



# IPSec and SSL Remote Access VPNs



XXX

October 20, 2009

# Agenda

- IPsec or SSL VPN ?
- IPsec Remote Access VPNs
  - Refresher
  - Configuration Example
  - Troubleshooting and Monitoring
  - Feature Integration
  - Case Studies
- SSL Remote Access VPN
  - Refresher
  - Clientless
  - AnyConnect
  - CSD
  - Dynamic Access Policies
  - Case Studies

# IPSec or SSL VPN?

# IPSec or SSL VPN?

## Differences



Feature	IPSec	SSL VPN
Client Software	Uses Cisco VPN Client software for complete network access.	Uses a standard web browser to access limited corporate network resources. Eliminates need for separate client software
Management	You must install and configure Cisco VPN client.	You do not need to install a VPN client. No configuration is required on the client machine.
Encryption	Uses a variety of encryption and hashing algorithms such as DES, 3DES, AES, SHA & MD5	Uses SSL encryption native to web browsers.
Applications	Encapsulates all IP protocols, including TCP, UDP, and ICMP.	Supports limited TCP-based client/server applications in clientless mode. Encapsulates all IP protocols with AnyConnect client

# IPSec or SSL VPN?

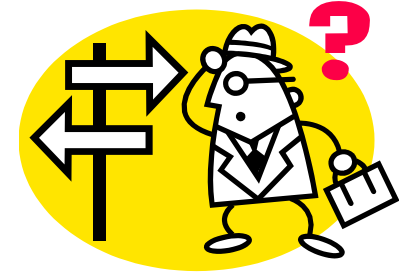
## Differences



Feature	IPSec	SSL VPN
Cost	Free License	Must purchase a license Many different types of licenses: <ul style="list-style-type: none"><li>❖ AnyConnect Essential,</li><li>❖ AnyConnect Premium,</li><li>❖ AnyConnect Mobile,</li><li>❖ SSL Shared Premium</li></ul>
User Environment	Suited for permanent or full-time telecommuters	Suited for all types of users including contractors, temp workers or even fulltime workers
Connectivity	Establishes seamless connection to network.	Supports application connectivity through browser portal.
End-Workstations	Only 32-bit Windows operating systems are supported	32- and 64-bit Windows operating systems are supported

# IPSec or SSL VPN?

## Deployment Considerations

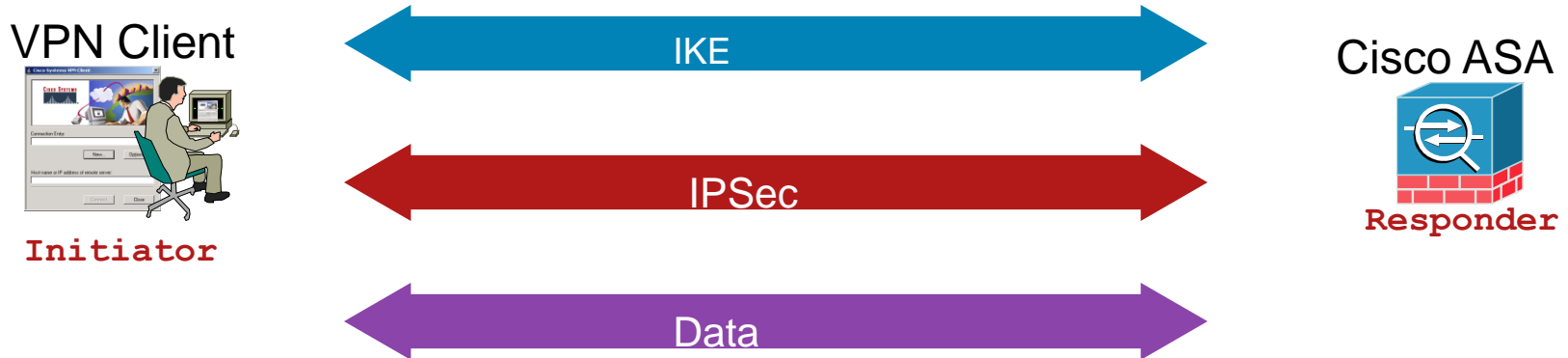


- **Client Workstations**
  - Are the client workstations company owned?
  - Will the users be connecting from Internet Kiosks, guest machines?
  - Will the users be using mobile stations (such as PDA etc)
  
- **User Type**
  - Do you want to deploy the remote access solution for contractors or part-time employees?
  - Do you currently have a software deployment solution?
  
- **Connectivity**
  - Are all applications browser-based?
  - Do you want to provide full network access or application based restrictive access?
  - Are residential broadband providers blocking and/or charging more for IPSec traffic?
  - Are remote access users coming in through NAT routers?

# Cisco IPSec Remote Access VPN

Refresher

# IKE (Two-Phase Protocol)



- Two-phase protocol

**Phase I exchange:** two peers establish a secure, authenticated channel with which to communicate; **main mode** or **aggressive mode** accomplishes a **phase I** exchange; In RA VPNs, we use

1. **Aggressive mode** when **preshared** keys are used
2. **Main mode** when **digital certificates** are used

**Phase II exchange:** security associations are negotiated on behalf of IPsec services; **quick mode** accomplishes a phase II exchange

- Each phase has its SAs: **ISAKMP SA** (phase I) and **IPsec SA** (phase II)

- Phase 1.5 is Cisco specific to handle:

**X-Auth:** to achieve User Authentication

**Mode Configuration:** to assign user specific attributes



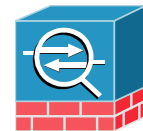
# Aggressive Mode with Pre-Shared Key

VPN Client



Initiator

Cisco ASA



Responder



HDR, SA<sub>proposal</sub>, KE<sub>I</sub>, N<sub>I</sub>, ID<sub>I</sub>, VID<sub>I</sub>

DH key exchange complete,  
share secret **SKEYID** derived

Phase 1 SA parameter  
negotiation complete

HDR, SA<sub>choice</sub>, KE<sub>R</sub>, N<sub>R</sub>, ID<sub>R</sub>, VID<sub>R</sub>, HASH<sub>R</sub>

HDR, HASH<sub>I</sub>

IDs are exchanged, **HASH** is  
verified for authentication

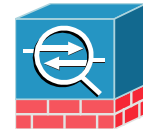
# Phase 1.5 with Pre-Shared Key

VPN Client



**Initiator**

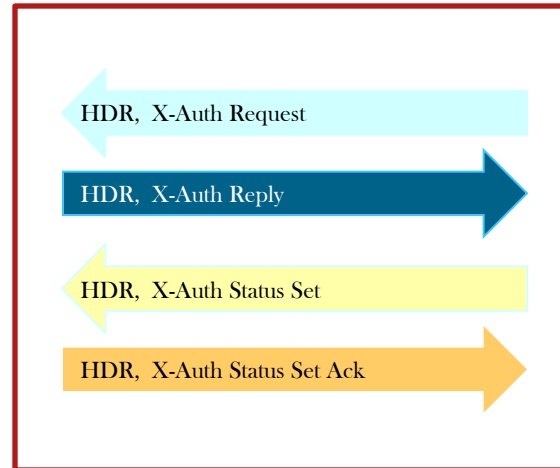
Cisco ASA



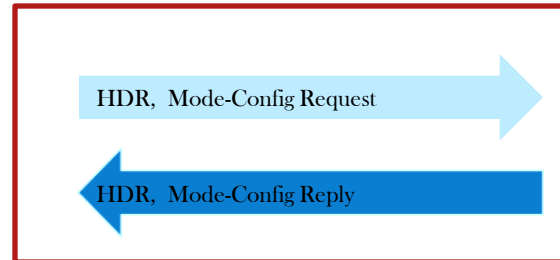
**Responder**



**X-AUTH**



**Mode-Config**



# Phase II Quick Mode Negotiation

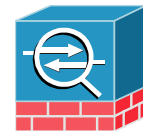
VPN Client



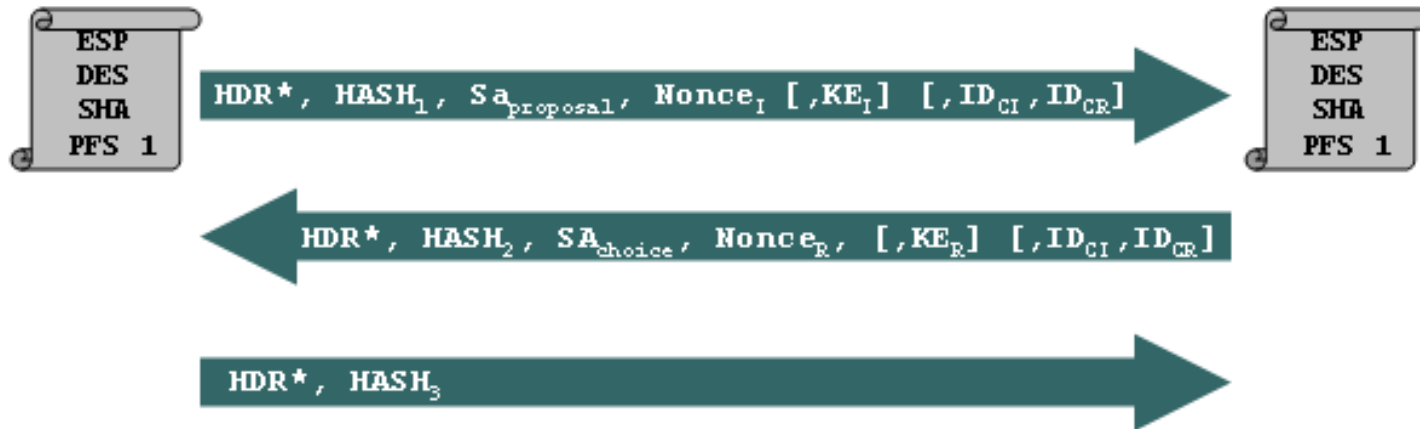
Initiator



Cisco ASA



Responder

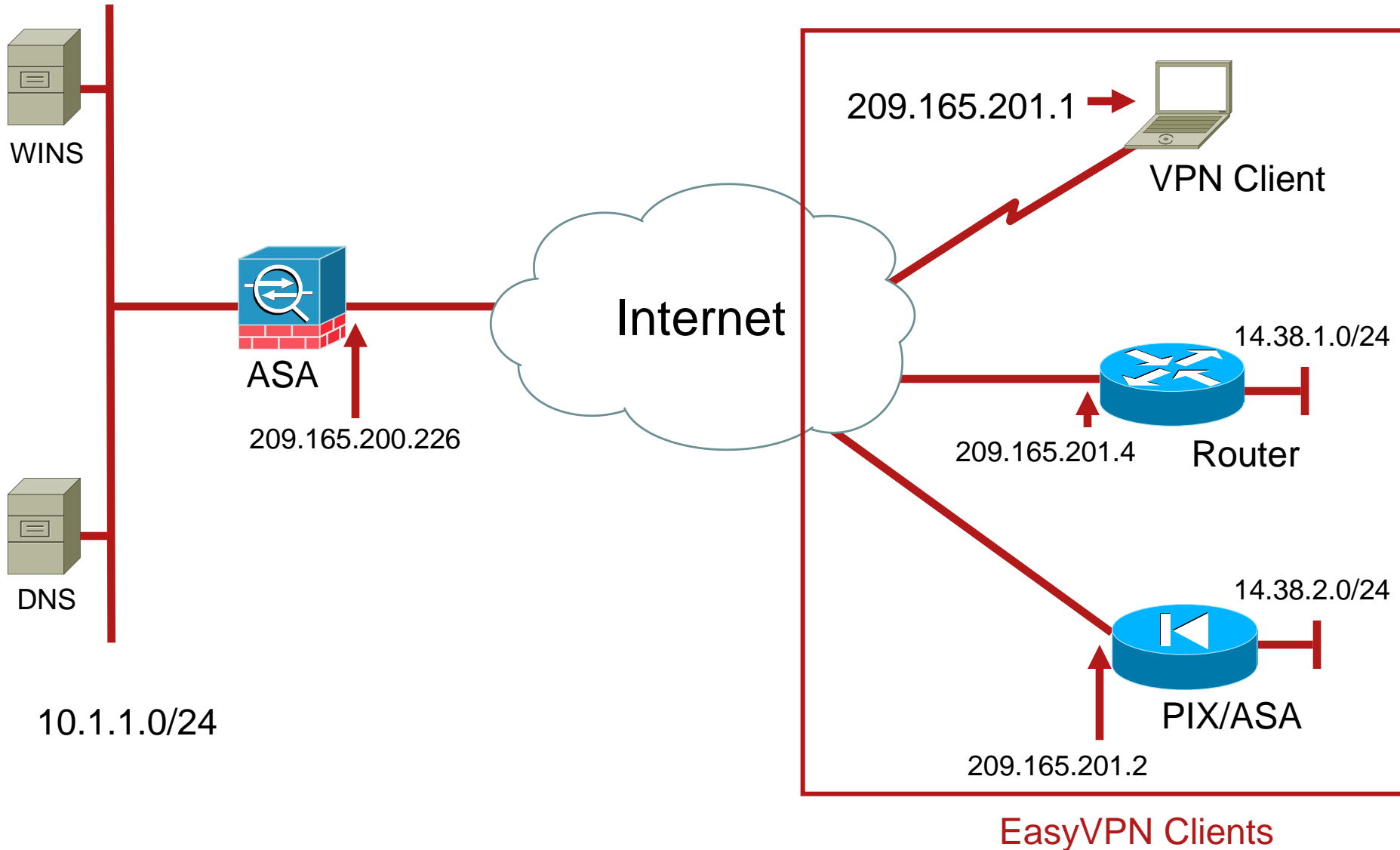


- Protected by Phase 1 SA
- Optional DH exchange for **Perfect Forward Secrecy** (PFS)
- Negotiate IPsec SA parameters, including proxy identities  $[\text{ID}_{\text{CI}}, \text{ID}_{\text{CR}}]$
- Two unidirectional IPsec SA established with unique **SPI** number

# Cisco IPSec Remote Access VPN

## Configuration Example

# Layout



# Cisco VPN Client to Cisco ASA 8.0 +

no nat-control

← To bypass NAT. Enabled by default

isakmp enable outside

isakmp policy 10 authen pre-share

isakmp policy 10 encrypt 3des

isakmp policy 10 hash sha

isakmp policy 10 group 2

isakmp policy 10 lifetime 86400

← ISAKMP Policy Defines Phase 1 Parameters

crypto ipsec transform-set myset esp-3des esp-md5-hmac

crypto dynamic-map dynmap 20 set transform-set myset

crypto map clientmap 65535 ipsec-isakmp dynamic dynmap

crypto map clientmap interface outside

← Dynamic crypto map

← Static crypto map

sysopt connection permit-vpn

← Sysopt Command Bypasses Conduits or ACLs Checking for the Inbound VPN Packets after Decryption

ip local pool ippool 192.168.1.1-192.168.1.254 mask 255.255.255.0

# Cisco VPN Client to Cisco ASA 8.0 + (Cont.)

```
username cisco password cisco123  
username pix password cisco123
```

← User accounts

```
tunnel-group vpnclient type ipsec-ra  
tunnel-group vpnclient general-attributes  
  default-group-policy vpnclient  
  address-pool ippool  
tunnel-group vpnclient ipsec-attributes  
  pre-shared-key cisco123
```

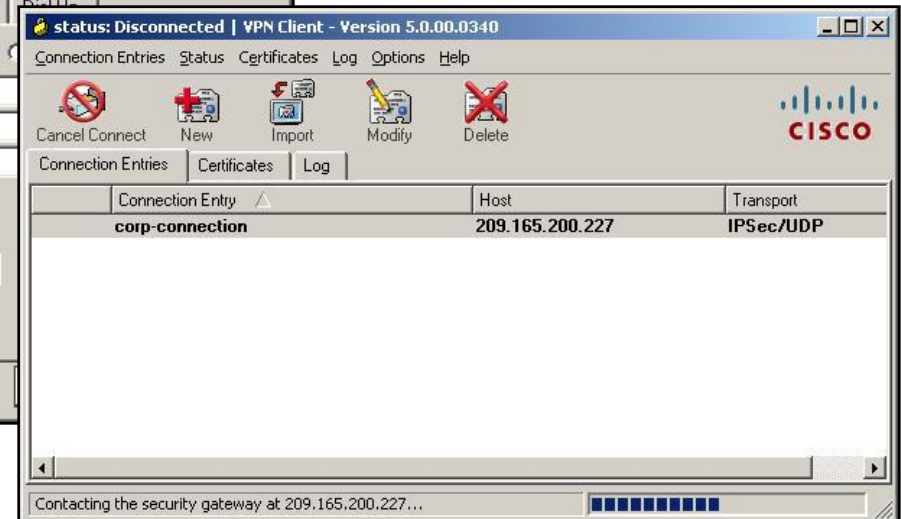
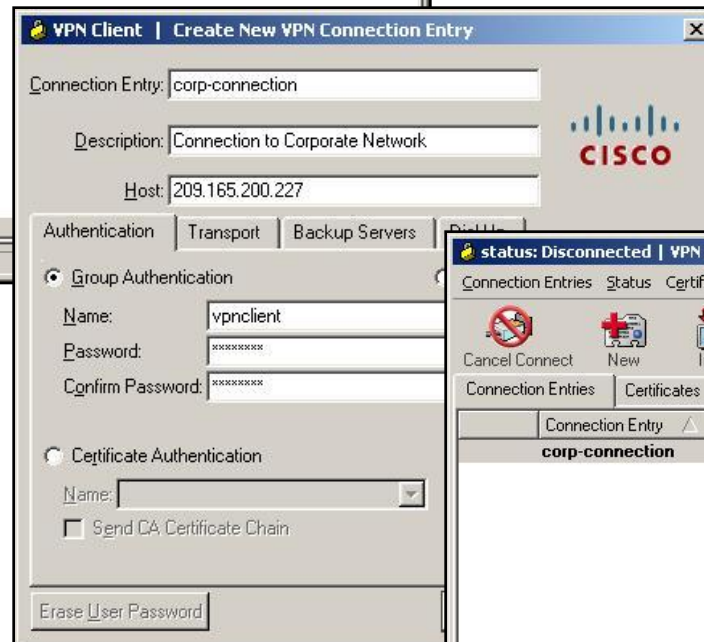
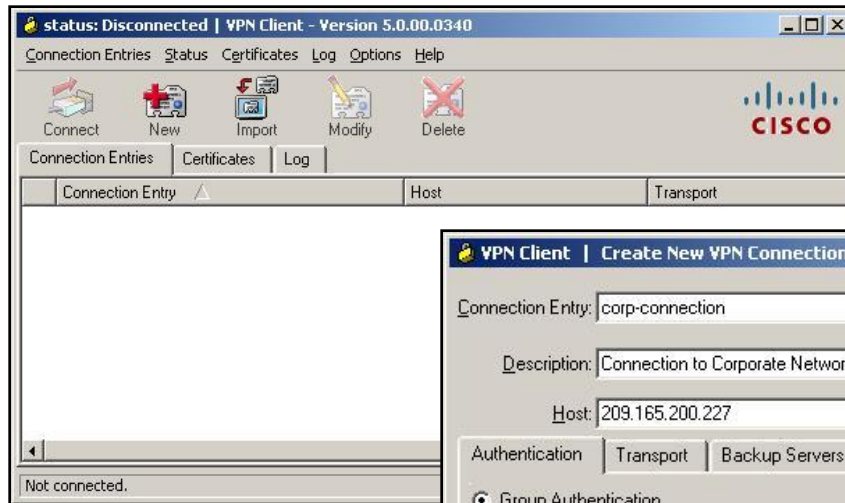
← Tunnel-group specifies the VPN group and the preshared key

```
group-policy vpnclient internal  
group-policy vpnclient attributes  
  dns-server value 10.1.1.10  
  wins-server value 10.1.1.20  
  default-domain value cisco.com  
  nem enable
```

← Group-policy command specifies the mode-config attributes for a VPN group

# Software VPN Client Configuration

To Launch the VPN client, click:  
**Start | Programs | Cisco Systems VPN client | VPN Client**



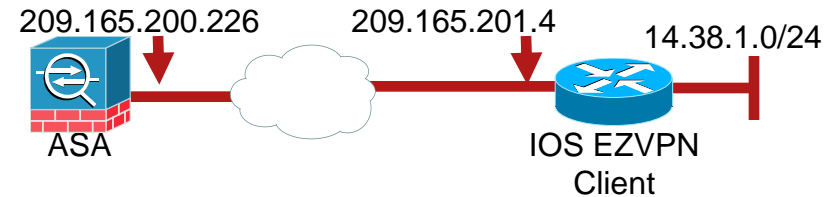


# Cisco IOS EasyVPN Client

```
crypto ipsec client ezvpn ezvpnclient
connect auto
group vpnclient key cisco123
mode network-extension
peer 209.165.200.226
username cisco password cisco123

interface Ethernet0
ip address 14.38.1.1 255.255.255.0
crypto ipsec client ezvpn ezvpnclient inside

interface Ethernet1
ip address 209.165.201.4 255.255.255.224
crypto ipsec client ezvpn ezvpnclient outside
```

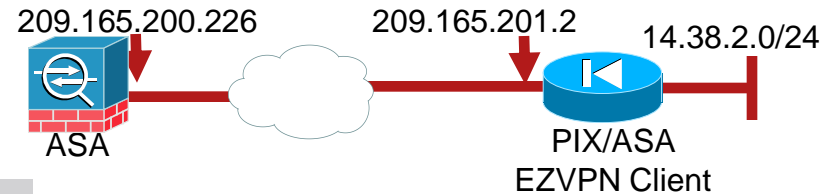


“crypto ipsec client ...” commands define the connection parameters to establish an EasyVPN tunnel

