicação: O NAM envia um hello do cliente encapsulado no mensagem EAP e espera servidores hello para vir. O server olá! contém o certificado ISE, assim que toma algum tempo para terminar transferir.

```
1622: TESTPC: May 16 2016 17:55:17.216 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: 8021X (4)
recvd EAP PEAP frame (dotlx_util.c 305)
1632: TESTPC: May 16 2016 17:55:17.216 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
SSL STATE: SSLv3 read server hello A (eap_auth_tls_p.c 394)
1633: TESTPC: May 16 2016 17:55:17.216 +0600: %NAM-6-INFO_MSG: %[tid=1468][comp=SAE]: CERT (0)
looking up: "/CN=ISE20-1.kurmai.com" (lookup.c 100)
1634: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-6-INFO_MSG: %[tid=1468][comp=SAE]: CERT (0)
Certificate not found: "/CN=ISE20-1.kurmai.com" (lookup.c 133)
1646: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
SSL_ERROR_WANT_X509_LOOKUP (eap_auth_tls_p.c 193)
```

Explicação: O NAM extraiu o nome do sujeito do server ISE do certificado de servidor. Desde que não tem o certificado de servidor instalado na loja da confiança, você não a encontra lá.

```
1649: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (5)
EAP_EVENT_CRED_REQUEST queued (eapCredProcess.c 496)
```

```
1650: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-7-DEBUG_MSG: %[tid=1464][comp=SAE]: EAP (5)
EAP: CRED_REQUEST (eapMessage.c 355)
1662: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Getting credentials
from logon.
1685: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
Auth[WiredPEAP:user-auth]: ...resumed
```

Explicação: O NAM procura identidade **interna/protegida** a ser enviada ao servidor Radius depois que o túnel é estabelecido. Neste caso, **“use automaticamente meu nome de logon de Windows e a opção da senha”** foi permitida no adaptador prendido, assim que o NAM usa credenciais de logon dos indicadores em vez de pedir o usuário ele.

```
1700: TESTPC: May 16 2016 17:55:17.247 +0600: %NAM-7-DEBUG_MSG: %[tid=1464][comp=SAE]: EAP (0)
SSL STATE: SSLv3 write client key exchange A (eap_auth_tls_p.c 394)
1701: TESTPC: May 16 2016 17:55:17.247 +0600: %NAM-7-DEBUG_MSG: %[tid=1464][comp=SAE]: EAP (0)
SSL STATE: SSLv3 write change cipher spec A (eap_auth_tls_p.c 394)
1750: TESTPC: May 16 2016 17:55:17.278 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
SSL STATE: SSL negotiation finished successfully (eap_auth_tls_p.c 394)
1751: TESTPC: May 16 2016 17:55:17.278 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
EAP-PEAP: SSL handshake done (eap_auth_tls_p.c 425)
1752: TESTPC: May 16 2016 17:55:17.278 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
EAP-PEAP: New session. (eap_auth_tls_p.c 433)
1753: TESTPC: May 16 2016 17:55:17.278 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
EAP-PEAP: session cipher AES256-SHA. (eap_auth_tls_p.c 441)
```

Explicação: O NAM enviou a chave do cliente e as specs. da cifra ao server e recebeu a confirmação. A negociação de SSL é bem sucedida e um túnel é estabelecido.

```
1810: TESTPC: May 16 2016 17:55:17.294 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Protected
identity/(Username) sent.
1814: TESTPC: May 16 2016 17:55:17.294 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
Auth[WiredPEAP:user-auth]: Authentication state transition:
AUTH_STATE_UNPROTECTED_IDENTITY_ACCEPTED -> AUTH_STATE_PROTECTED_IDENTITY_SENT
1883: TESTPC: May 16 2016 17:55:17.310 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
Auth[WiredPEAP:user-auth]: Authentication state transition: AUTH_STATE_PROTECTED_IDENTITY_SENT -
> AUTH_STATE_PROTECTED_IDENTITY_ACCEPTED
```

Explicação: A identidade protegida é enviada ao server, que aceita a identidade. Agora o server pede a senha.

```
1902: TESTPC: May 16 2016 17:55:17.310 +0600: %NAM-7-DEBUG_MSG: %[tid=1464][comp=SAE]: EAP (5)
deferred password request (eapRequest.c 147)
1918: TESTPC: May 16 2016 17:55:17.310 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Protected password
sent.
1921: TESTPC: May 16 2016 17:55:17.325 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
Auth[WiredPEAP:user-auth]: Authentication state transition:
AUTH_STATE_PROTECTED_IDENTITY_ACCEPTED -> AUTH_STATE_CREDENTIAL_SENT
```

Explicação: O NAM recebe o pedido da senha e envia a senha ao server.

```
2076: TESTPC: May 16 2016 17:55:17.856 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
```



```
Auth[WiredPEAP:user-auth]: Authentication state transition: AUTH_STATE_CREDENTIAL_SENT ->
AUTH_STATE_SUCCESS
2077: TESTPC: May 16 2016 17:55:17.856 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: STATE (4)
S_enterStateAux called with state = AUTHENTICATED (dot1x_sm.c 142)
```

Explicação: O server recebe a senha, verifica-a e envia-o o EAP-sucesso. A autenticação é bem sucedida neste momento, e o cliente continua enquanto obtém o endereço IP de Um ou Mais Servidores Cisco ICM NT do DHCP.