“crypto ipsec client ... inside” command defines the private subnet for the IPsec encryption

“crypto ipsec client ...” command is then applied to an outbound interface

# PIX/ASA EasyVPN



```
hostname vpn-pix501b  
domain-name cisco.com
```

```
vpnclient server 209.165.200.226  
vpnclient mode network-extension-mode  
vpnclient vpngroup vpnclient password *****  
vpnclient username cisco password *****  
vpnclient enable
```

```
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
```

```
ip address outside 209.165.201.2 255.255.255.224  
ip address inside 14.38.2.1 255.255.255.0
```

“vpnclient ...” commands define the connection parameters to establish an EasyVPN tunnel

# Cisco IPSec Remote Access VPN

## Troubleshooting and Monitoring

# Debugs from successful connection

debug crypto isakmp 127  
debug crypto ipsec 127



Initiator

HDR, SA<sub>proposal</sub>, KE<sub>1</sub>, N<sub>1</sub>, ID<sub>1</sub>, VID<sub>1</sub>

HDR, SA<sub>...</sub>, KE<sub>...</sub>, N<sub>...</sub>, ID<sub>...</sub>, VID<sub>...</sub>, HASH<sub>...</sub>

HDR, HASH<sub>1</sub>



Responder

[IKEv1]: IP = 209.165.201.1, **IKE\_DECODE RECEIVED Message** (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 853

[IKEv1 DEBUG]: IP = 209.165.201.1, processing SA payload

[IKEv1 DEBUG]: IP = 209.165.201.1, processing ke payload

[IKEv1 DEBUG]: IP = 209.165.201.1, processing ISA\_KE payload

[IKEv1 DEBUG]: IP = 209.165.201.1, processing nonce payload

[IKEv1 DEBUG]: IP = 209.165.201.1, processing ID payload

[IKEv1 DEBUG]: IP = 209.165.201.1, processing VID payload

[IKEv1 DEBUG]: IP = 209.165.201.1, Received xauth V6 VID

[IKEv1 DEBUG]: IP = 209.165.201.1, processing VID payload

[IKEv1 DEBUG]: IP = 209.165.201.1, Received DPD VID

[IKEv1 DEBUG]: IP = 209.165.201.1, processing VID payload

[IKEv1 DEBUG]: IP = 209.165.201.1, Received Fragmentation VID

[IKEv1 DEBUG]: IP = 209.165.201.1, processing VID payload

[IKEv1 DEBUG]: IP = 209.165.201.1, Received NAT-Traversal ver 02 VID

[IKEv1 DEBUG]: IP = 209.165.201.1, processing VID payload

[IKEv1 DEBUG]: IP = 209.165.201.1, Received Cisco Unity client VID

[IKEv1]: IP = 209.165.201.1, **Connection landed on tunnel\_group vpnclient**

Received 1<sup>st</sup> packet from VPN Client

Decoding received attributes

Group lookup successful

# Debugs from successful connection

debug crypto isakmp 127  
debug crypto ipsec 127



[IKEv1]: IP = 209.165.201.1, **IKE\_DECODE SENDING Message** (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 444

← Sending 2<sup>nd</sup> packet of AM

[IKEv1]: IP = 209.165.201.1, **IKE\_DECODE RECEIVED Message** (msgid=0) with payloads : HDR + HASH (8) + NOTIFY (11) + NAT-D (130) + NAT-D (130) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 168

← Received 3<sup>rd</sup> packet of AM

[IKEv1 DEBUG]: Group = vpnclient, IP = 209.165.201.1, processing hash payload

[IKEv1 DEBUG]: Group = vpnclient, IP = 209.165.201.1, Computing hash for ISAKMP

...

[IKEv1 DEBUG]: Group = vpnclient, IP = 209.165.201.1, Received Cisco Unity client VID

[IKEv1]: Group = vpnclient, IP = 209.165.201.1, Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

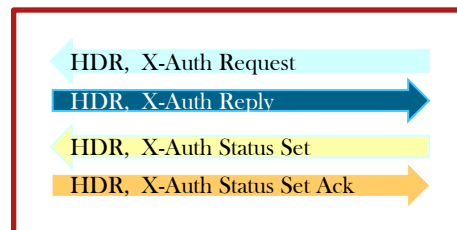
← NAT-T Checking

# Debugs from successful connection

```
debug crypto isakmp 127
debug crypto ipsec 127
```



Initiator



Responder

[IKEv1]: IP = 209.165.201.1, IKE\_DECODE SENDING Message (msgid=bd373d00) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 72



X-AUTH Request & Reply

[IKEv1]: IP = 209.165.201.1, IKE\_DECODE RECEIVED Message (msgid=f71ca4ac) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 85

[IKEv1]: IP = 209.165.201.1, IKE\_DECODE SENDING Message (msgid=2d68ba91) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 64



X-AUTH Status Set & Ack

[IKEv1]: IP = 209.165.201.1, IKE\_DECODE RECEIVED Message (msgid=2d68ba91) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60

# Debugs from successful connection

```
debug crypto isakmp 127
debug crypto ipsec 127
```



Initiator

HDR, Mode-Config Request

HDR, Mode-Config Reply



Responder

[IKEv1]: IP = 209.165.201.1, **IKE\_DECODE RECEIVED Message** (msgid=d826db5d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 195

[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, MODE\_CFG: Received request for IPV4 address!

[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, MODE\_CFG: Received request for IPV4 net mask!

[IKEv1]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, Received unsupported transaction mode attribute: 5

[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, MODE\_CFG: Received request for Banner!

← Mode Config Request

[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, Obtained IP addr (192.168.1.1) prior to initiating Mode Cfg (XAuth enabled)

[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, Sending subnet mask (255.255.255.0) to remote client

[IKEv1]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, Assigned private IP address 192.168.1.1 to remote user

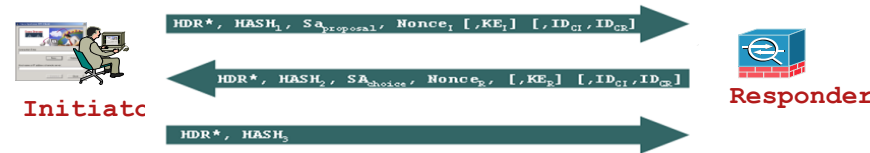
[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, constructing blank hash payload

[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, construct\_cfg\_set: default domain = cisco.com

← Mode Config Reply

# Debugs from successful connection

```
debug crypto isakmp 127
debug crypto ipsec 127
```



```
[IKEv1]: IP = 209.165.201.1, IKE_DECODE RECEIVED Message (msgid=cb6587f3) with payloads : HDR +
HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 1026
```

```
[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, processing hash payload
```

```
[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, processing SA payload
```

```
[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, processing nonce payload
```

```
[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, processing 1st packet of Phase 2
```

```
[IKEv1]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, Received remote Proxy Host data in ID
Payload: Address 192.168.1.1, Protocol 0, Port 0
```

```
[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, processing ID payload
```

```
[IKEv1 DECODE]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, ID_IPV4_ADDR_SUBNET ID
received--0.0.0.0--0.0.0.0
```

```
[IKEv1]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, Received local IP Proxy Subnet data in
ID Payload: Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0
```

```
[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, processing IPsec SA payload
```

```
[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, IPsec SA Proposal # 8,
Transform # 1 acceptable
```

```
[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, Transmitting Proxy Id:
```

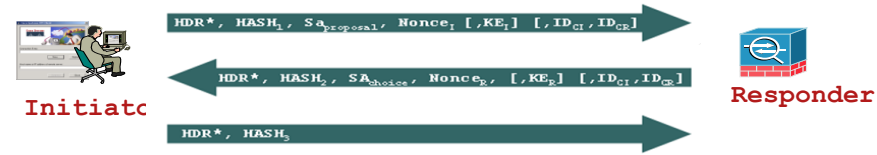
```
Remote host: 192.168.1.1 Protocol 0 Port 0
```

```
Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0
```



# Debugs from successful connection

debug crypto isakmp 127  
debug crypto ipsec 127



```
IPSEC: New embryonic SA created @ 0xADC39168,  
SCB: 0xAE1E6698,  
Direction: inbound  
SPI : 0x47AA58AF  
Tunnel type: ra  
Protocol : esp
```

```
[IKEv1]: IP = 209.165.201.1, IKE_DECODE SENDING Message (msgid=cb6587f3) with payloads : HDR +  
HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 184
```

```
[IKEv1]: IP = 209.165.201.1, IKE_DECODE RECEIVED Message (msgid=cb6587f3) with payloads : HDR  
+ HASH (8) + NONE (0) total length : 52
```

```
[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, processing hash payload
```

```
IPSEC: New embryonic SA created @ 0xAFE0B580,
```

```
SCB: 0xADAC4E88,  
Direction: outbound  
SPI : 0x7DD8ED8C  
Tunnel type: ra  
Protocol : esp
```

Creating IPsec inbound and outbound SA

```
[IKEv1 DEBUG]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, loading all IPSEC SAs
```

```
[IKEv1]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, Security negotiation complete for User  
(cisco) Responder, Inbound SPI = 0xd7311531, Outbound SPI = 0x4a35a7b4
```

```
[IKEv1]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, Adding static route for client address:  
192.168.1.1
```

Phase 2 negotiation completed

```
[IKEv1]: Group = vpnclient, Username = cisco, IP = 209.165.201.1, PHASE 2 COMP
```

# Software VPN Client Logs

## Initial Contact

To Launch the VPN client, click:

**Start | Programs | Cisco Systems VPN client | VPN Client | Log**

```
Cisco Systems VPN Client Version 5.0.02.0090
Copyright (C) 1998-2007 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
```

```
1      11:44:44.703  05/17/09  Sev=Info/4      CM/0x63100002
Begin connection process
```

```
2      11:44:44.703  05/17/09  Sev=Info/4      CM/0x63100004
Establish secure connection
```

```
3      11:44:44.703  05/17/09  Sev=Info/4      CM/0x63100024
Attempt connection with server "209.165.200.226"
```

```
4      11:44:44.718  05/17/09  Sev=Info/6      IKE/0x6300003B
Attempting to establish a connection with 209.165.200.226.
```

```
5      11:44:44.718  05/17/09  Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID(Xauth), VID(dpd), VID(E
T), VID(Unity)) to 209.165.200.226
```

```
6      11:44:44.765  05/17/09  Sev=Info/4      IPSEC/0x63700008
IPSec driver successfully started
```

```
8      11:44:44.765  05/17/09  Sev=Info/6      IPSEC/0x6370002C
Sent 12 packets, 0 were fragmented.
```

```
9      11:44:44.765  05/17/09  Sev=Info/5      IKE/0x6300002F
Received ISAKMP packet: peer = 209.165.200.226
```

VPN client initiates a new connection

# Software VPN Client Logs

## Aggressive Mode Exchange

```
10      11:44:44.765  05/17/09  Sev=Info/4      IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID(Unity), VID(dpd), VID(?), VID(Xauth), VID(Nat-T), KE, ID, NON,
HASH, NAT-D, NAT-D) from 209.165.200.226

11      11:44:44.765  05/17/09  Sev=Info/5      IKE/0x63000001
Peer is a Cisco-Unity compliant peer

12      11:44:44.765  05/17/09  Sev=Info/5      IKE/0x63000001
Peer supports DPD

14      11:44:44.765  05/17/09  Sev=Info/5      IKE/0x63000001
Peer supports XAUTH

15      11:44:44.765  05/17/09  Sev=Info/5      IKE/0x63000001
Peer supports NAT-T

16      11:44:44.781  05/17/09  Sev=Info/6      IKE/0x63000001
IOS Vendor ID Contruction successful

17      11:44:44.781  05/17/09  Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT, NAT-D, NAT-D. VID(?). VID(Unity))
to 209.165.200.226

18      11:44:44.781  05/17/09  Sev=Info/4      IKE/0x63000083
IKE Port in use - Local Port = 0x0454, Remote Port = 0x01F4

19      11:44:44.781  05/17/09  Sev=Info/5      IKE/0x63000072
Automatic NAT Detection Status:
Remote end is NOT behind a NAT device
This end is NOT behind a NAT device

20      11:44:44.781  05/17/09  Sev=Info/4      CM/0x6310000E
Established Phase 1 SA. 1 Crypto Active IKE SA, 0 User Authenticated IKE SA in the system
```

The 2<sup>nd</sup> packet of IKE exchange is decoded by the VPN client

VPN client sends the 3<sup>rd</sup> packet of IKE exchange

# Software VPN Client Logs

## XAUTH

```
25      11:44:44.781  05/17/09  Sev=Info/5      IKE/0x6300002F
Received ISAKMP packet: peer = 209.165.200.226

26      11:44:44.781  05/17/09  Sev=Info/4      IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 209.165.200.22627      11:44:44.781  05/17/09
      Sev=Info/4      CM/0x63100015
Launch xAuth application

28      11:44:48.078  05/17/09  Sev=Info/4      CM/0x63100017
xAuth application returned

29      11:44:48.078  05/17/09  Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 209.165.200.226

30      11:44:48.093  05/17/09  Sev=Info/5      IKE/0x6300002F
Received ISAKMP packet: peer = 209.165.200.226

31      11:44:48.093  05/17/09  Sev=Info/4      IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 209.165.200.226

32      11:44:48.093  05/17/09  Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 209.165.200.226

33      11:44:48.093  05/17/09  Sev=Info/4      CM/0x6310000E
Established Phase 1 SA.  1 Crypto Active IKE SA, 1 User Authenticated IKE SA in the system

34      11:44:48.109  05/17/09  Sev=Info/5      IKE/0x6300005E
Client sending a firewall request to concentrator

35      11:44:48.109  05/17/09  Sev=Info/5      IKE/0x6300005D
Firewall Policy: Product=Cisco Systems Integrated Client Firewall, Capability= (Centralized Protection
Policy).
```

← Router sends XAUTH request to VPN client

← XAUTH response to the ASA

← XAUTH status sent by ASA

← XAUTH status ack by VPN client

# Software VPN Client Logs

## Mode Config

```
36      11:44:48.109 05/17/09  Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 209.165.200.226

37      11:44:48.109 05/17/09  Sev=Info/5      IKE/0x6300002F
Received ISAKMP packet: peer = 209.165.200.226

38      11:44:48.109 05/17/09  Sev=Info/4      IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 209.165.200.226

39      11:44:48.109 05/17/09  Sev=Info/5      IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 192.168.1.10

40      11:44:48.109 05/17/09  Sev=Info/5      IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 10.1.1.20

42      11:44:48.109 05/17/09  Sev=Info/5      IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000

43      11:44:48.109 05/17/09  Sev=Info/5      IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: , value = cisco.com

44      11:44:48.109 05/17/09  Sev=Info/5      IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value = 0x00000001

45      11:44:48.109 05/17/09  Sev=Info/5      IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc ASA5520 Version 8.2(1)
built by builders on Tue 05-May-09 22:45
```

Mode Config Request

Mode Config response

# Software VPN Client Logs

## Quick Mode Exchange

```

48      11:44:48.109  05/17/09  Sev=Info/4      CM/0x63100019
Mode Config data received
50      11:44:48.125  05/17/09  Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 209.165.200.226
  
```

← 1<sup>st</sup> packet of Quick mode exchange

```

51      11:44:48.125  05/17/09  Sev=Info/5      IKE/0x6300002F
Received ISAKMP packet: peer = 209.165.200.226
  
```

```

52      11:44:48.125  05/17/09  Sev=Info/4      IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from
      209.165.200.226
  
```

← Response packet from router

```

55      11:44:48.125  05/17/09  Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 209.165.200.226
  
```

```

56      11:44:48.125  05/17/09  Sev=Info/5      IKE/0x63000059
Loading IPsec SA (MsgID=B848779F OUTBOUND SPI = 0x2C032B77 INBOUND SPI =
  
```

← 3<sup>rd</sup> packet of Quick mode exchange

```

57      11:44:48.125  05/17/09  Sev=Info/5      IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x2C032B77
  
```

```

58      11:44:48.125  05/17/09  Sev=Info/5      IKE/0x63000026
Loaded INBOUND ESP SPI: 0x6FF48217
  
```

← Current Routing Table

```

59      11:44:48.234  05/17/09  Sev=Info/5      CVPND/0x63400013
Destination      Netmask      Gateway      Interface      Metric
0.0.0.0          0.0.0.0      209.165.200.226  209.165.201.1  20
127.0.0.0        255.0.0.0    127.0.0.1      127.0.0.1      1
209.165.200.0    255.255.255.0  209.165.201.1  209.165.201.1  20
209.165.201.1    255.255.255.255  127.0.0.1      127.0.0.1      20
209.165.200.255  255.255.255.255  209.165.201.1  209.165.201.1  20
224.0.0.0        240.0.0.0    209.165.201.1  209.165.201.1  20
255.255.255.255  255.255.255.255  209.165.201.1  209.165.201.1  1
  
```

# Software VPN Client Logs

## Routing Table

60 11:44:49.078 05/17/09 Sev=Info/4 CM/0x63100034

The Virtual Adapter was enabled:

IP=192.168.1.10/255.0.0.0

DNS=10.1.1.20,0.0.0.0

WINS=0.0.0.0,0.0.0.0

Domain=cisco.com

Split DNS Names=

← Network settings of virtual interface

61 11:44:49.078 05/17/09 Sev=Info/5 CVPND/0x63400013

← Modified routing table

Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	209.165.200.226	209.165.201.1	20
14.0.0.0	255.0.0.0	192.168.1.10	192.168.1.10	20
192.168.1.10	255.255.255.255	127.0.0.1	127.0.0.1	20
14.255.255.255	255.255.255.255	192.168.1.10	192.168.1.10	20
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
209.165.200.0	255.255.255.0	209.165.201.1	209.165.201.1	20
209.165.201.1	255.255.255.255	127.0.0.1	127.0.0.1	20
209.165.200.255	255.255.255.255	209.165.201.1	209.165.201.1	20
224.0.0.0	240.0.0.0	192.168.1.10	192.168.1.10	20
224.0.0.0	240.0.0.0	209.165.201.1	209.165.201.1	20
255.255.255.255	255.255.255.255	192.168.1.10	192.168.1.10	1
255.255.255.255	255.255.255.255	209.165.201.1	209.165.201.1	1

62 11:44:49.093 05/17/09 Sev=Info/4 CM/0x63100038

Successfully saved route changes to file.

# Software VPN Client Logs

```
64      11:44:49.093  05/17/09  Sev=Info/6      CM/0x63100036
The routing table was updated for the Virtual Adapter

65      11:44:49.140  05/17/09  Sev=Info/4      CM/0x6310001A
One secure connection established

66      11:44:49.203  05/17/09  Sev=Info/4      CM/0x6310003B
Address watch added for 209.165.201.1.  Current hostname: home-pc, Current address(es): 192.168.1.10,
192.168.1.13, 209.165.201.1.

73      11:44:49.218  05/17/09  Sev=Info/4      IPSEC/0x6370002F
Assigned VA private interface addr 192.168.1.10
```

← Fully Functional Tunnel



# Common Issues

- In ASA/PIX7.0, enable **nem enable** under the group policy to allow Network Extension mode
- EasyVPN client functionality is limited to PIX 6.x. On the ASA 5505, it is supported on 7.2 or higher images.
- After decryption, PIX/ASA will check the access-lists or conduits against the decrypted IP packets; Access-lists or conduits need to be configured to permit decrypted IP traffic
- Enable **sysopt connection permit-vpn** to bypass the access-list/conduit checking against VPN traffic after decryption
- Unlike the router, ISAKMP is not enabled by default on the PIX or ASA. Use the command **isakmp enable <interface>** to enable it on an interface

# Conditional Debugs

- To limit the debug to a particular session or a peer, use the **debug crypto condition** command
- Useful to filter a session among thousands of peers

```
CiscoASA# debug crypto condition ?
exec mode commands/options:
  error      Display debug error messages regardless of filters
  group      Filter on a group name
  peer       Filter on a peer address or subnet
  reset      Clear the crypto debug filters
  spi        Filter on an IPsec SPI
  unmatched  Display messages with insufficient context to match
  a filter
  user       Filter on a user name
CiscoASA# debug crypto condition peer 209.165.201.1
CiscoASA# debug crypto isakmp 127
CiscoASA# debug crypto ipsec 127
```

# Conditional Debugs (Cont.)

```
CiscoASA# show crypto debug-condition
```

```
Crypto conditional debug is turned ON  
IKE debug context unmatched flag:  OFF  
IPSec debug context unmatched flag:  OFF  
IKE debug context error flag:  OFF  
IPSec debug context error flag:  OFF
```

```
IKE peer IP address filters:  
209.165.201.1/32
```

```
CiscoASA# show debug
```

```
debug crypto ipsec enabled at level 127  
debug crypto isakmp enabled at level 127
```

# Show Commands

## show crypto protocol statistics all

```
CiscoASA# show crypto protocol statistics all
```

```
[IKEv1 statistics]
```

```
Encrypt packet requests: 198  
Encapsulate packet requests: 198  
Decrypt packet requests: 198  
Decapsulate packet requests: 198  
HMAC calculation requests: 234  
SA creation requests: 2  
SA rekey requests: 0  
SA deletion requests: 1
```

```
[IPsec statistics]
```

```
Encrypt packet requests: 27  
Encapsulate packet requests: 27  
Decrypt packet requests: 27  
Decapsulate packet requests: 27  
HMAC calculation requests: 54  
SA creation requests: 4  
SA rekey requests: 0  
SA deletion requests: 2
```

# Show Commands (Cont.)

## show crypto isakmp sa

```
CiscoASA# show crypto isakmp sa
  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 209.165.201.1
   Type      : user           Role       : responder
   Rekey     : no            State      : AM_ACTIVE
```

## show crypto isakmp sa detail

```
CiscoASA# show crypto isakmp sa detail
  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 209.165.201.1
   Type      : user           Role       : responder
   Rekey     : no            State      : AM_ACTIVE
   Encrypt   : 3des          Hash        : SHA
   Auth      : preshared      Lifetime   : 86400
Lifetime Remaining: 86357
```

# Show Commands (Cont.)

```
show crypto ipsec sa
```

```
Router# show crypto ipsec sa
interface: FastEthernet0/1
  Crypto map tag: clientmap, local addr 209.165.200.226

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port):
  (192.168.1.10/255.255.255.255/0/0)
current_peer 209.165.201.1 port 4411
  PERMIT, flags={}
#pkts encaps: 203, #pkts encrypt: 203, #pkts digest: 203
#pkts decaps: 293, #pkts decrypt: 293, #pkts verify: 293
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

# Show Commands (Cont.)

## show crypto ipsec sa (Cont.)

inbound esp sas:

spi: 0x4579753B(1165587771)

transform: esp-3des esp-md5-hmac ,

in use settings ={RA, Tunnel, }

slot: 0, conn id: 3001, flow\_id: 1, crypto map: clientmap

sa timing: remaining key lifetime (sec): 28392

IV size: 8 bytes

replay detection support: Y

outbound esp sas:

spi: 0x8E1CB77A(2384246650)

transform: esp-3des esp-md5-hmac ,

in use settings ={RA, Tunnel, }

slot: 0, conn id: 3002, flow\_id: 2, crypto map: clientmap

sa timing: remaining key lifetime (sec): 28392

IV size: 8 bytes

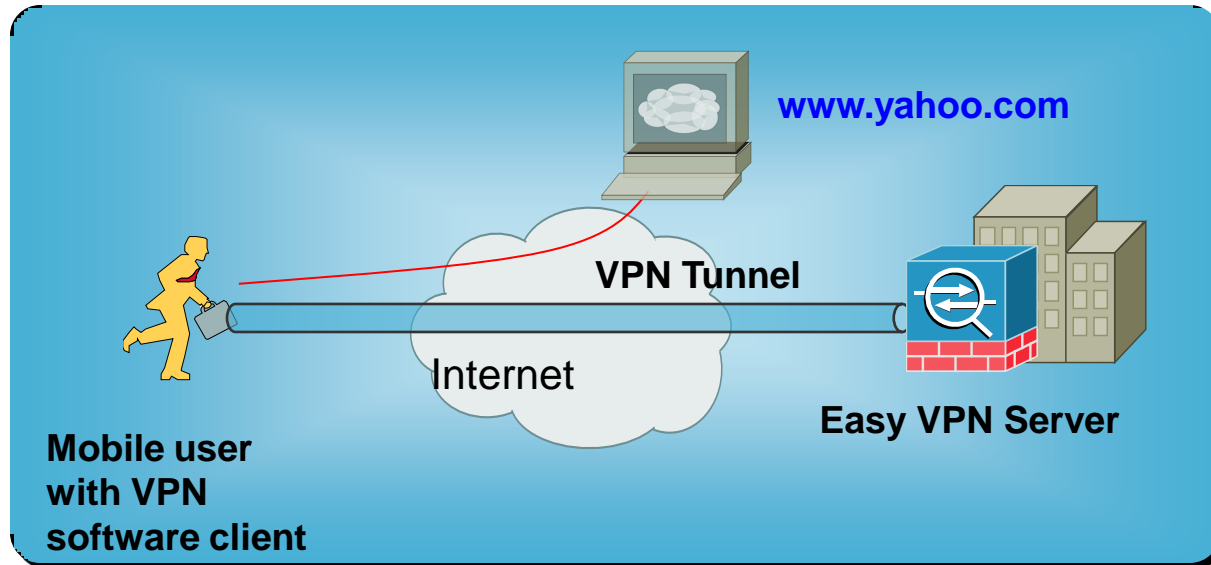
replay detection support: Y

# Cisco IPSec Remote Access VPN

## Feature Integration



# Centralized Policy Push Split Tunneling

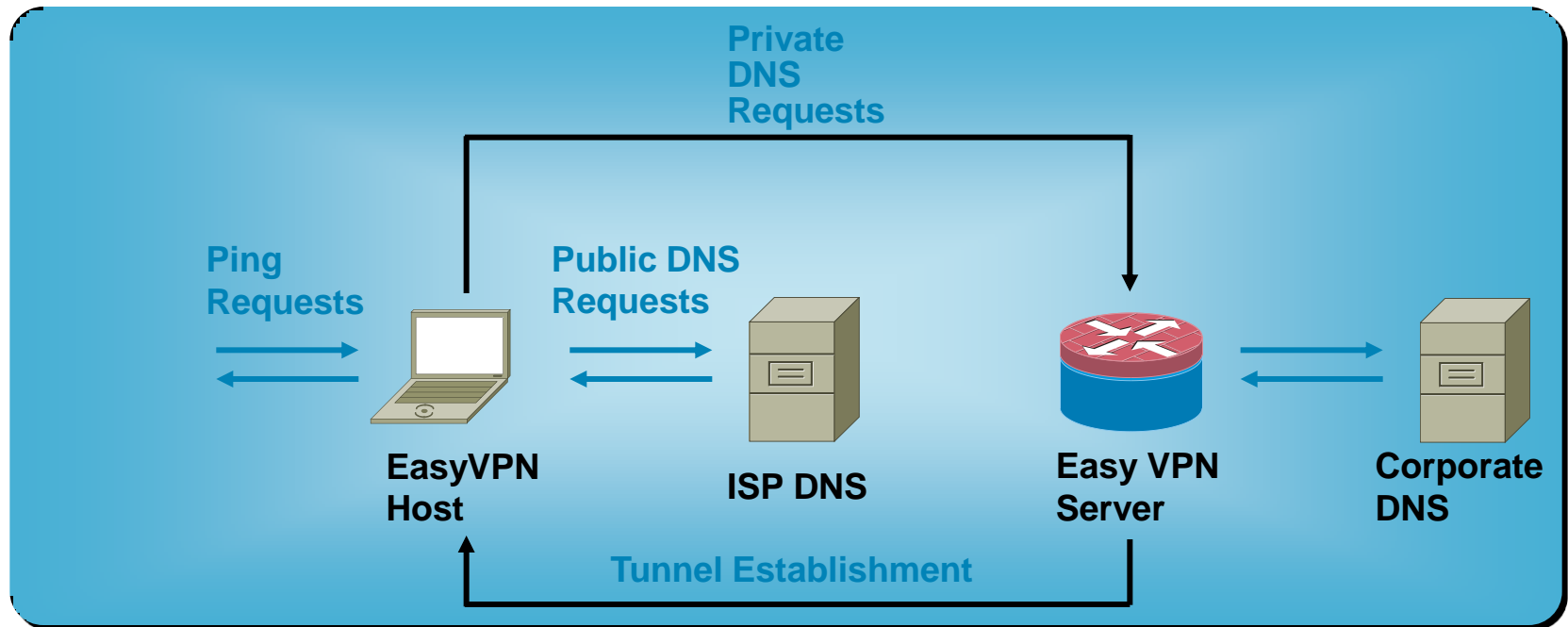


- Traffic goes directly to the Internet without forwarding it over the encrypted tunnel
- Less traffic over the tunnel saves bandwidth of the Easy VPN server and internal resources

```
access-list ST_List standard permit 10.1.1.0 255.255.255.0
```

```
group-policy vpnclient attributes  
split-tunnel-policy tunnelspecified  
split-tunnel-network-list value ST_List
```

# Centralized Policy Push Split DNS



- Reduced workload for internal DNS server
- Faster DNS resolve for Internet URLs
- Used in conjunction with split tunneling

```
CiscoASA(config)# group-policy vpnclient attributes  
CiscoASA(config-group-policy)# split-dns value cisco.com
```

# Network Integration

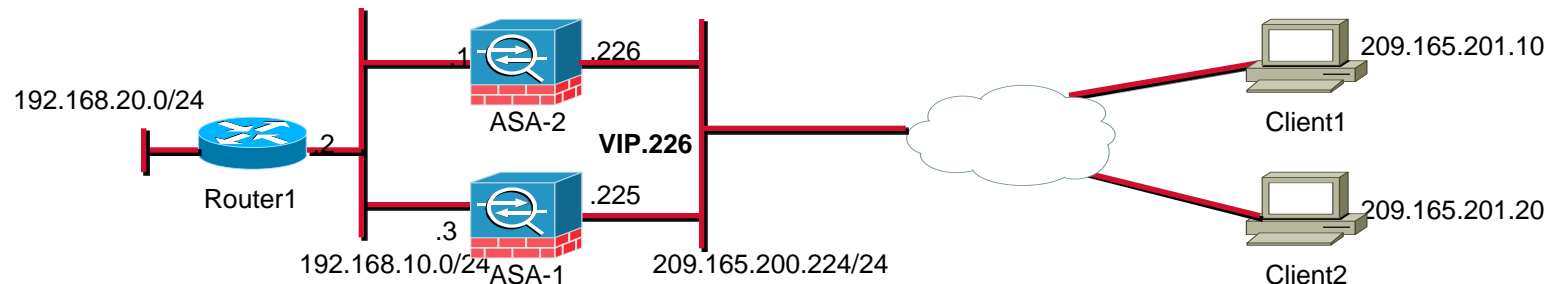
## VPN Load Balancing

### Problem Statement

- Our current Cisco ASA 5520 supports up to 750 remote access connections but we want to expand this functionality to more than 1000 users. What can we do?

### Solution:

- Buy a bigger box (such as ASA 5540) and replace it with 5520
- Buy another ASA5520 and enable load-balancing



vpn load-balancing  
cluster ip address 209.165.200.226  
priority 6  
participate

# Network Integration

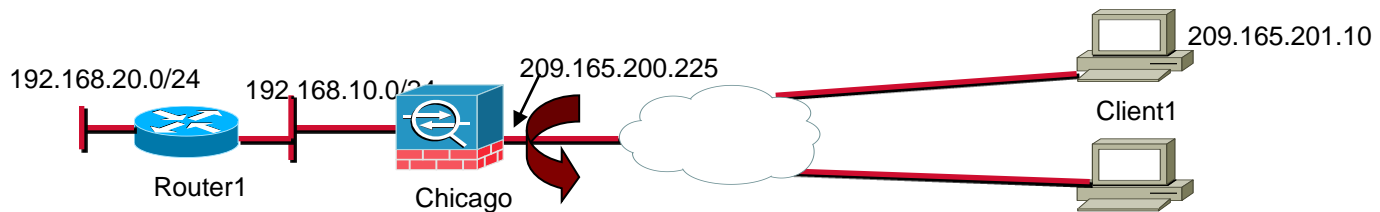
## IPSec Hairpinning

### Problem Statement

- We don't want to use split-tunneling and want all traffic to be tunneled to our ASA. How are the clients going to access the internet?

### Solution:

1. Enable IPSec hairpinning by permitting “intra-interface” routing
2. Configure nat and global statements to translate assigned addresses



*!--- Command that permits IPsec traffic to enter and exit the same interface.*

**same-security-traffic permit intra-interface**

[www.cisco.com](http://www.cisco.com)

*!--- The address pool for the VPN Clients.*

**ip local pool ippool 192.168.1.1-192.168.1.254**

*!--- The global address for Internet access used by VPN Clients.*

**global (outside) 1 209.165.200.230**

*!--- The NAT statement to define what to encrypt (the addresses from the IP-Pool).*

**nat (outside) 1 192.168.1.0 255.255.255.0**

# Network Integration

## Client Auto-update

### Problem Statement

- We have a large deployment of IPsec clients and they all run different software versions. We want to standardize our client deployment and want to use the same version of client software

### Solution:

- Use the client update feature to update the software and hardware based IPsec clients
- Use can choose to upgrade all IPsec clients, or the clients connected to specific tunnel groups

client-update enable

client-update type Windows url http://192.168.10.10/vpnclient-win-5.05.Rel-k9.exe  
rev-nums 5.05.Rel

# Network Integration

## Client Firewalling

### Problem Statement

- We want to use split-tunneling feature in our IPSec deployment, but we are concerned about the security of the VPN clients if they are accessing the internet directly. Can we do anything about it?

### Solution:

- You certainly can!!. Enable the firewall checks on the VPN client. During tunnel negotiations, the VPN client is checked for an active firewall process. If running, then the VPN client is allowed to connect

```
ASA(config-group-policy)# client-firewall req ?
```

```
cisco-integrated      Cisco Integrated Client Firewall
```

```
cisco-security-agent  Cisco Security Agent
```

```
...
```

```
zonelabs-zonearmorpro Zone Labs ZoneAlarm or ZoneAlarm Pro
```

```
zonelabs-zonealarmpro Zone Labs ZoneAlarm Pro
```

```
ASA(config-group-policy)# client-firewall req cisco-security-agent
```

# Network Integration

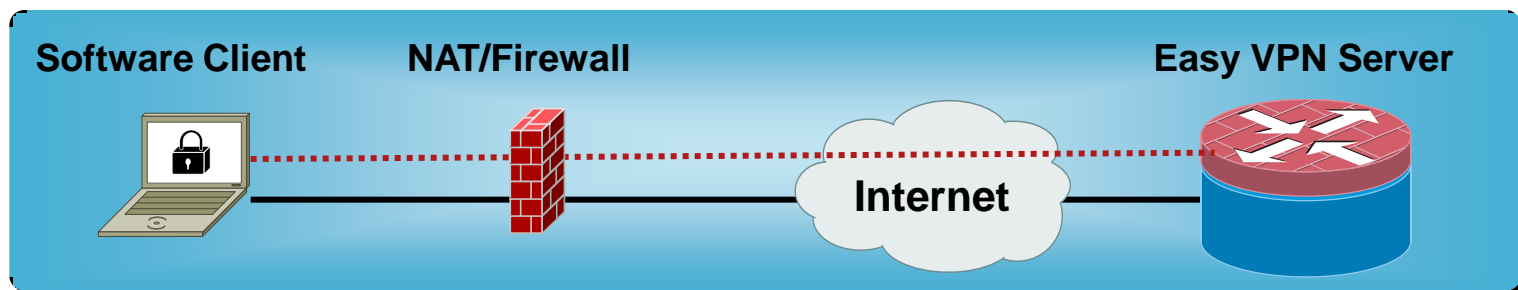
## TCP-Based Firewall Traversal

### Problem Statement

- Mobile users operating out of hotel rooms and airports often see their IPSec traffic blocked by third party firewall/NAT devices
- Original NAT Traversal specifications (NAT-T, rfc3947 and rfc3948) do not consider this

### Solution: Cisco Tunneling Control Protocol (cTCP)

- IPSec traffic tunneled inside TCP, traverses firewall and NAT



```
CiscoASA(config)# isakmp ipsec-over-tcp port 10000
```

Enable IPSec over TCP on the VPN client under Transparent tunneling

# NAT Issues with IPSec on ASA/PIX

- Nat needs to be bypassed on the PIX/ASA in order for the remote side to access the private network behind the ASA seamlessly
- ASA/PIX 7.0 allows NAT enforcement to be disabled by using the **no nat-control** command. NAT enforcement is turned off by default
- If nat-control is enabled, use the **NAT 0** command with an access list to achieve that

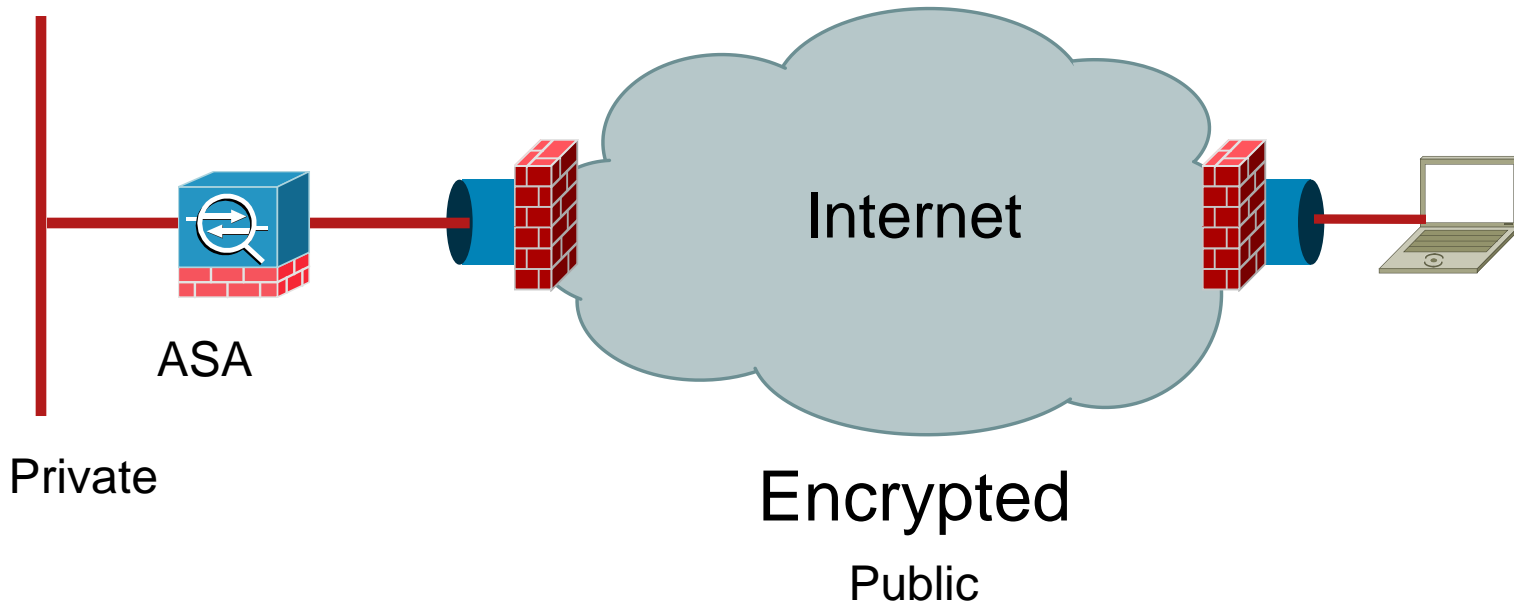
```
access-list no-nat permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0  
nat (inside) 0 access-list no-nat
```



# NAT in the Middle of an IPSec Tunnel

- In many cases, VPN clients are behind NAT/PAT devices
- **IPSec pass-thru** feature is supported on certain NAT/PAT devices; ISAKMP cookie and ESP SPI are used to build translation table
- IPSec over NAT (NAT Traversal or NAT-T) support was first introduced in version 6.3 for PIX
- Use **isakmp nat-traversal <natkeepalive>** to turn on NAT-T on PIX/ASA
- Turn on IPSec over UDP or IPSec over TCP feature in PIX/ASA 7.x/8.x

# Firewall in the Middle



- ESP (IP protocol type 50)
- UDP port 500 (ISAKMP), and/or UDP port 4500 (NAT-T)
- If ISP blocks ISAKMP, use IPsec over TCP

# Firewalling and IPSec

- Firewall on the IPSec endpoint PIX

**Sysopt connection permit-vpn** (no conduit or access-list is needed)

**Use of conduits or access-list** (no sysopt connection permit-ipsec is needed—gives you more security for the decrypted pkts)

# Cisco IPSec Remote Access VPN

## Case Study

# Case Studies (Remote IPSec VPN)

## Requirements:

SecureMe has recently installed a Cisco ASA in its Brussels office to provide VPN access to its mobile users. They want:

1. All traffic from the VPN clients to be encrypted even if they access the internet.
2. To ensure VPN traffic passes through even if ISP blocks ESP or ISAKMP traffic
3. To check for a firewall on remote workstations before establishing the connectivity.
4. To use a centralized user database for authentication

# Case Studies (Remote IPSec VPN)

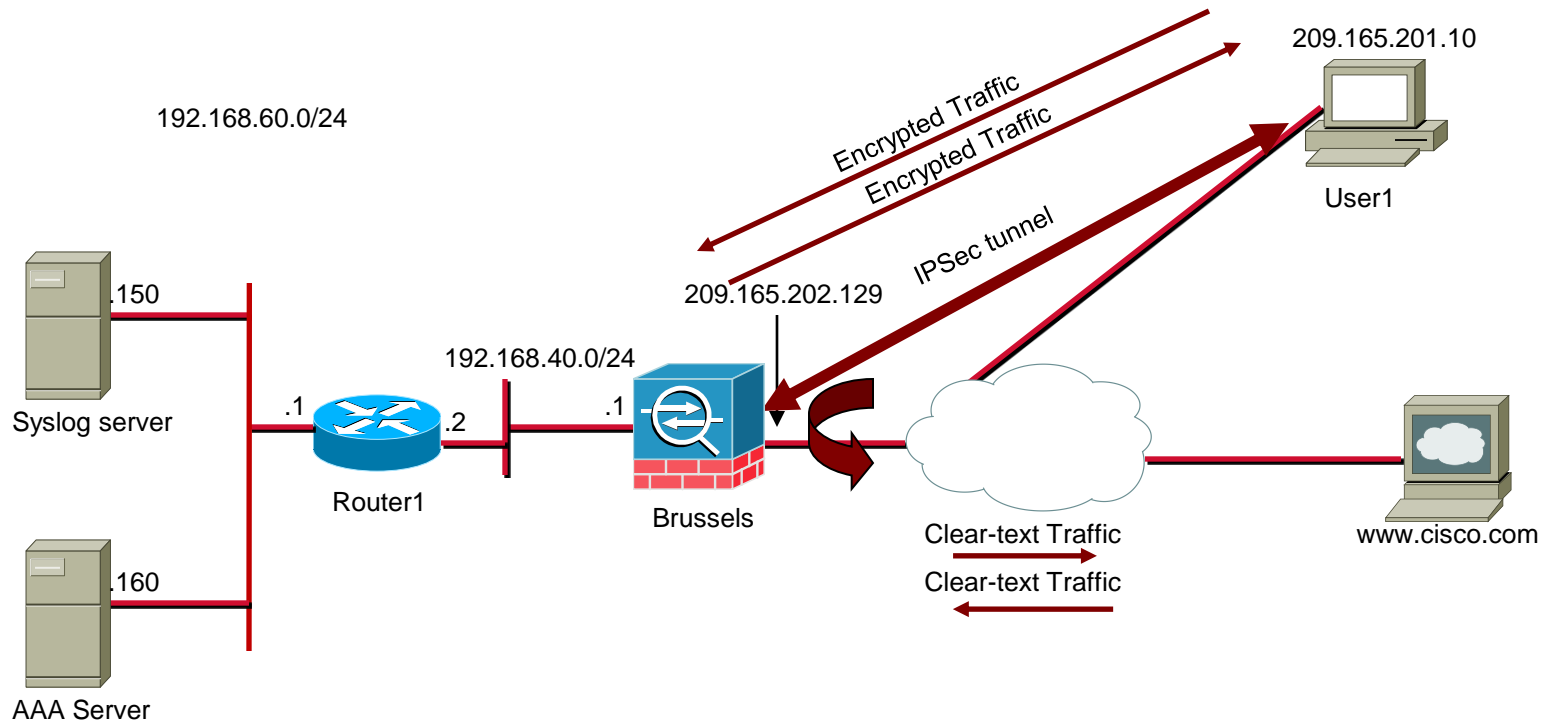
## Solution:

A solution has been put together with the following key points:

1. Disable split tunneling and encrypt all traffic leaving the clients
2. Enforce Cisco Security Agent check.
3. Use IPSec over TCP on port 9000 as the encapsulation protocol.
4. Configure IPSec hairpinning to allow VPN clients to talk to host on the internet.
5. Use radius authentication for remote VPN users.

# Case Studies (Remote IPsec VPN)

## Topology:



# Case Studies (Remote IPsec VPN)

## Configuration:

! To Allow IPsec hairpinning on the same interface  
same-security-traffic permit intra-interface

! Enable logging to send syslog messages to 192.168.60.150

logging enable

logging timestamp

logging host inside 192.168.60.150

logging trap notifications

! IP Pool used to assign IP address to the VPN client

ip local pool ippool 192.168.50.1-192.168.50.100 mask 255.255.255.0

! Default gateways.

route outside 0.0.0.0 0.0.0.0 209.165.202.130 1

route inside 192.168.60.0 255.255.255.0 192.168.40.2

! RADIUS Server Definition

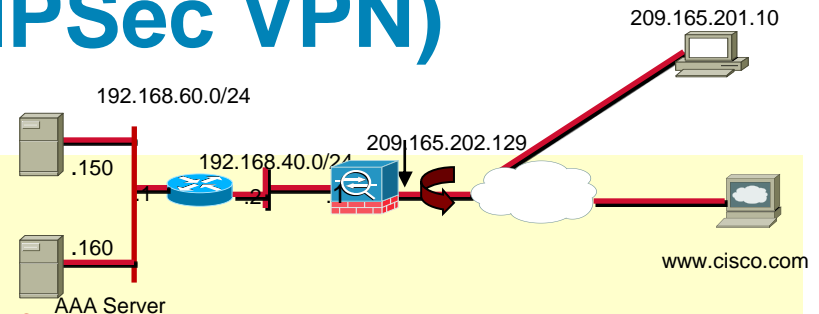
aaa-server RADIUS protocol radius

aaa-server RADIUS (inside) host 192.168.60.160

! Address Translation

global (outside) 1 209.165.202.132

nat (outside) 1 192.168.50.0 255.255.255.0





# Case Studies (Remote IPsec VPN)

## Configuration:

! Configuration of an internal user-group called SecureMeGrp  
group-policy SecureMeGrp internal

! Configuration of user-group attributes  
group-policy SecureMeGrp attributes  
default-domain value securemeinc.com  
client-firewall req cisco-security-agent

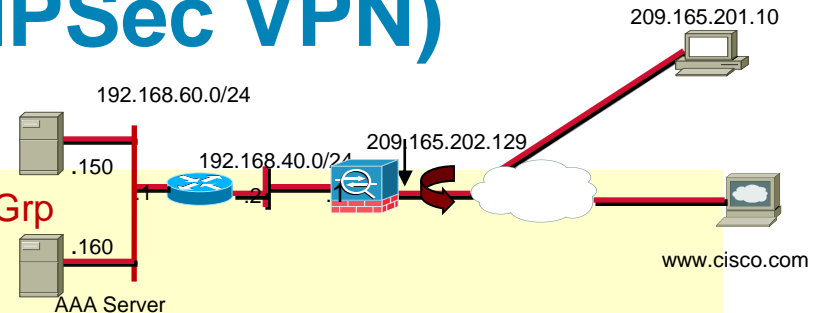
! sysopt to bypass traffic filters  
sysopt connection permit-vpn

! Transform set to specify encryption and hashing algorithm  
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac

! Dynamic crypto-map for Remote-Access Clients  
crypto dynamic-map outside\_dyn\_map 10 set transform-set ESP-3DES-SHA

! Dynamic crypto-map is mapped to the static crypto-map  
crypto map outside\_map 65535 ipsec-isakmp dynamic outside\_dyn\_map

! Static crypto-map is applied to the outside interface  
crypto map outside\_map interface outside



# Case Studies (Remote IPsec VPN)

## Configuration:

### ! isakmp configuration

```
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
```

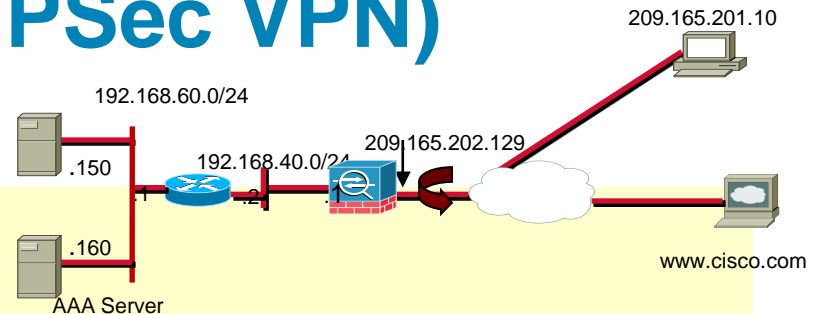
### ! Tunnel Encapsulation to use IPsec over TCP over port 9000

```
isakmp ipsec-over-tcp port 9000
```

### ! tunnel-group configuration for VPN client. The group name is ciscovpn

```
tunnel-group ciscovpn type ipsec-ra
tunnel-group ciscovpn general-attributes
authentication-server-group RADIUS
address-pool ippool
default-group-policy SecureMeGrp
```

```
tunnel-group ciscovpn ipsec-attributes
pre-shared-key *
```



# Case Studies (Connectivity Issue on ASA)

## Scenario:

You are responsible for managing the IPSec remote access solution on an ASA. All VPN users claim that they can access resources on the private network, but cannot access any resources on the internet.

What can you do to troubleshoot this issue?

# Case Studies (Connectivity Issue on ASA)

## Some ideas to troubleshoot this issue:

- 1) Verify the VPN tunnel is successfully established
  - a) Show crypto isakmp sa
  - b) Show crypto ipsec sa
  
- 2) Send traffic from the VPN client to a host over the Internet.
  
- 3) Verify the VPN traffic is transmitted by the VPN client
  - a) Status -> Statistics
  - b) If traffic is not transmitted, make sure that:
    - i. Deterministic Network Adaptor is bound to the physical interface
    - ii. Split-Tunneling is disabled
  
- 4) Verify the traffic is being received by the ASA
  - a) Show crypto ipsec sa

# Case Studies (Connectivity Issue on ASA)

## Some ideas to troubleshoot this issue:

### 5) Verify the Cisco ASA is configured with the following:

*!-- Command that permits IPsec traffic to enter and exit the same interface.*  
**same-security-traffic permit intra-interface**

*!-- The address pool for the VPN Clients.*  
**ip local pool ippool 192.168.1.1-192.168.1.254**

*!-- The global address for Internet access used by VPN Clients.*  
**global (outside) 1 209.165.200.230**

*!-- The NAT statement to define what to encrypt (the addresses from the IP-Pool).*  
**nat (outside) 1 192.168.1.0 255.255.255.0**

### 6) Check if traffic is redirected by the ASA to an internet site

#### a) Capture traffic sent by VPN client to an internet host

*!-- Define an ACL to identify traffic originated by VPN destined to cisco.com (internet host) and vice-versa.*

**access-list DebugInternetACL permit tcp host 209.165.200.230 host 198.133.219.25 eq 25**  
**access-list DebugInternetACL permit tcp host 198.133.219.25 eq 25 host 209.165.200.230**

*!-- Enable Capture with the ACL mapped to it. Apply it to the outside interface (internet facing)*  
**capture DebugInternet access-list DebugInternetACL interface outside**

# Case Studies (Connectivity Issue on ASA)

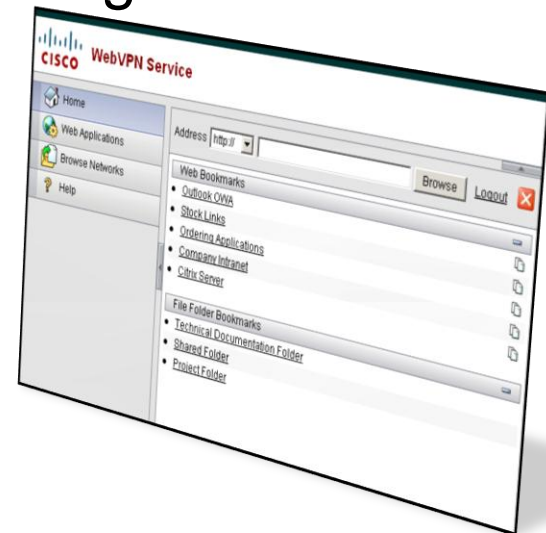
## Some ideas to troubleshoot this issue:

- 5) Verify traffic is transmitted and received
  - a) Show capture DebugInternet
  
- 6) If clear-text traffic is received and transmitted by the ASA, but not encrypted back to the VPN client, check:
  - a) NAT statements
    - i. Show running nat
    - ii. Show running global
    - iii. Show running static
  - b) Firewall ACLs
    - i. Show access-list
  
- 7) If traffic is encrypted by the ASA and not received by the VPN client, check for firewalls and NAT devices between the VPN peers.

# Remote Access SSL VPNs

# Secure Sockets Layer (SSL) Overview

- Protocol developed by Netscape for secure e-commerce
- Creates a tunnel between web browser and web server
  - Authenticated and encrypted (RC4, 3DES, DES, AES)
- Capability shipped by default in leading browsers
  - Self-signed certificate
- `https://`
  - Usually over port :443
  - Closed lock indicates SSL-enabled





# SSL VPN Introduction

## Clientless

- Basic web access
- E-mail access
- CIFS access
- Customized user screen

## Thin-Client

- Port redirection for only TCP applications
- Smart tunnel

## Client-Based

- Full-SSL tunnel
- AnyConnect
- SVC
- CSD

# Clientless SSL VPN

# Clientless Access (Web-Based Applications)

- **Applications**

- Support for Intranet HTML web pages and web-based (webified) applications

- Added support for OWA 2000/2003

- Added support for Windows file share (CIFS)

- **Benefits**

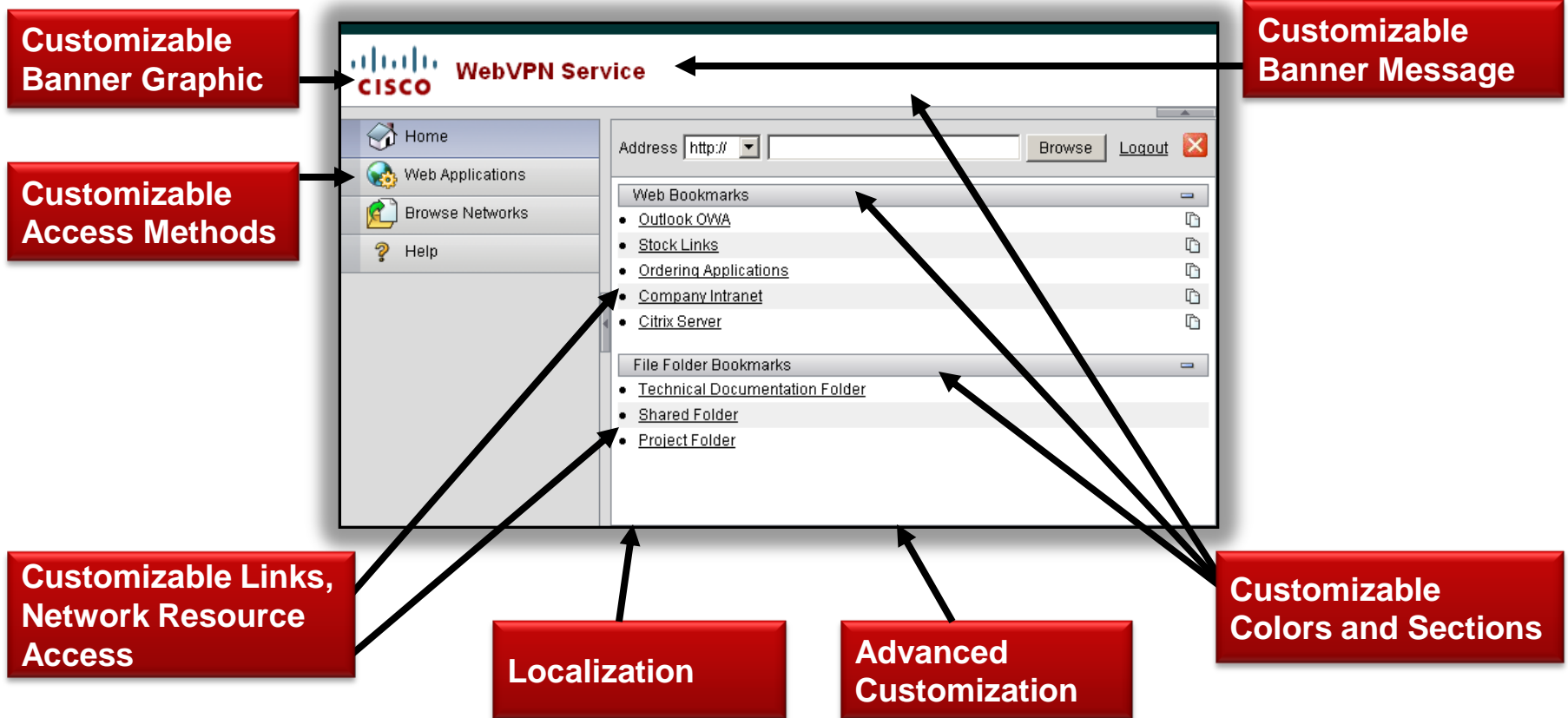
- This is where a user can connect in, with little requirements beyond a basic web browser

- Do not require admin rights on the machine

- **Restrictions**

- Rewrite engine needs constant support due to dynamic content; common issues with embedded Java and Active X applets

# SSL VPN Clientless (L7) Customization



# Complex Content Handling

- Smart Tunnels

Allows **Winsock v2** TCP applications to use the VPN security appliance as a proxy gateway to the private side of a network

- Port Forwarding

Local “thin” client acts as proxy

Tunnels and forwards application traffic

- Application Profile Customization Framework

- Plug-ins

Cirtix ICA, RDP, SSH/TELNET, VNC provided by Cisco

Extensible framework for other popular protocols

# Smart Tunnels

## Applications Use VPN Appliance as Proxy Gateway

- Must create list of “authorized” processes
- Smart Tunnels loads a stub into each authorized process and intercepts socket calls and redirects them through the VPN appliance
- The parent of each authorized process passes on the information (cookie, etc.) to its children if a child is an authorized process
- Example
  - Launch telnet via telnet.exe
  - telnet.exe must be authorized process

# Configuring Clientless (WebVPN) SSL VPN

## ASDM Wizard

**SSL VPN Wizard**

**SSL VPN Wizard**

**SSL VPN Connection Type (Step 1 of 6)**

The security appliance provides Secure Socket Layer (SSL) remote access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption. The security appliance provides two different types of SSL VPN connection.

Please select the type of SSL VPN connection to configure:

**Clientless SSL VPN Access**

The security appliance allows SSL-enabled web browsers to access HTTP or HTTPS web servers on a portal page.

Cisco SSL VPN Client (AnyConnect VPN Client)

The security appliance downloads a self-installing AnyConnect VPN Client to the remote PC that allows full, secure access to resources of an internal corporate network.

**Select Clientless SSL VPN Access**

Browser based Internet SSL VPN Gateway Group Policy

Cisco Client Internet SSL VPN Gateway Group Policy

< Back Next > Finish Cancel Help

# SSL VPN Wizard (Cont.)

**SSL VPN Wizard**

**SSL VPN Interface (Step 2 of 6)**

Provide a connection name and the interface that SSL VPN users connect to.

Connection Name:

The interface users access for SSL VPN connections.

SSL VPN Interface:

**Digital Certificate**

When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.

Certificate:

**Connection Group Settings**

Connection Group Alias/URL

Display Group Alias list at the login page

**Information**

URL to access SSL VPN Service: <https://209.165.201.1>

URL to access SSL VPN Service via group-url: <https://209.165.201.1/vpn>

URL to access ASDM: <https://209.165.201.1/admin>

< Back   Next >   Finish   Cancel   Help

Connection Name Is an Arbitrarily Name

Interface Where VPN Users Will Connect

Select Installed Digital Certificate that VPN User's Web Browser Will Use

Connection Alias



# SSL VPN Wizard (Cont.)

**SSL VPN Wizard**

**SSL VPN Wizard**

**User Authentication (Step 3 of 6)**

The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login.

Authenticate using a AAA server group

AAA Server Group Name:

Authenticate using the local user database

**User to be Added**

Username:

Password:

Confirm Password:

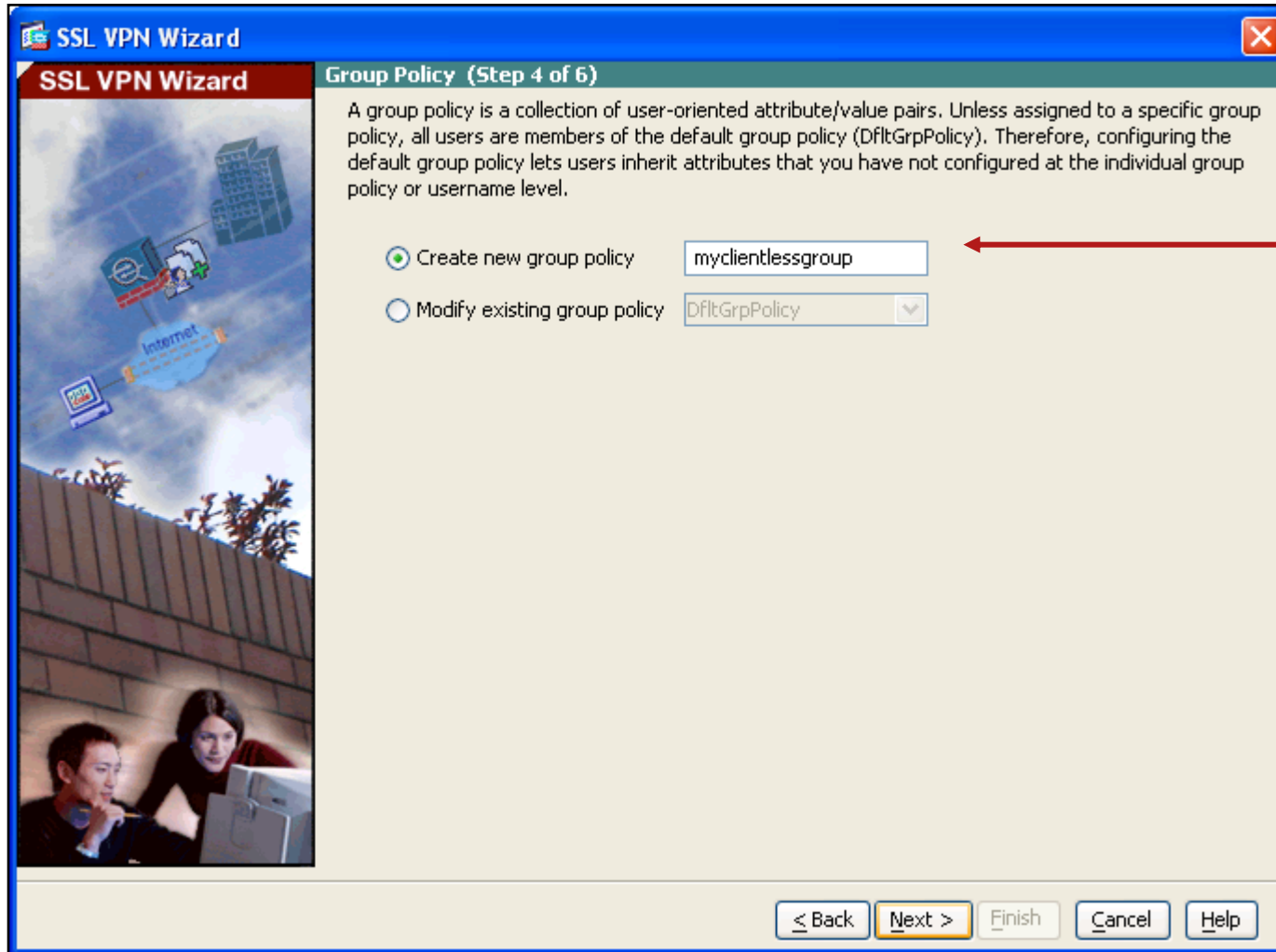
user1

< Back Next > Finish Cancel Help

This Option Allows You to Configure AAA Groups for External Authentication Servers (i.e., Radius, AD, SDI, LDAP, etc.)

In this Example Local Users Are Created

# SSL VPN Wizard (Cont.)



**A New Group Policy Is Created Called myclientlessgroup.**

**A Group Policy Is a Collection of User Attributes and Value Pairs.**

# SSL VPN Wizard (Cont.)

The screenshot displays the SSL VPN Wizard configuration interface, showing four steps in the process of configuring bookmark lists for clientless connections.

**Step 1:** In the **Clientless Connections Only - Bookmark List (Step 5 of 6)** window, the **Bookmark List** is set to **-- None --**. The **Manage...** button is highlighted with a red box and the number 1.

**Step 2:** In the **Configure GUI Customization Objects** window, the **Add** button is highlighted with a red box and the number 2.

**Step 3:** In the **Add Bookmark List** window, the **Bookmark List Name** is set to **Intranet Sites**. This text is highlighted with a red box and the number 3.

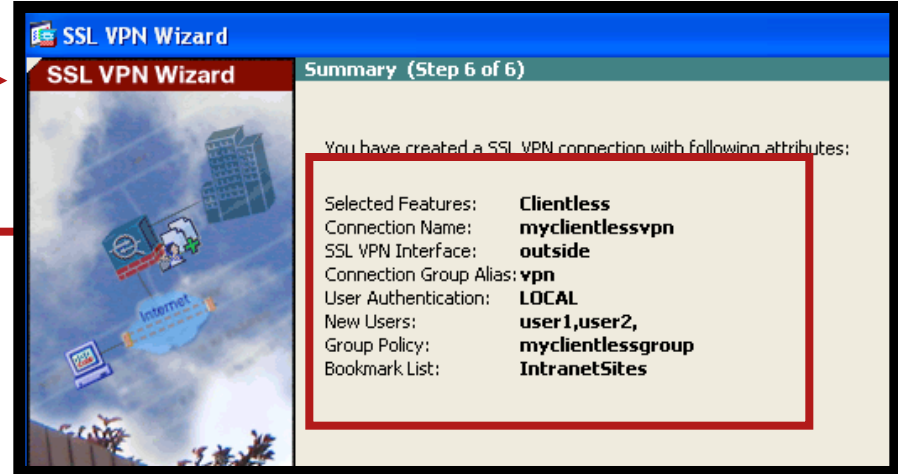
**Step 4:** In the **Add Bookmark Entry** window, the **Bookmark Title** is set to **Main Employee Intranet Site** and the **URL Value** is set to **http://intranetsite.cisco.com**. These fields are highlighted with a red box and the number 4.

# SSL VPN Wizard (Cont.)

## CLI Configuration

```
webvpn
  enable outside
  tunnel-group-list enable
group-policy myclientlessgroup internal
group-policy myclientlessgroup attributes
  vpn-tunnel-protocol webvpn
webvpn
  url-list value IntranetSites
username user1 password 08S9WUsiSMr3RauN encrypted privilege 0
username user1 attributes
  vpn-group-policy myclientlessgroup
username user2 password 08S9WUsiSMr3RauN encrypted privilege 0
username user2 attributes
  vpn-group-policy myclientlessgroup
tunnel-group myclientlessvpn type remote-access
tunnel-group myclientlessvpn general-attributes
  default-group-policy myclientlessgroup
tunnel-group myclientlessvpn webvpn-attributes
  group-alias vpn enable
  group-url https://209.165.201.1/vpn enable
```

## ASDM Summary



SSL VPN Wizard Summary (Step 6 of 6)

You have created a SSL VPN connection with following attributes:

Selected Features:	<b>Clientless</b>
Connection Name:	<b>myclientlessvpn</b>
SSL VPN Interface:	<b>outside</b>
Connection Group Alias:	<b>vpn</b>
User Authentication:	<b>LOCAL</b>
New Users:	<b>user1,user2,</b>
Group Policy:	<b>myclientlessgroup</b>
Bookmark List:	<b>IntranetSites</b>

# Client/Server Plug-ins

## Feature Overview

- ASA v8.0 and later supports a number of common client/server applications via Java plugins such as

Windows Terminal Server (RDP)

Telnet/SSH

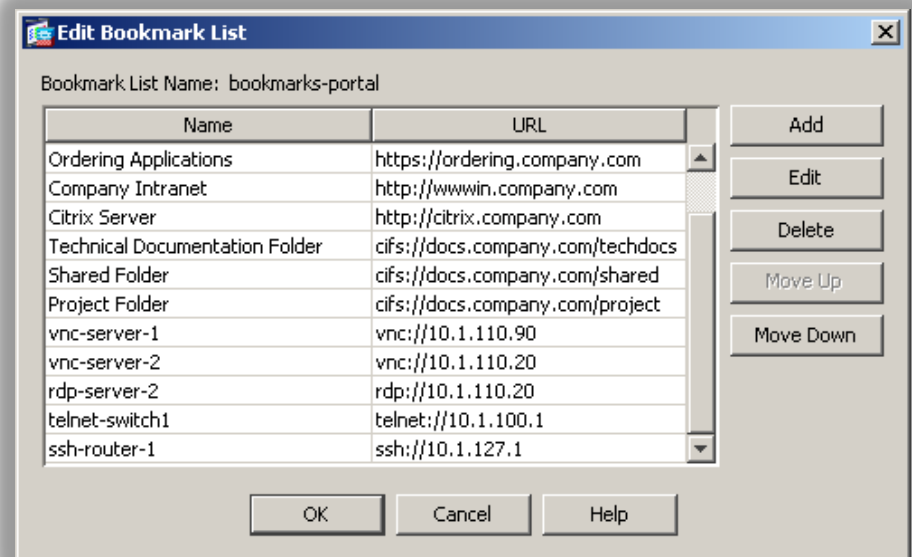
Citrix ICA Client

VNC

- Resource is defined as a URL with the appropriate protocol type

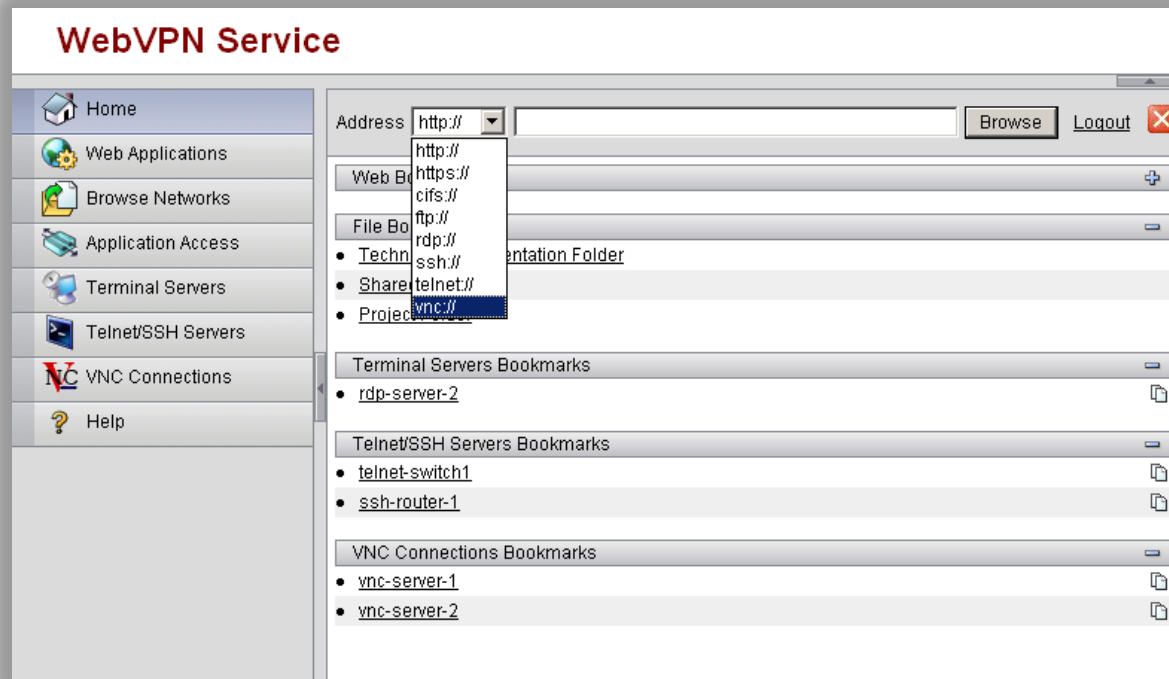
`rdp://server:port`

- Support for these third party applications exists in the form of packaged single archive files in the .jar file format

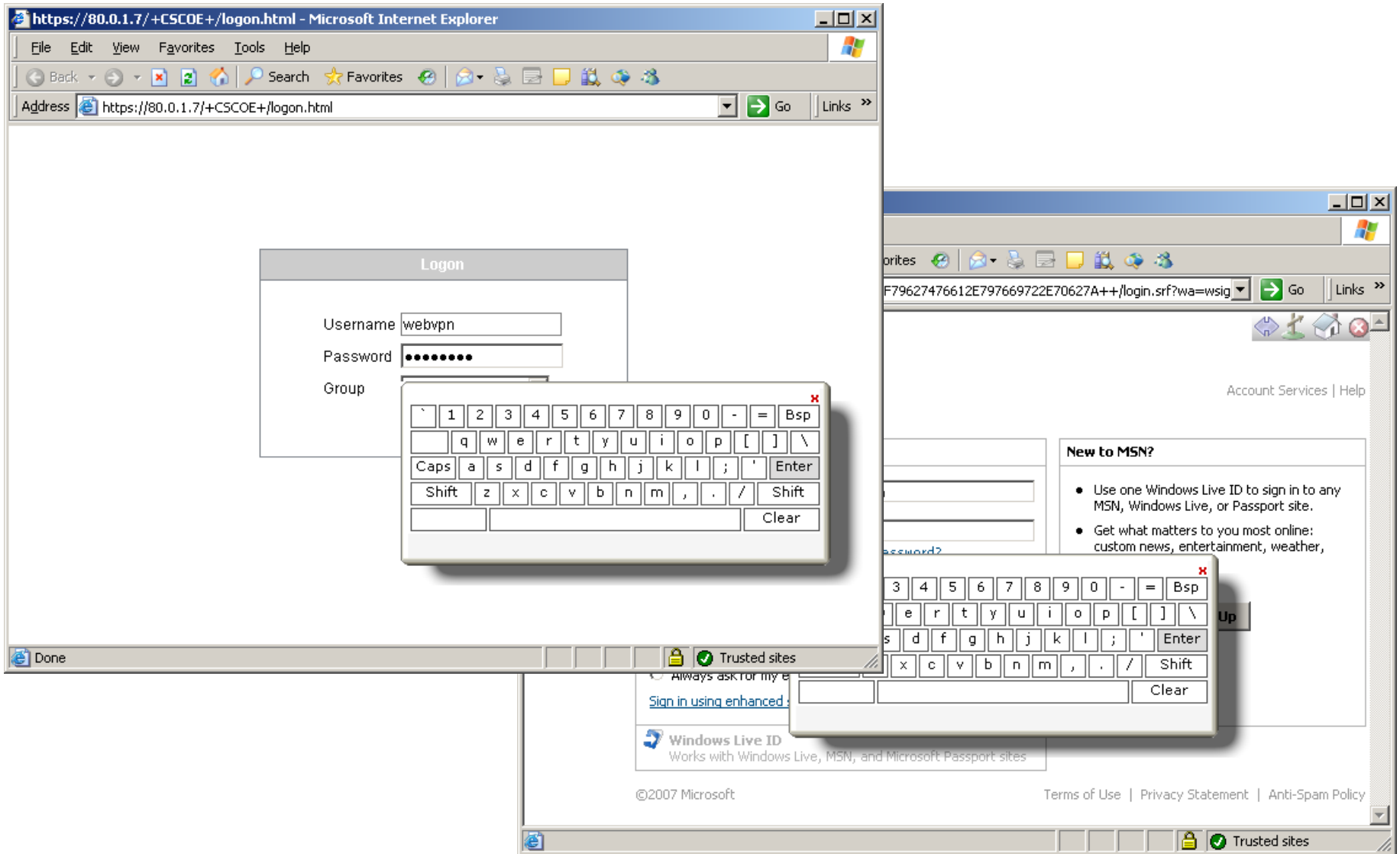


# Client/Server Plug-ins

- When clicking on a resource link, a dynamic page is generated that hosts the ActiveX/Java applet
- The Java applet is rewritten and re-signed, ActiveX parameters are rewritten, and the helper port-forwarder ActiveX is injected if needed
- The Java applet is transparently cached in the gateway cache



# Virtual Keyboard



# Double Authentication

Two-factor authentication for Anyconnect and Clientless SSL VPN for compliance with the Payment Card Industry (PCI) Standards Council Data Security Standard.

## New tunnel-group general-attributes commands:

**secondary-authentication-server-group** - the secondary AAA server group (cannot be an SDI server)

**secondary-username-from-certificate** - Allows for extraction of a few standard DN fields from a certificate for use as a username.

**secondary-pre-fill-username** - Enables username extraction for Clientless or AnyConnect client connection.

**authentication-attr-from-server** – Specifies which authentication server authorization attributes are applied to the connection.

**authenticated-session-username** - Specifies which authentication username is associated with the session.



# Configuring Double Authentication

The screenshot displays the Cisco ASDM 6.2 interface for configuring a Remote Access VPN. The configuration is divided into several sections, with five key steps highlighted by red boxes and numbered 1 through 5:

- Step 1:** The **Configuration** tab is selected in the top navigation bar.
- Step 2:** The **Remote Access VPN** section is expanded in the left-hand navigation pane.
- Step 3:** The **Secondary Authentication** sub-section is selected under the Remote Access VPN configuration.
- Step 4:** In the **Add SSL VPN Connection Profile** dialog, the **Server Group** dropdown menu is set to **my-radius-group**.
- Step 5:** A secondary dialog titled **Assign Secondary Authorization Server Group to Int...** is shown, where the **Server Group** dropdown is set to **Microsoft\_AD**.

The main configuration window shows the following settings for the **Secondary Authentication** section:

- Default Secondary Authentication Server Group:** my-radius-group
- Attributes Server:** Primary (selected)
- Secondary Name Server:** Primary (selected)
- Interface-Specific Secondary Authentication Server Groups:** A list containing Microsoft\_AD.

The status bar at the bottom indicates: "Device configuration loaded successfully." and the system time is 3/23/09 9:07:24 AM UTC.

# General Authentication Problems

**DEBUG = debug webvpn 255**

## Good Authentication

```
WebVPN: calling AAA with ewsContext (-925550560) and nh (-927982512)!  
WebVPN: started user authentication...  
WebVPN: AAA status = (ACCEPT)  
WebVPN: user: (user1) authenticated.
```

## Bad Authentication

```
WebVPN: calling AAA with ewsContext (-925889312) and nh (-927982512)!  
WebVPN: started user authentication...  
WebVPN: AAA status = (REJECT)  
WebVPN: user: (user1) rejected.  
http_remove_auth_handle(): handle 4 not found!
```

# RADIUS Authentication Problems

DEBUG = debug radius

## RADIUS Server not Responding

```
RADIUS packet decode (authentication request)
-----
Raw packet data (length = 63).....
01 01 00 3f 57 44 2d 62 f3 b0 29 ae 4f dc e5 ba   |   ...?WD-b..) .O...
6b c8 61 86 01 07 75 73 65 72 31 02 12 68 63 cb   |   k.a...user1..hc.
44 f0 ac 02 03 1c a0 59 d8 80 78 95 7a 04 06 0a   |   D.....Y..x.z...
Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 1 (0x01)
Radius: Length = 63 (0x003F)
Radius: Vector: 57442D62F3B029AE4FDCE5BA6BC86186
Radius: Type = 1 (0x01) User-Name
Radius: Length = 7 (0x07)
Radius: Value (String) = 75 73 65 72 31 |   user1
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.200.10.1 (0x0AC80A01)
...
send pkt 172.18.85.181/1645
RADIUS_SENT:server response timeout
RADIUS_DELETE
```

# Domain Authentication Problems

**DEBUG = debug ntdomain**

## Domain Controller Communication Problem

```
smb: negotiate phase failed: syserr = Network is down  
Cifs_Connect_Server() returned FALSE, error_code = 18  
ntdomain_process_ntinfo - state is NTDOMAIN_DELETE  
INFO: Attempting Authentication test to IP address  
<172.18.85.123> (timeout: 12 seconds)  
ERROR: Authentication Server not responding: No error
```

**Note:** In this Example the Administrator Attempts to Authenticate to the Active Directory Server Using the TEST Utility Within ASDM

# Authentication Test Utility

The screenshot shows the Cisco ASDM 6.0 for ASA interface. The main window displays the configuration for AAA Server Groups. A dialog box titled "Test AAA Server - 172.18.85.123" is open, prompting the user to enter a username and password for testing. The dialog box contains the following information:

- AAA Server Group: NTGroup (NT Domain)
- Host: 172.18.85.123
- Authentication options:  Authorization,  Authentication
- Username: domainuser
- Password: \*\*\*\*\*

The "Test" button in the dialog box is highlighted with a red box. The background configuration table shows the following AAA Server Groups:

Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		
NTGroup	NT Domain		Depletion

Using the CLI:

test aaa-server authentication NYGroup host 172.18.85.123 user domainuser password 123qweasd

# Additional Notes

## Additional External Authentication Debugs

`debug ldap (1-255)`

`debug sdi (1-255)`

`debug kerberos (1-255)`

You Can Combine the Debugs Listed Above with the **debug webvpn**, when Troubleshooting Clientless Authentication Problems.

# Clientless SSL VPN Debugs

Problem	Debug Command
Accessing CIFS Shares	debug webvpn cifs (1-255)
Accessing NFS Shares	debug webvpn nfs(1-255)
Citrix Connection Problems	debug webvpn citrix (1-255)
Javascript Mangling Problems (User Specific)	debug webvpn javascript trace user user1

# Useful Show Commands

## show webvpn statistics

```
asa# show webvpn statistics
Total number of objects served          105
      html                             55
      js                                2
      css                               21
      vb                                0
      java archive                       3
      java class                          2
      image                              11
      undetermined                       1
```

## show webvpn group-alias

```
asa1# show webvpn group-alias
Tunnel Group: myclientlessvpn          Group Alias: vpn enabled
```



# Capturing WebVPN Data

The CLI **capture** Command Lets You Log Information About Websites that Do not Display Properly over a WebVPN Connection. This Data Can Help You Troubleshoot Problems.

To start the WebVPN capture utility use the following command:

```
capture <capture_name> type webvpn user  
<webvpn_username>
```

**For Example:**

```
hostname# capture mycapture type webvpn user user1  
WebVPN capture started.  
capture name mycapture  
user name user1
```

# Anyconnect Client

# Cisco AnyConnect VPN client

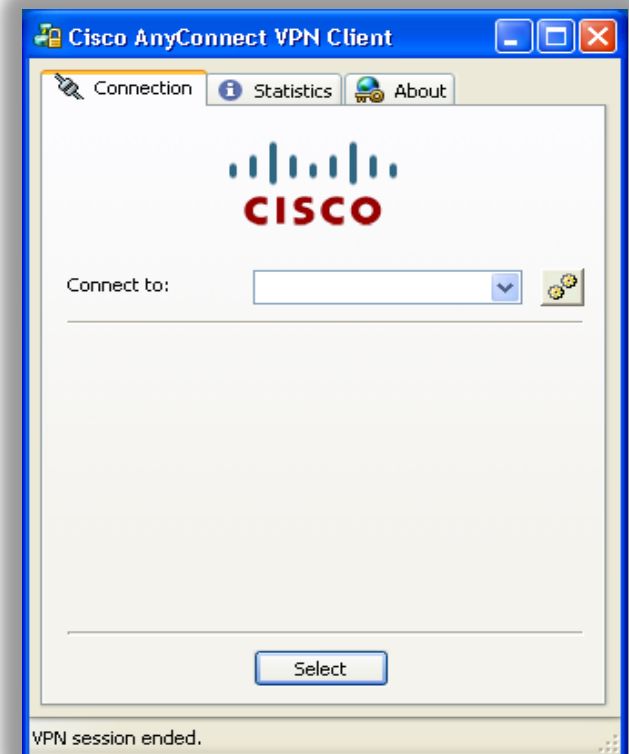
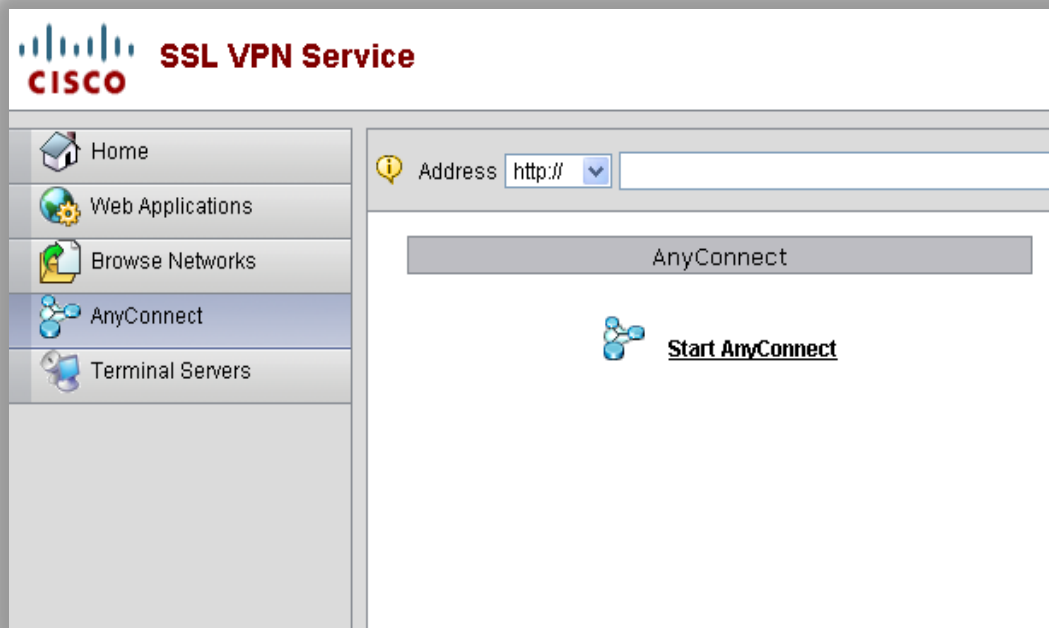
“Thick client”, “Full Tunneling”, or “Tunnel” Client

- Traditional-style client delivered via automatic download
- Requires administrative privileges for initial install only
- Pre-deployment MSI package available
- Can use TLS or DTLS as transport
- Can be upgraded from a previous version upon connection
- Can create client profiles for personalization
- User configurable preference for:
  - Local LAN Access
  - Minimize on Connect
  - Connect on start-up

# Cisco AnyConnect VPN client

## Methods of Deployment:

- Web-based
- Pre-deploy (Standalone client)



# AnyConnect Essentials

**AnyConnect Essentials** is a separately licensed SSL VPN client, entirely configured on the Cisco ASA, that provides the full AnyConnect capability, with the following exceptions:

- No CSD (including HostScan/Vault/Cache Cleaner)
- No clientless SSL VPN
- Optional Windows Mobile Support

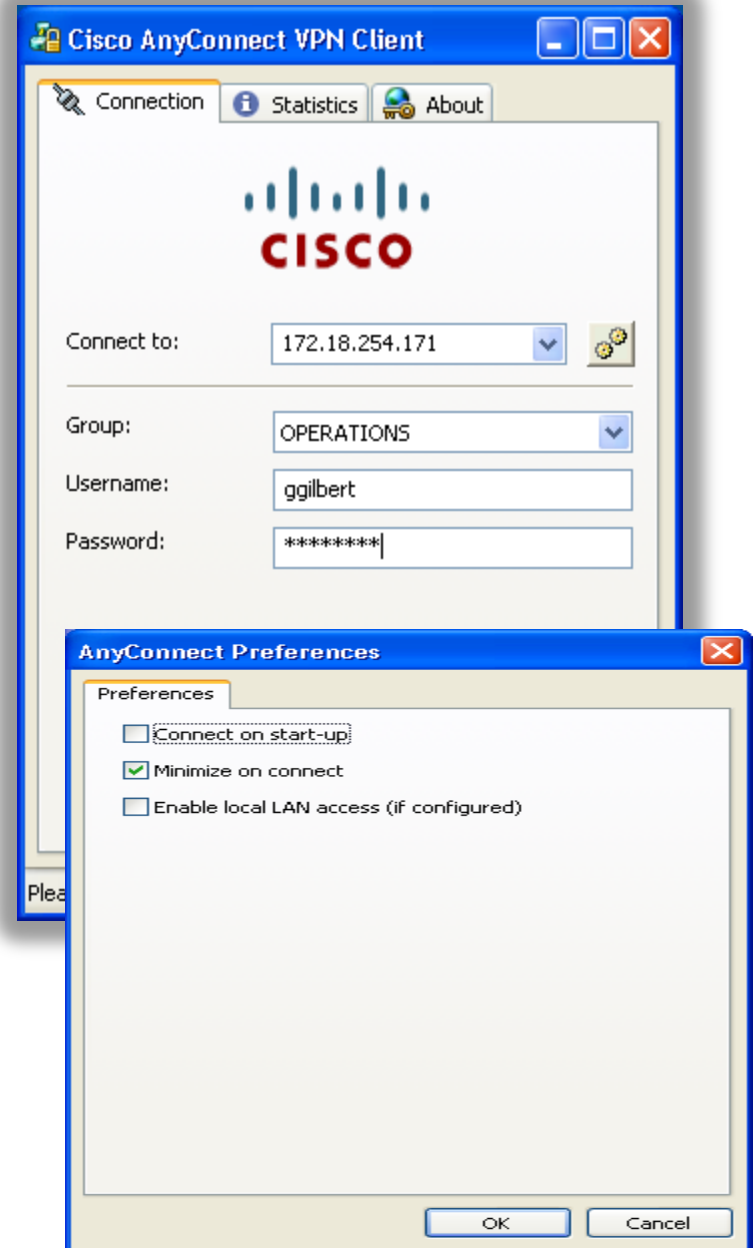
**ASDM:** Configuration > Remote Access VPN > Advanced > AnyConnect Essentials License

**CLI:**                   webvpn  
                          anyconnect-essentials

# AnyConnect Client

## Cisco AnyConnect VPN Client for Secure Remote Productivity

- Extends the in-office experience
  - LAN-like full-network access, supports latency sensitive apps like voice (via DTLS transport)
- Access across platforms
  - Windows 2K/XP (x86/x64)/Vista (x86/x64)
  - Mac OS X 10.4 and 10.5, Linux Intel
  - Windows Mobile 5 Pocket PC Edition (coming soon)
- Only supported on ASA 8.0 and later
  - No reboots required
  - Standalone, web launch, portal connection
  - Start before login (2K/XP)
  - MSI—Windows preinstallation package
  - Initial installation requires admin rights; however, upgrading an existing install with a pushed package does not



# AnyConnect Client (Cont.)

## Cisco AnyConnect VPN Client—GUI Details (Statistics)

The image displays two screenshots of the Cisco AnyConnect VPN Client GUI. The left screenshot shows the main 'Statistics' tab with a 'Details...' button circled in red and labeled '1'. A red arrow points from this button to the right screenshot. The right screenshot shows the 'Statistics Details' window with an 'Export...' button circled in red and labeled '2'.

**Statistics**

Tunnel State:	Connected
Client Address:	10.21.104.31
Server Address:	171.70.192.85
Bytes Sent:	1082580
Bytes Received:	337148
Time Connected:	00:03:25

**Connection Information**

Tunnel State:	Connected
Tunneling Mode:	All Traffic
Duration:	00:02:39

**Bytes**

Sent:	1079430
Received:	335247

**Frames**

Sent:	1682
Received:	1283

**Address Information**

Client:	10.21.104.31
Server:	171.70.192.85

**Transport Information**

Protocol:	DTLS
Cipher:	RSA_AES_256_SHA1
Compression:	None
Proxy Address:	No Proxy

**Posture Assessment**

Last Performed:	Disabled
-----------------	----------

The **Export** Button Saves the Information on the **Details** Screen, Along with Other Connection Information, to a Text File for Troubleshooting

# AnyConnect—Command Line Syntax

```
webvpn
  enable outside
  cache-fs limit 15
  svc image disk0:/vpn-win32-Release-2.0.0090-k9.pkg 1
  svc image disk0:/vpn-Linux-Release-2.0.0090-k9.pkg 2
  svc image disk0:/vpn-Darwin_powerpc-Release-2.0.0090-k9.pkg 3
  svc image disk0:/vpn-Darwin_i386-Release-2.0.0090-k9.pkg 4
  svc image disk0:/sslclient-win-1.1.2.169.pkg 5
  svc enable
  dtls enable outside
```

```
group-policy MyGroup attributes
  webvpn
    svc dtls enable
```



# AnyConnect User XML Profile

**The AnyConnect Client Uses an XML File for User Profiles and Configuration Settings**

- On Windows machines, the profile will be stored in  
Documents and Settings\All Users\Application  
Data\Cisco\Cisco AnyConnect VPN  
Client\Profile\AnyConnectProfile.tmp
- On non-Windows machines the location will be  
`/opt/cisco/vpn/profile/AnyConnectProfile.tmp`
- The profile may be validated using the `AnyConnectProfile.xsd` file.  
This file is installed during installation
- On Windows the preferences are stored in: `C:\Documents and  
Settings\<user>\Application Data\Cisco\Cisco AnyConnect VPN  
Client\preferences.xml`

# AnyConnect ASA Config for XML Profile

```
webvpn
memory-size percent 25
enable outside
enable inside
cache-fs limit 15
svc image disk0:/vpn-win-Release-
  2.0.1-k9.pkg 1
svc profiles newProfile3
  disk0:/AnyConnectProfile.xml
svc enable

group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol svc webvpn
user-authentication enable
address-pools value myPool
webvpn
  svc compression none
  svc profiles value newProfile3
  svc ask enable
  http-comp none
```

- On the ASA, the XML profile is loaded into file management and then configured under the webvpn section globally and then for the group
- Note that the xml file name does not have to be AnyConnectProfile.xml
- A new file “newProfile3” will appear on the workstation with an XML extension
- More than one profile may be loaded into the global webvpn section but only one is allowed per group

# Troubleshooting AnyConnect

- Logging on Windows will utilize the Windows event viewer; review the log messages in **Cisco AnyConnect VPN Client**
- You can save the “Cisco AnyConnect VPN Client” log from the event viewer in **“.evt” format**

Linux location:  
**/var/log/messages**

Mac location:  
**/var/log/system.log**

**Configuration Settings:**  
Keep Installed: enabled  
Rekey Method: disabled  
Compression: disabled  
Proxy: pac url  
(<http://www.myCorp.com/myPACFile.pac>)  
Local LAN: disabled  
Split Tunneling: disabled  
Client Address: **10.10.11.170**  
Client IPv6 Address: unknown  
MTU: 1300  
TLS Keep Alive: disabled  
TLS Rekey Interval: none  
TLS DPD: 0  
DTLS: disabled  
DTLS Keep Alive: disabled  
DTLS Rekey Interval: none  
DTLS DPD: 30

# Event Viewer

## An Example of How Windows Event Viewer Looks

The screenshot displays the Windows Event Viewer application. The left pane shows the event log hierarchy with 'Cisco AnyConnect VPN Client' selected. The main pane shows a list of 162 events for this source. The 'Event Properties' dialog is open, showing details for an error event.

Type	Date	Time
Information	2/9/2007	10:03:46 ...
Error	2/9/2007	10:03:46 ...
Information	2/9/2007	10:03:46 ...
Information	2/9/2007	10:03:46 ...
Warning	2/9/2007	10:03:46 ...
Error	2/9/2007	10:03:46 ...
Information	2/9/2007	10:03:46 ...
Information	2/9/2007	10:03:46 ...
Warning	2/9/2007	10:03:46 ...
Information	2/9/2007	10:03:46 ...
Information	2/9/2007	10:03:46 ...
Error	2/9/2007	10:03:46 ...
Information	2/9/2007	10:03:46 ...
Information	2/9/2007	10:03:46 ...
Information	2/9/2007	10:03:43 ...
Information	2/9/2007	10:03:43 ...
Warning	2/8/2007	6:55:31 PM
Warning	2/8/2007	6:55:31 PM

**Event Properties**

Event

Date: 2/9/2007 Source: vpngina  
Time: 10:03:46 AM Category: None  
Type: Error Event ID: 1  
User: N/A  
Computer: TABLETPC

Description:

Function: loadProfile  
Return code: 0  
File: C:\temp\build\thehoff\release0.936942955233-Fri-19-Jan-2007-15-40-16\release\Api\ProfileMgr.cpp  
Line: 201  
Description: Duplicate host <sjc> found in the profile <C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile\sjcprofile.xml>. Host discarded.

Data:  Bytes  Words

OK Cancel Apply

# Show Commands

```
ciscoasa# show vpn-sessiondb summary
```

```
Active Session Summary
```

```
Sessions:                Active : Cumulative : Peak Concurrent
WebVPN                   :           2 :           13 :           7
SSL VPN Client           :           1 :           4 :           1
Email Proxy              :           0 :           0 :           0
IPSec LAN-to-LAN        :           0 :           0 :           0
IPSec Remote Access     :           0 :           0 :           0
Totals                   :           3 :           17
```

```
License Information:
```

```
IPSec : 250 Configured : 250 Active : 0 Load : 0%
WebVPN : 250 Configured : 250 Active : 2 Load : 1%
Total : 500 Configured : 500 Active : 2 Load : 0%
```

```
Active : Cumulative : Peak Concurrent
IPSec : 0 : 0 : 0
WebVPN : 2 : 13 : 7
Totals : 2 : 13
```

```
Tunnels:                Active : Cumulative : Peak Concurrent
WebVPN                   :           2 :           13 :           7
SSL-Tunnel               :           1 :           4 :           1
Totals                   :           3 :           17
```

# AnyConnect Logging

```
ciscoasa(config)# logging class auth console 6
```

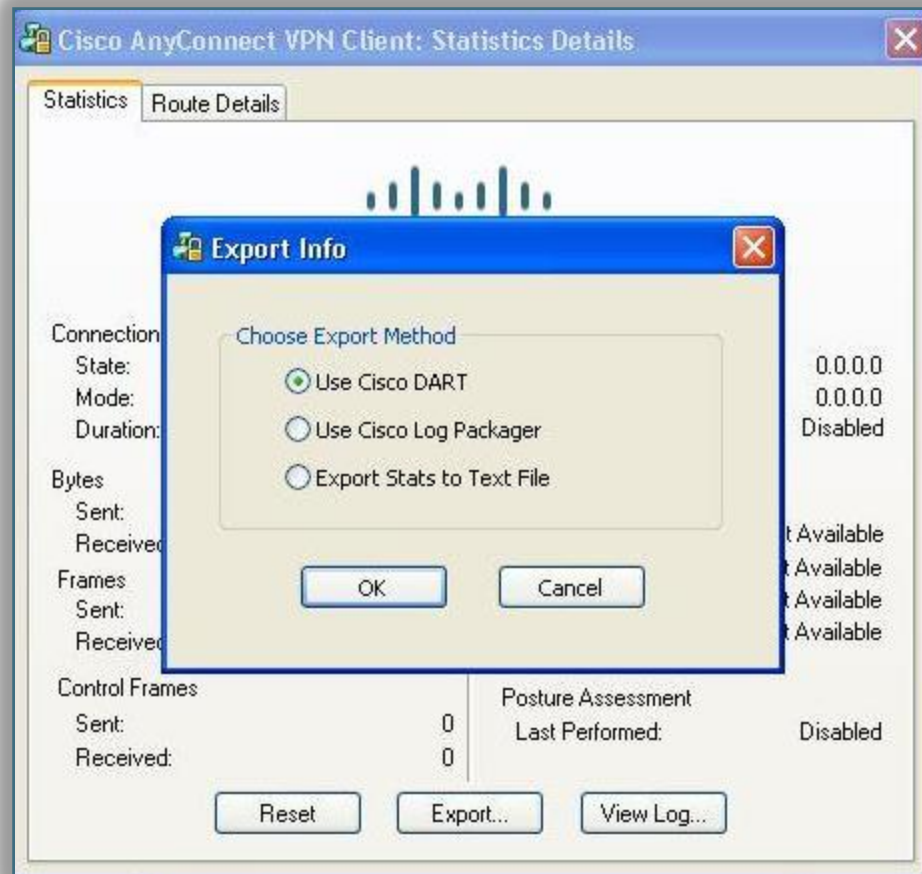
```
%ASA-6-113012: AAA user authentication Successful : local database : user = basic
%ASA-6-113003: AAA group policy for user basic is being set to DfltGrpPolicy
%ASA-6-113011: AAA retrieved user specific group policy (DfltGrpPolicy) for user =
basic
%ASA-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user = basic
%ASA-6-113008: AAA transaction status ACCEPT : user = basic
%ASA-4-113019: Group = DefaultWEBVPNGroup, Username = basic, IP = 10.209.10.3, Session
disconnected. Session Type: Remote-Access, Duration: 0h:00m:25s, Bytes xmt: 1918,
Bytes rcv: 9611, Reason: Unknown
```

```
ciscoasa(config)# logging class webvpn console 7
```

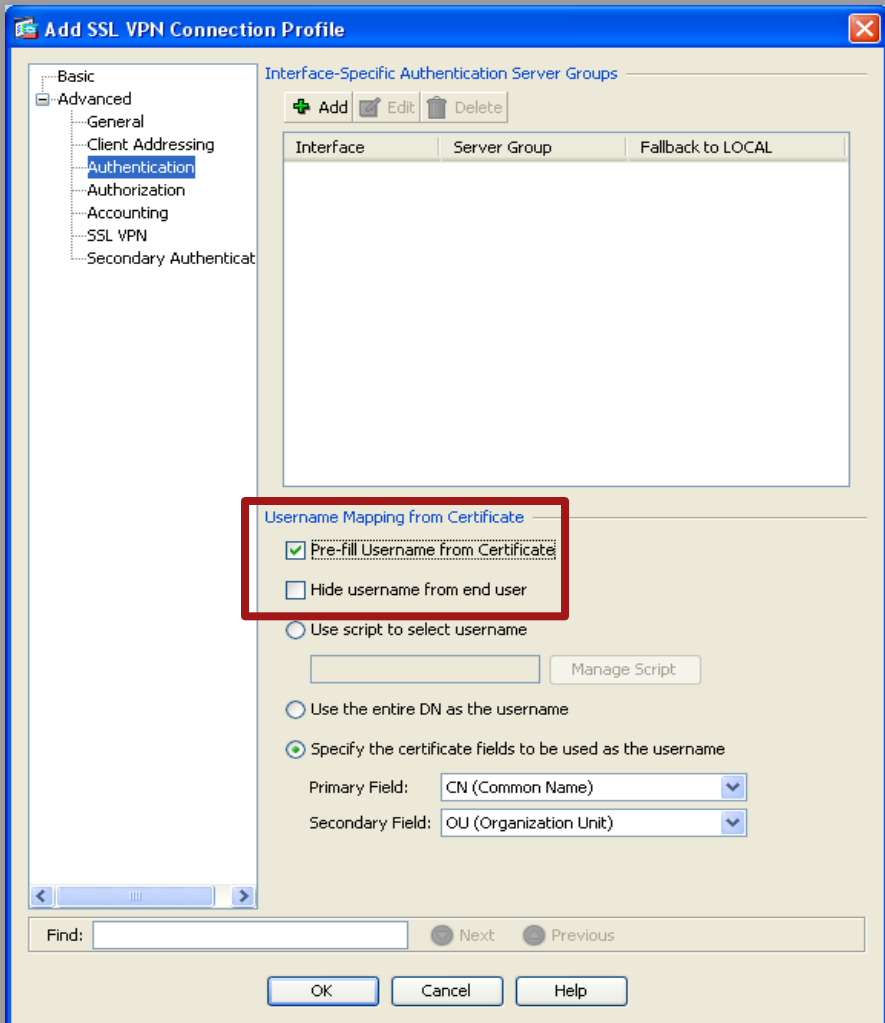
```
%ASA-6-716001: Group <DfltGrpPolicy> User <basic> IP <10.10.10.3> WebVPN
session started.
%ASA-6-716038: Group <DfltGrpPolicy> User <basic> IP <10.10.10.3>
Authentication: successful, Session Type: WebVPN.
%ASA-6-716002: Group <DfltGrpPolicy> User <basic> IP <10.10.10.3> WebVPN
session terminated: User Requested.
```

# Diagnostic AnyConnect Reporting Tool (DART)

**DART** bundles specified log files and diagnostic information that can be used for analyzing and debugging the AnyConnect client connection.



# Pre-fill Username from Certificate



- Enables the use of a **username** extracted from a certificate for username/password authentication and authorization. The username is “pre-filled” into the login screen, with the user being prompted only for the password.
- To use this feature, you must configure both the **pre-fill username** and the **username-from-certificate** commands in **tunnel-group general-attributes** configuration mode.

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Advanced > Authentication .



# Miscellaneous Features

- **EKU Extensions for Certificate Mapping** - ability to create certificate maps that look at the Extended Key Usage extension of a client certificate and use these values in determining what connection profile the client should use. If the client does not match that profile, it uses the default group.
- Clientless SSL VPN sessions now support **Microsoft Office SharePoint Server 2007**.
- **Shared license for SSL VPN sessions** - you can purchase a shared license with a large number of SSL VPN sessions and share the sessions as needed among a group of adaptive security appliances by configuring one of the adaptive security appliances as a shared license server, and the rest as clients.

# Cisco Secure Desktop (CSD)

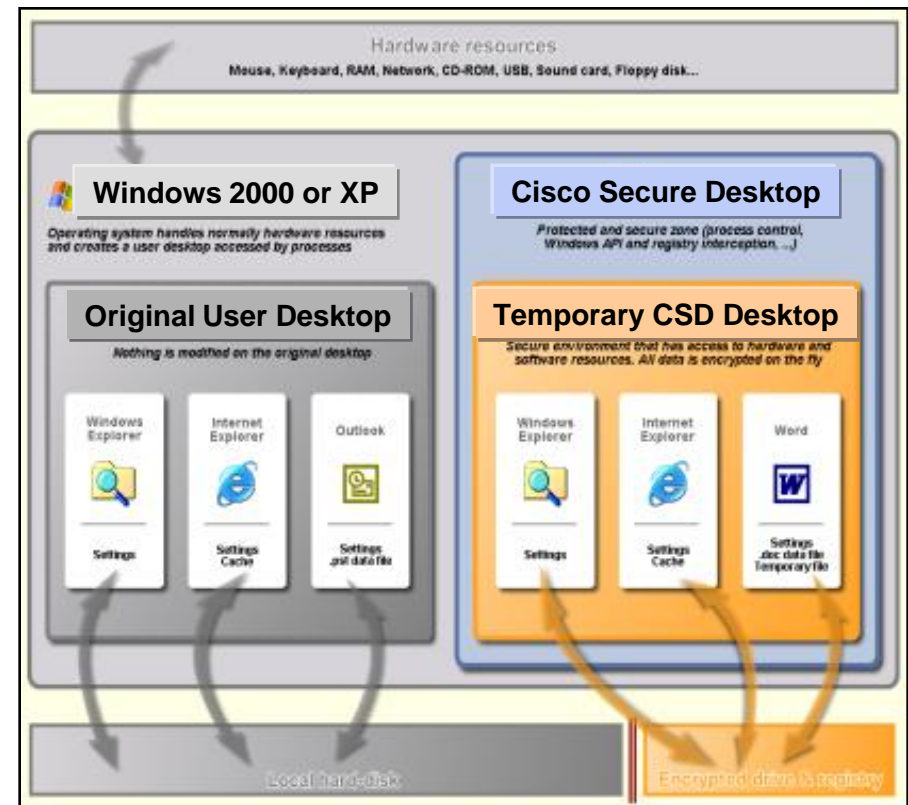
# Cisco Secure Desktop

- End user systems cant always be trusted due to some security risk of
  - Cannot ensure total removal of all data
  - Potentially malicious third party software might be installed.
- CSD with other security controls and mechanism within the context of an effective risk management strategy can help reduce risks
- CSD is part of SSL VPN and a functionality of ASA/IOS SSL VPNs

# Cisco Secure Desktop

## Comprehensive Endpoint Security for SSL VPN

- Works with desktop guest permissions
  - No admin privileges required
- Complete pre-connect assessment:
  - Location assessment—managed or unmanaged desktop?
  - Gathers data for Dynamic Access Policy
  - Specific applications running—defined by admin
- Comprehensive session protection:
  - Malware detection
  - Data sandbox and encryption protects every aspect of session
- Post-session clean-up:
  - Encrypted partition overwrite (not just deletion) using DoD algorithm
  - Cache, history and cookie overwrite
  - File download and email attachment overwrite
  - Auto-complete password overwrite



# Comprehensive EndPoint Security

- Cisco Secure Desktop (CSD) now supports hundreds of pre-defined products, updated frequently



Anti-virus, anti-spyware, personal firewall, and more

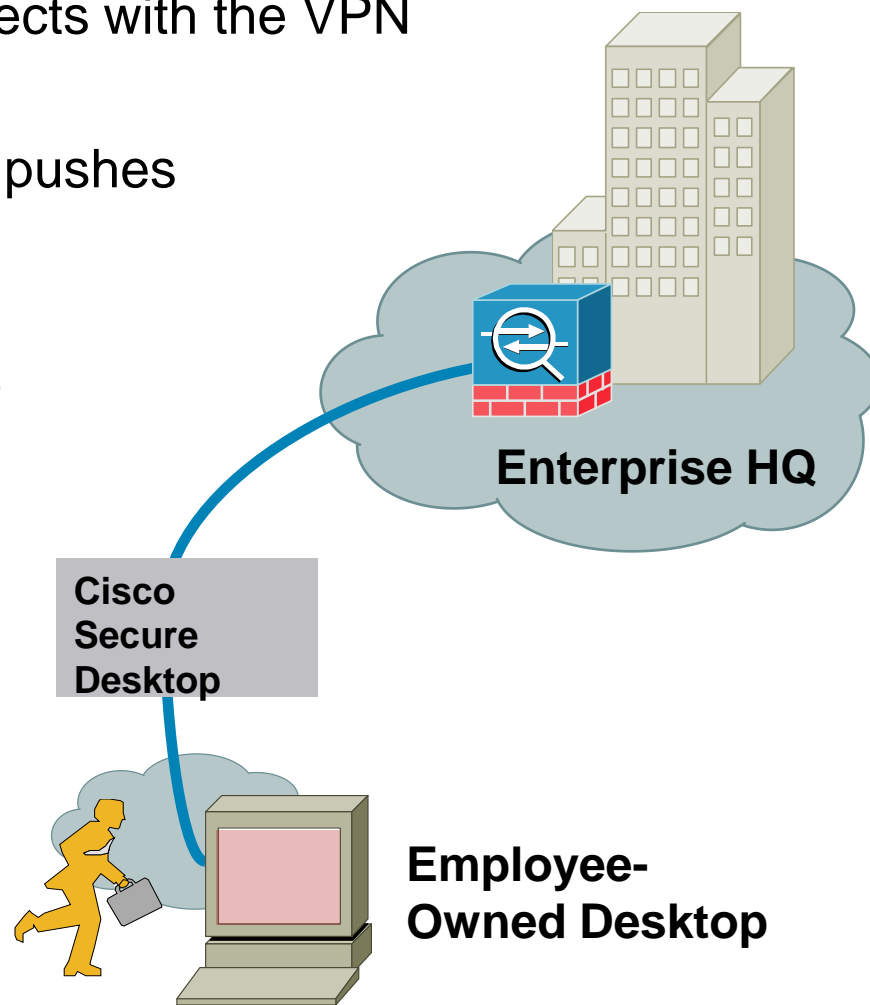
- Administrators can define custom checks including running processes
- CSD posture policy presented visually to simplify configuration and troubleshooting



# Cisco Secure Desktop

## How it Works (Pre-Login)

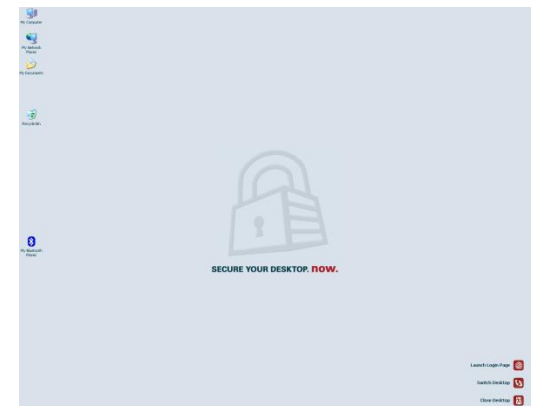
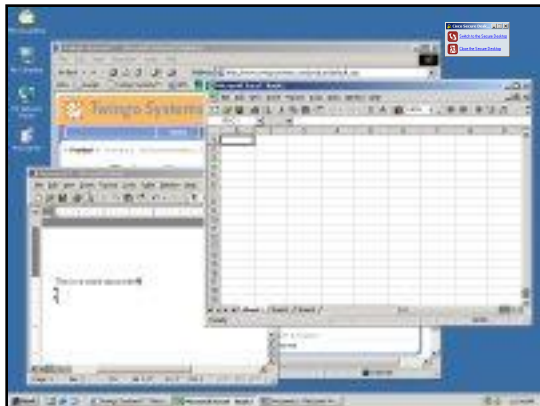
- **Step One:** A remote user connects with the VPN appliance via SSL
- **Step Two:** The VPN appliance pushes down the Secure Desktop
- **Step Three:** Based on checks, determine location (or fail login)
- **Step Four:** Based on location settings apply CSD policies



# Cisco Secure Desktop

## How It Works (Login Phase)

- **Step Five:** Check for keystroke logger and host emulation
- **Step Six:** Create the vault and switch to secure desktop
- **Step Seven:** Present login to user
- **Step Eight:** User logs in and initiates VPN session
- **Step Nine:** Host scan information gathered from endpoint for DAP



# Cisco Secure Desktop

## How It Works (Post Login)

- **Step Ten:** DAP checks applied
- **Step Eleven:** VPN connection active
- **Step Twelve:** User is able to access resources
- **Step Thirteen:** After session complete (or idle timeout expired) VPN is disconnected and Secure Desktop post session cleanup initiated





# Cisco Secure Desktop

## Installation of CSD

- CSD tries different methods to install itself on Windows client computer until it finds a method that works

Installation Method	Remote User Requirement
Active X	Admin Privileges (privi.)
Microsoft Java VM*	Power-User Privi.
Sun Java VM*	Any User
Exe	Any User with Execution Privi.

\* VM = Virtual Machine

# Cisco Secure Desktop

## Installation of CSD on ASA

The screenshot displays the Cisco ASDM 6.2 for ASA interface. The main window title is "Cisco ASDM 6.2 for ASA - 172.18.104.179". The navigation pane on the left shows the "Remote Access VPN" configuration tree, with "Secure Desktop Manager" selected and "Setup" highlighted. The main content area shows the "Secure Desktop Manager" configuration page, which includes a "Location:" field, a "Browse Flash..." button, an "Enable Secure Desktop" checkbox, an "Upload..." button, and an "Uninstall" button. An "Upload Image" dialog box is open in the foreground, containing the following text: "Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish." The dialog box has two input fields: "Local File Path:" with the value "C:\Documents and Settings\omar\Desktop\csd\_3" and a "Browse Local Files..." button; and "Flash File System Path:" with the value "disk0:/csd\_3.4.1108.pkg" and a "Browse Flash..." button. At the bottom of the dialog box are "Upload File", "Close", and "Help" buttons. A red rectangle highlights the input fields and their respective browse buttons.

# Cisco Secure Desktop

## Secure Session (Vault)

- Encrypts the data and files associated with or downloaded during a remote session into a secure partition
- Graphical representation of a desktop that includes an image of a lock to signify a safe environment for the remote user to work in
- After the remote session ends, a U.S. Department of Defense (DoD) sanitation algorithm removes the encrypted partition
- Typically used during clientless SSL VPN sessions, Secure Session attempts to reduce the possibility that cookies, browser history, temporary files, and downloaded content remain after a remote user logs out, the session times out, or after an abrupt termination occurs. This feature is available on Microsoft Windows XP and Windows 2000

# Cisco Secure Desktop

## Cache Cleaner

- Alternative to Secure Session attempts to eliminate information in the browser cache at the end of a session
- Cleans up passwords entered during the session, auto-completed text, files cached by the browser, and browser configuration changes
- Cache Cleaner runs on Microsoft Windows Vista, Windows XP, Windows 2000, Apple Mac OS X 10.4, 10.5 (PowerPC or Intel), and Linux

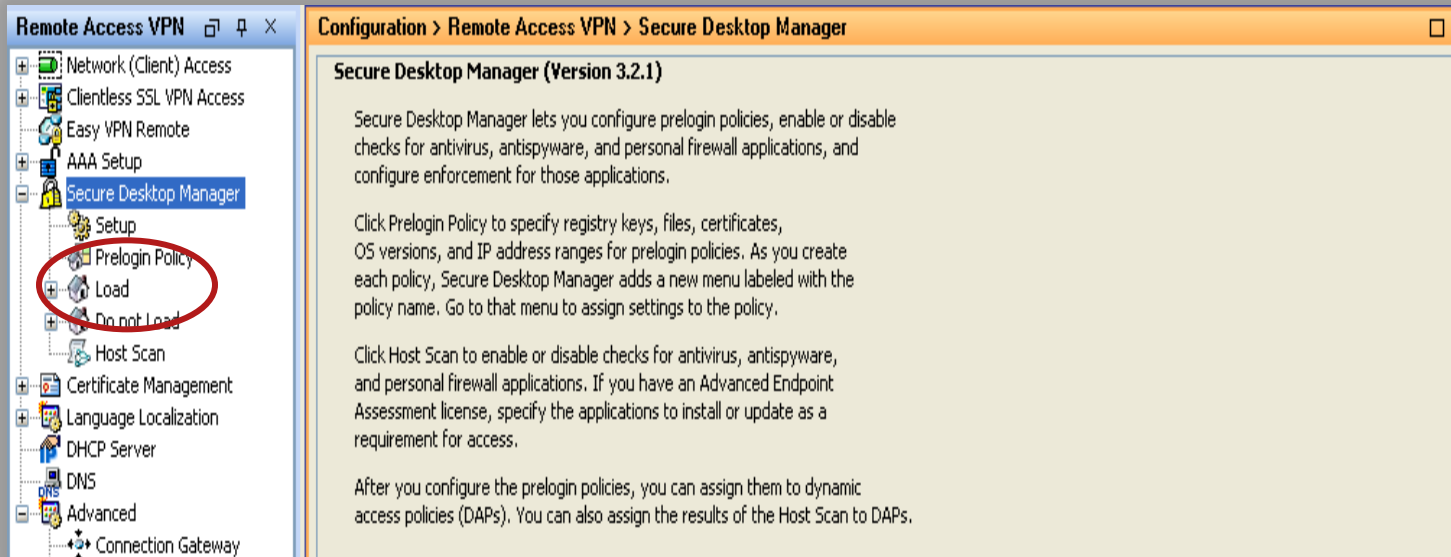
# Cisco Secure Desktop

## Keystroke Logger Detection and Host Emulation Detection

- Denies access based on the presence of a suspected keystroke logging application or a host emulator
- Configure Cisco Secure Desktop Manager to specify the keystroke logging applications that are safe
- Allows the remote user interactively approve the applications and host emulator the scan identifies
- Both keystroke logger detection and host emulation detection are available with Cache Cleaner, Secure Session, and Host Scan

# Cisco Secure Desktop

- After loading CSD, the following options are provided to configure
  - Host scan
  - Pre-login policy
  - Load
  - Do not load policy



# Cisco Secure Desktop

## Pre-Login Policy

- Allows administrator to specify the checks to be performed between the time the user establishes a connection with the security appliance and the time the user enters the login credentials
- These checks determine whether to assign a prelogin policy or whether to display a "Login Denied" message for the remote user
- The settings of the matched prelogin policy determine whether Secure Session or Cache Cleaner loads. The application of a prelogin policy to a dynamic access policy (DAP) determines the access rights and restrictions placed on the connection

# CSD Configuration (Cont.)

The screenshot shows the ASDM (Cisco Systems Desktop Management) configuration interface. The left pane displays a tree view of configuration options, with 'Windows Location Settings' selected under 'Secure Desktop Manager'. The main pane shows the 'Windows Location Settings' configuration page. A diagram illustrates a pre-login decision tree with a 'Start' node pointing to a '+' sign, which then points to a 'Default' node. A red arrow points to the '+' sign. A text box below the diagram reads: 'To Configure the Flow of CSD Checking Start by Clicking on the + Sign. This Will Pull Up a Selection Box.' The interface includes a menu bar (File, View, Tools, Wizards, Window, Help), a toolbar (Home, Configuration, Monitoring, Save, Refresh, Back, Forward, Help), and a status bar at the bottom showing the user 'chcurry', page number '15', and the date/time '1/29/07 9:47:06 AM UTC'.

**ASDM** (Cisco Systems Desktop Management) interface showing configuration for Windows Location Settings.

**Configuration Path:** Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Windows Loc...

**Windows Location Settings**

Below is the pre-login decision tree for the Windows Locations. Additional checks can be inserted by clicking the + symbol at the beginning of a node. Checks can be removed by selecting the node and pressing delete. Leaf nodes can either be set to "Login Denied", a Windows Location, or link to a subsequence.

**Diagram:** Start → (+) → Default

**Text Box:** To Configure the Flow of CSD Checking Start by Clicking on the + Sign. This Will Pull Up a Selection Box.

Close all open browser windows after installation

Apply All    Reset All

chcurry    15    1/29/07 9:47:06 AM UTC



# CSD Configuration (Cont.)

The screenshot shows the ASDM (Cisco Systems Desktop Manager) configuration interface. The left pane displays a tree view of configuration options under 'Remote Access VPN', with 'Windows Location Settings' selected. The main pane shows the 'Windows Location Settings' configuration page. A diagram illustrates a pre-login decision tree starting with 'Start' and leading to a 'Default' node. A red arrow points from a text box to a dialog box titled 'Select the type of check that you would like to insert'. The dialog box contains a 'Check:' dropdown menu with the following options: Registry Check, File Check, Certificate Check, Windows Version Check, and IP Address Check. The 'Registry Check' option is currently selected. The dialog also includes 'Add' and 'Cancel' buttons. The bottom status bar shows the user 'chcurry', the page number '15', and the date/time '1/29/07 9:48:46 AM UTC'.

**ASDM** (Cisco Systems Desktop Manager) - 68.109.228.183

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Windows Loc...

### Windows Location Settings

Below is the pre-login decision tree for the Windows Locations. Additional checks can be inserted by clicking the + symbol at the beginning of a node. Checks can be removed by selecting the node and pressing delete. Leaf nodes can either be set to "Login Denied", a Windows Location, or link to a subsequence.

Start → + Default

**These Are the Types of Checks CSD will Check for.**

Select the type of check that you would like to insert

Check: Registry Check (selected)  
File Check  
Certificate Check  
Windows Version Check  
IP Address Check

Buttons: Add, Cancel, Reset All

Footer: chcurry | 15 | 1/29/07 9:48:46 AM UTC

# Cisco Secure Desktop— ASDM Configuration (Cont.)

The screenshot shows the ASDM configuration interface for a Cisco device. The left pane displays a tree view of configuration options, with 'Windows Location Settings' selected under 'Secure Desktop Manager'. The main pane shows the 'Windows Location Settings' configuration page. A flowchart illustrates the pre-login decision tree: 'Start' leads to a 'File Check?' node. If successful, it leads to 'Default'; if failed, it leads to 'Login Denied'. Below the flowchart is a configuration dialog for the 'File Check?' node, showing 'File Path: C:\test.txt', 'Exists' selected, and buttons for 'Update', 'Delete', and 'Cancel'. A blue callout box on the right contains the text: 'By Selecting File Check You Will Get a Selection Box Like Below. Add the File Path, Version of File, and or Checksum Value of the File.'

**ASDM** (release) - 68.109.228.183

File View Tools Wizards Window Help Look For: Find

Home Configuration Monitoring Save Refresh Back Forward Help

Device List

Remote Access VPN

- Network (Client) Access
  - IPSec Connections
  - SSL VPN Connections
  - Group Policies
  - Dynamic Access Policies
  - Address Assignment
  - Advanced
- Clientless SSL VPN Access
  - Connections
  - Portal
  - Group Policies
  - Dynamic Access Policies
  - Advanced
- Secure Desktop Manager
  - CSD Setup
  - Windows Location Settings**
  - Default
  - Mac and Linux Cache Cleaner
  - Host Scan
- Encoding
- Proxy Bypass

Device Setup Firewall Remote Access VPN Site-to-Site VPN Trend Micro Content Security Device Management

**Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Windows Loc...**

### Windows Location Settings

Below is the pre-login decision tree for the Windows Locations. Additional checks can be inserted by clicking the + symbol at the beginning of a node. Checks can be removed by selecting the node and pressing delete. Leaf nodes can either be set to "Login Denied", a Windows Location, or link to a subsequence.

```
graph LR; Start([Start]) -- "+" --> FileCheck[File Check?]; FileCheck -- Success --> Default[Default]; FileCheck -- Failure --> LoginDenied[Login Denied];
```

File Path: C:\test.txt

Exists  Does Not Exist

Version

Checksum (in hex)

Close all open browser windows after installation

chcurry 15 1/29/07 9:50:16 AM UTC

# CSD Configuration (Cont.)

ASDM

Release) - 68.109.228.183

The screenshot shows the ASDM configuration interface for a Cisco device. The left pane displays the configuration tree under 'Remote Access VPN' > 'Clientless SSL VPN Access' > 'Advanced' > 'Secure Desktop Manager' > 'Windows Location Settings'. The main pane shows the 'Windows Location Settings' configuration page. Below the introductory text is a decision tree diagram:

```
graph LR; Start([Start]) --> FileCheck{File Check?}; FileCheck -- Success --> RegistryCheck{Registry Check?}; FileCheck -- Failure --> LoginDenied1[Login Denied]; RegistryCheck -- Success --> Default[Default]; RegistryCheck -- Failure --> LoginDenied2[Login Denied];
```

The 'Registry Check?' dialog box is open, showing the following configuration:

- Key Path: HKEY\_LOCAL\_MACHINE \ SYSTEM\CSD
- Exists
- Does Not Exist
- DWORD value
- String
- Case Sensitive

Buttons: Update, Delete, Cancel

At the bottom of the main pane, there is a checkbox:  Close all open browser windows after installation

Buttons: Apply All, Reset All

A blue callout box on the right contains the text: **Create a Registry Check for a Unique Value.**

Device configuration loaded successfully.

chcurry | 15 | 2/5/07 9:51:07 AM UTC

# CSD Configuration (Cont.)

The screenshot shows the ASDM (Cisco Systems Desktop Manager) interface. The main window displays the configuration path: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Windows Location Settings**. The left sidebar shows a tree view of the configuration, with **Windows Location Settings** selected. The main content area shows the **Windows Location Settings** configuration page. It includes a pre-login decision tree diagram and a configuration dialog box.

**Windows Location Settings**

Below is the pre-login decision tree for the Windows Locations. Additional checks can be inserted by clicking the + symbol at the beginning of a node. Checks can be removed by selecting the node and pressing delete. Leaf nodes can either be set to "Login Denied", a Windows Location, or link to a subsequence.

```
graph LR; Start([Start]) -- "+" --> FileCheck[File Check?]; FileCheck -- Success --> RegistryCheck[Registry Check?]; FileCheck -- Failure --> EngSub[subsequence: Engineering]; RegistryCheck -- Success --> Default[Default]; RegistryCheck -- Failure --> EngSub; EngSub --> Eng([Engineering]); Eng -- "+" --> EngLD[Login Denied];
```

The configuration dialog box shows the following options:

- Login Denied
- Location
- Subsequence

Label:

Buttons: Update, Cancel

Close all open browser windows after installation

Buttons: Apply All, Reset All

**Create a Subsequence if Different Requirements Are Needed for Multiple Groups/Departments.**

# CSD Configuration (Cont.)

**ASDM** (release) - 68.109.228.183

File View Tools Wizards Window Help Look For: Find

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

- Network (Client) Access
- Clientless SSL VPN Access
  - Connections
  - Portal
  - Group Policies
  - Dynamic Access Policies
  - Advanced
    - Secure Desktop Manager
      - CSD Setup
      - Windows Location Settings**
      - Default
      - Mac and Linux Cache Cleaner
      - Host Scan
    - Encoding
    - Proxy Bypass
    - Proxies
    - Java Code Signer
    - Content Cache
    - Content Rewrite
    - Application Helper

Device Setup Firewall Remote Access VPN Site-to-Site VPN Trend Micro Content Security Device Management

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Windows Loca...

### Windows Location Settings

Below is the pre-login decision tree for the Windows Locations. Additional checks can be inserted by clicking the + symbol at the beginning of a node. Checks can be removed by selecting the node and pressing delete. Leaf nodes can either be set to "Login Denied", a Windows Location, or link to a subsequence.

```
graph LR; Start([Start]) -- "+" --> FileCheck{File Check?}; FileCheck -- Success --> RegistryCheck1{Registry Check?}; FileCheck -- Failure --> EngSub[subsequence: Engineering]; RegistryCheck1 -- Success --> Default[Default]; RegistryCheck1 -- Failure --> LoginDenied1[Login Denied]; EngSub -- "+" --> RegistryCheck2{Registry Check?}; RegistryCheck2 -- Success --> LoginDenied2[Login Denied]; RegistryCheck2 -- Failure --> LoginDenied3[Login Denied];
```

**Make Sure the Default Success Value of a Subsequence Is Changed to Reflect the Correct Value. If not the Login Will Fail.**

Close all open browser windows after installation

Apply All Reset All

Device configuration loaded successfully.

chcurry 15 2/5/07 9:53:47 AM UTC

# CSD Configuration (Cont.)

The screenshot shows the ASDM (Cisco Systems Desktop Management) interface. The left pane displays a tree view of configuration options under 'Remote Access VPN' > 'Clientless SSL VPN Access' > 'Advanced' > 'Secure Desktop Manager' > 'Windows Location Settings'. A red arrow points from this menu item to the main configuration area. The main area shows the 'Windows Location Settings' configuration page. It includes a pre-login decision tree diagram and a text box with instructions. The decision tree starts with a 'Start' node leading to a 'File Check?' node. If successful, it leads to a 'Registry Check?' node, which then branches to 'Default' (Success) or 'Login Denied' (Failure). If the 'File Check?' fails, it leads to a 'subsequence: Engineering' node. The 'Engineering' node leads to another 'Registry Check?' node, which branches to 'Engineering' (Success) or 'Login Denied' (Failure). At the bottom, there are 'Apply All' and 'Reset All' buttons, and a checkbox for 'Close all open browser windows after installation'. The status bar at the bottom indicates 'Device configuration loaded successfully.' and shows the user 'chcurry' at '15' on '2/5/07 10:37:57 AM UTC'.

**ASDM** (68.109.228.183)

File View Tools Wizards Window Help Look For: Find

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

- Network (Client) Access
- Clientless SSL VPN Access
  - Connections
  - Portal
  - Group Policies
  - Dynamic Access Policies
  - Advanced
    - Secure Desktop Manager
      - CSD Setup
      - Windows Location Settings
      - Default
      - Engineering
      - Mac and Linux Cache Cleaner
      - Host Scan
    - Encoding
    - Proxy Bypass
    - Proxies
    - Java Code Signer
    - Content Cache
    - Content Rewrite

Device Setup Firewall Remote Access VPN Site-to-Site VPN Trend Micro Content Security Device Management

**Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Windows Loca...**

### Windows Location Settings

Below is the pre-login decision tree for the Windows Locations. Additional checks can be inserted by clicking the + symbol at the beginning of a node. Checks can be removed by selecting the node and pressing delete. Leaf nodes can either be set to "Login Denied", a Windows Location, or link to a subsequence.

```
graph LR; Start([Start]) --> FileCheck{File Check?}; FileCheck -- Success --> RegCheck1{Registry Check?}; FileCheck -- Failure --> EngSubseq[subsequence: Engineering]; RegCheck1 -- Success --> Default[Default]; RegCheck1 -- Failure --> LoginDenied1[Login Denied]; EngSubseq --> RegCheck2{Registry Check?}; RegCheck2 -- Success --> Eng[Engineering]; RegCheck2 -- Failure --> LoginDenied2[Login Denied];
```

**Notice that When the Value Is Changed to a Location the Value Is Added to Location Settings. Make Sure the Location Settings Are Configured.**

Close all open browser windows after installation

Apply All Reset All

Device configuration loaded successfully. | chcurry | 15 | 2/5/07 10:37:57 AM UTC

# CSD Configuration (Cont.)

The screenshot displays the ASDM (Cisco Systems Desktop Management) configuration interface. The main window title is "ASDM" and the address bar shows "release) - 68.109.228.183". The interface includes a menu bar (File, View, Tools, Wizards, Window, Help) and a toolbar with navigation buttons (Home, Configuration, Monitoring, Save, Refresh, Back, Forward, Help). The left sidebar shows a "Device List" with a tree view of configuration options. The main content area is titled "Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Default". Under "Location Settings", the "Location Module" is set to "Secure Desktop" (checked) or "Cache Cleaner" (unchecked). The "Apply All" and "Reset All" buttons are visible at the bottom of the configuration area. The status bar at the bottom shows the user "chcurry", page number "15", and the date/time "1/29/07 10:41:07 AM UTC".

# CSD Configuration (Cont.)

The screenshot shows the ASDM (Cisco Systems Desktop Security Manager) interface. The main window title is "Remote Access VPN - 68.109.228.183". The breadcrumb navigation path is "Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Default > Keys...".

The left sidebar shows a tree view of the configuration hierarchy. The "Keystroke Logger & Safety Checks" option is selected under the "Default" configuration.

The main content area is titled "Keystroke Logger & Safety Checks" and contains the following configuration options:

- Check for keystroke loggers
- Force admin control on list of safe modules
- List of Safe Modules: (Empty list box with "Add", "Edit", and "Delete" buttons)
- Check for host emulation
- Always deny access if running within emulation

At the bottom of the configuration area are "Apply All" and "Reset All" buttons. The status bar at the bottom shows the user "chcurry", page number "15", and a timestamp "1/29/07 10:42:07 AM UTC".



# CSD Configuration (Cont.)

The screenshot displays the ASDM (Cisco Systems Desktop Manager) interface. The top-left corner features the ASDM logo. The main window title is "Cisco Systems Desktop Manager (Release) - 68.109.228.183". The menu bar includes File, View, Tools, Wizards, Window, and Help. The navigation pane on the left shows a tree structure under "Remote Access VPN" with "Cache Cleaner" highlighted in a red box. The main content area shows the "Cache Cleaner" configuration page with the following settings:

- Launch hidden URL after installation  
Hidden URL:
- Show success message at the end of successful installation
- Launch cleanup upon timeout based on inactivity  
Timeout After: 5 minute(s)
- Launch cleanup upon closing of all browser instances or SSL VPN connection
- Disable Cancel button when cleaning
- Clean the whole cache in addition to the current session cache (IE only)
- Secure Delete: 3 pass(es)

At the bottom of the configuration area are "Apply All" and "Reset All" buttons. The bottom status bar shows the user "chcurry", the page number "15", and the timestamp "1/29/07 10:43:07 AM UTC".

# CSD Configuration (Cont.)

The screenshot shows the ASDM (Cisco Secure Desktop Manager) configuration interface. The left pane displays a tree view of configuration options under 'Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Default > Secure Desktop General'. The 'Secure Desktop General' option is highlighted with a red box. The right pane shows the configuration details for 'Secure Desktop General'.

**ASDM** (Address) - 68.109.228.183

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Default > Secure Desktop General

**Secure Desktop General**

- Automatically switch to Secure Desktop after installation
- Enable switching between Secure Desktop and Local Desktop
- Enable Vault Reuse (User chooses a password)
- Suggest application uninstall upon Secure Desktop closing
- Force application uninstall upon Secure Desktop closing
- Enable Secure Desktop inactivity timeout
  - Timeout After: 5 minute(s)
- Open following web page after Secure Desktop closes
  - URL:
- Secure Delete: 3 pass(es)
- Launch the following application after installation:
  - Program Files\

Apply All    Reset All

chcurry    15    1/29/07 10:44:57 AM UTC

# CSD Configuration (Cont.)

The screenshot shows the ASDM (Cisco Systems Desktop Manager) interface. The top-left corner features a red 'ASDM' logo. The main window title is 'Cisco Systems Desktop Manager (Release) - 68.109.228.183'. The navigation pane on the left shows a tree structure under 'Remote Access VPN' with 'Secure Desktop Settings' highlighted by a red box. The main content area displays the 'Secure Desktop Settings' configuration page, which includes several unchecked checkboxes:

- Restrict application usage to the web browser only
- Disable access to network drives and network folders
  - Do not encrypt files on network drives
- Disable access to removable drives and removable folders
  - Do not encrypt files on removable drives
- Disable registry modification
- Disable command prompt access
- Disable printing
- Allow email applications to work transparently

At the bottom of the configuration area are 'Apply All' and 'Reset All' buttons. The bottom status bar shows the user 'chcurry', page number '15', and a timestamp '1/29/07 10:45:47 AM UTC'.

# CSD Configuration (Cont.)

The screenshot shows the ASDM (Cisco Systems Desktop Management) interface. The top-left corner features a red 'ASDM' label. The browser address bar shows '... (release) - 68.109.228.183'. The main navigation bar includes 'Home', 'Configuration', 'Monitoring', 'Save', 'Refresh', 'Back', 'Forward', and 'Help'. The left sidebar contains a 'Device List' and a tree view of configuration options. The right pane displays the 'Secure Desktop Browser' configuration page, which includes a 'Home Page' field set to 'about:blank', a 'Customize Bookmarks' section with a 'Favorites' folder, and buttons for 'Add Bookmark', 'Add Folder', 'Edit', and 'Delete'. At the bottom of the configuration pane are 'Apply All' and 'Reset All' buttons. The bottom status bar shows the user 'chcurry', page number '15', and the date/time '1/29/07 10:46:27 AM UTC'.

**ASDM** (release) - 68.109.228.183

File View Tools Wizards Window Help Look For: Find

Home Configuration Monitoring Save Refresh Back Forward Help

Device List

**Remote Access VPN**

- Group Policies
- Dynamic Access Policies
- Advanced
  - Secure Desktop Manager
    - CSD Setup
    - Windows Location Settings
    - Default
      - Keystroke Logger & Safety
      - Cache Cleaner
      - Secure Desktop General
      - Secure Desktop Settings
      - Secure Desktop Browser**
      - Mac and Linux Cache Cleaner
    - Host Scan
  - Encoding
  - Proxy Bypass
  - Proxies
  - Java Code Signer
  - Content Cache
  - Content Rewrite

Device Setup Firewall Remote Access VPN Site-to-Site VPN Trend Micro Content Security Device Management

**Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Default > Secu...**

**Secure Desktop Browser**

Home Page:

Customize Bookmarks:

Favorites

Add Bookmark Add Folder Edit Delete

Apply All Reset All

chcurry 15 1/29/07 10:46:27 AM UTC

# CSD Configuration (Cont.)

The screenshot shows the ASDM (Cisco Systems Desktop Security Manager) interface. The top navigation bar includes 'File', 'View', 'Tools', 'Wizards', 'Window', and 'Help'. The main content area is titled 'Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Mac and Linux...'. The left sidebar shows a tree view of configuration options, with 'Mac and Linux Cache Cleaner' highlighted in a red box. The main configuration area for 'Mac and Linux Cache Cleaner' includes the following settings:

- Launch cleanup upon global timeout
- Timeout After: 1 minute(s)
- Let user reset timeout
- Launch cleanup upon exiting of browser
- Enable cancellation of cleaning
- Secure Delete: 3 pass(es)

At the bottom of the configuration area, there are 'Apply All' and 'Reset All' buttons. The bottom status bar shows the user 'chcurry', page number '15', and the date/time '1/29/07 10:47:17 AM UTC'.

# CSD Configuration (Cont.)

The screenshot shows the ASDM configuration interface for a Cisco device. The left pane shows the configuration tree with 'Host Scan' selected under 'Advanced' > 'Secure Desktop Manager'. The main pane shows the 'Host Scan' configuration page. A table lists three types of configurable options: Registry, File, and Process. Below the table, there are sections for 'Host Scan Extensions' with two checked options: 'Advanced Endpoint Assessment ver 2.3.1.1' and 'Endpoint Assessment ver 2.3.1.1'. Two callout boxes provide additional information: one highlights the three types of configurable options, and another states that Endpoint Assessment gives the ability to check/enforce AV, AS, and Firewall software for CSD, and that the Advanced Endpoint Assessment option will be a licensed feature for release.

**ASDM** (release) - 68.109.228.183

File View Tools Wizards Window Help Look For: Find

Home Configuration Monitoring Save Refresh Back Forward Help

Device List

Remote Access VPN

- Network (Client) Access
- Clientless SSL VPN Access
  - Connections
  - Portal
  - Group Policies
  - Dynamic Access Policies
  - Advanced
    - Secure Desktop Manager
      - CSD Setup
      - Windows Location Settings
      - Default
      - Mac and Linux Cache Cleaner
      - Host Scan
    - Encoding
    - Proxy Bypass
    - Proxies
    - Java Code Signer
    - Content Cache
    - Content Rewrite
    - Application Helper

Device Setup Firewall Remote Access VPN Site-to-Site VPN Trend Micro Content Security Device Management

**Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Host Scan**

### Host Scan

Create entries to be scanned on the endpoint system. The scanned information will then be stored in the endpoint attribute. Access policies using the endpoint information can be configured under [Dynamic Access Policies](#).

Basic Host Scan

Type	ID	Info
Registry	Test1	HKEY_LOCAL_MACHINE\SY...
File	Test2	c:\test.txt
Process	Test3	test.exe

Add Edit... Delete

**The Configurations Above Are the Three Types of Configurable Options—Registry, File, and Process**

Host Scan Extensions

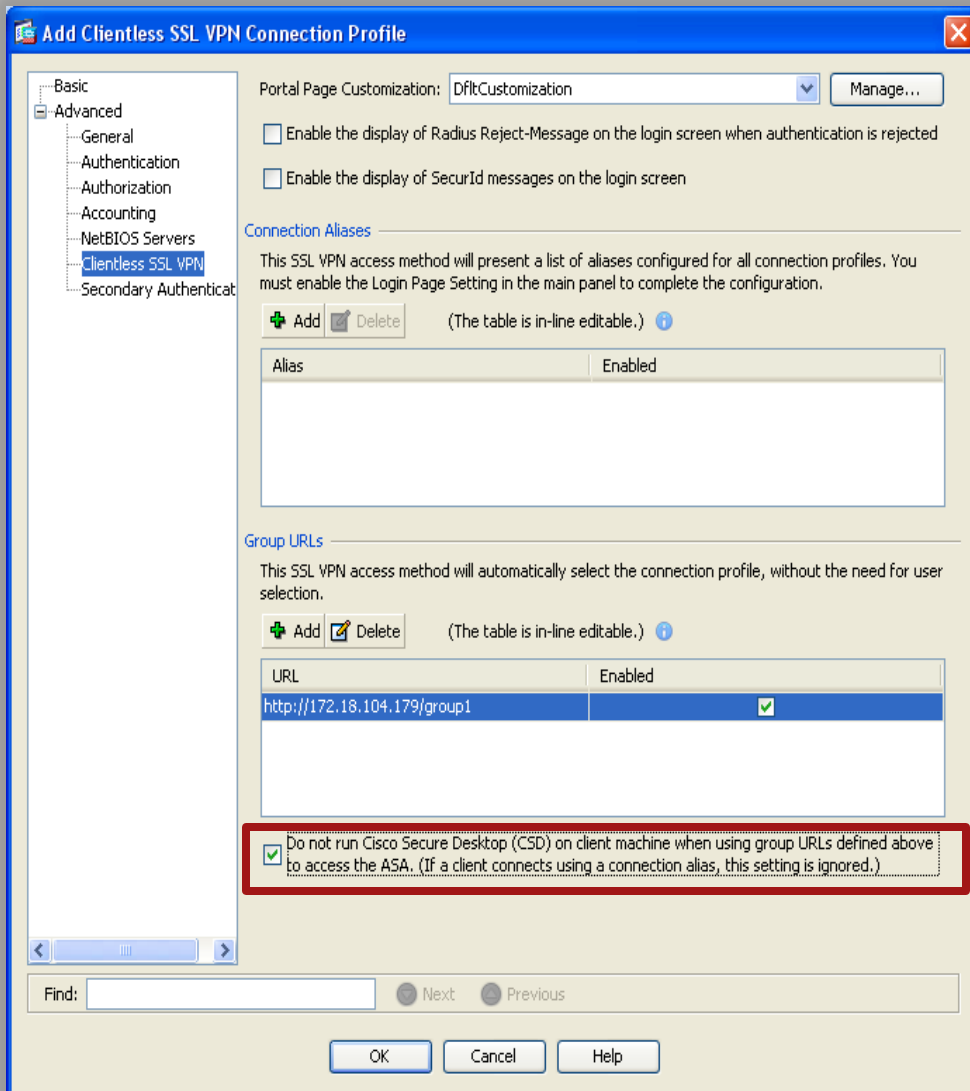
- Advanced Endpoint Assessment ver 2.3.1.1
- Endpoint Assessment ver 2.3.1.1

Configure...

Apply All Reset All

Device configuration loaded successfully. chcurry 15 1/30/07 2:04:38 PM UTC

# Disabling CSD per Connection Profile



Allows you to exempt certain users from running CSD on a per connection profile basis.

In ASDM, go to  
**Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles > Add or Edit > Advanced, Clientless SSL VPN Configuration**

or  
**Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add or Edit > Advanced > SSL VPN.**

## CLI Commands:

```
tunnel-group TunnelGroup1 webvpn-attributes
without-csd
```

# Debugging CSD

**DEBUG = debug dap trace**

```
ASA(config)# debug dap trace
```

```
The DAP policy contains the following attributes:
```

```
-----  
1: action = continue  
DAP_open: C9EEE930  
DAP_add_CSD: csd_token = [4287F77A4F7347A553F4619C]  
[ 0]: aaa.cisco.username = user2  
[ 1]: aaa.cisco.tunnelgroup = DefaultWEBVPNGroup  
dap_add_to_lua_tree:aaa["cisco"]["username"] = "user2";  
dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "DefaultWEBVPNGroup";  
dap_clienttype_to_string(3) returns CLIENTLESS  
dap_add_to_lua_tree:endpoint["application"]["clienttype"] = "CLIENTLESS";  
dap_add_csd_data_to_lua:  
endpoint.os.version = "Windows XP";  
endpoint.os.servicepack = "2";  
endpoint.location = "Default";  
endpoint.protection = "secure desktop";  
endpoint.fw["MSWindowsFW"] = {};  
endpoint.fw["MSWindowsFW"].exists = "true";
```



# Debugging CSD (Cont.)

## Continuation of debug dap trace

```
endpoint.fw["MSWindowsFW"].description = "Microsoft Windows Firewall";
endpoint.fw["MSWindowsFW"].enabled = "true";
endpoint.av["McAfeeAV"] = {};
endpoint.av["McAfeeAV"].exists = "true";
endpoint.av["McAfeeAV"].description = "McAfee VirusScan Enterprise";
endpoint.av["McAfeeAV"].version = "7.0.0";
endpoint.av["McAfeeAV"].activescan = "true";
endpoint.av["McAfeeAV"].lastupdate = "132895";
endpoint.as["SpyBot"] = {};
endpoint.as["SpyBot"].exists = "true";
endpoint.as["SpyBot"].description = "Spybot - Search & Destroy 1.4";
endpoint.as["SpyBot"].version = "1.4";
endpoint.as["SpyBot"].activescan = "false";
endpoint.as["SpyBot"].lastupdate = "996895";
endpoint.enforce = "success";
Selected DAPs: McAfee-7,SpyBot
dap_request: memory usage = 19%
dap_process_selected_daps: selected 3 records
dap_aggregate_attr: rec_count = 3
DAP_close: C9EEE930
```

# Dynamic Access Policy (DAP)

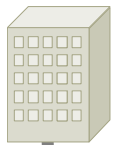
# Policy Control for all users



**Client-based SSL or IPsec VPN**

**Mobile Workers**

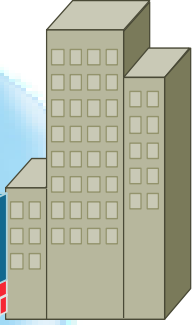
Easy access to corporate network resources



**Partners / Consultants**

Controlled access to specific resources and applications

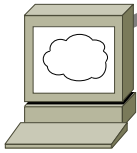
**Clientless SSL VPN**



Public Internet

**ASA 5500**

**Clientless SSL VPN**



**Roamers**

Seamless access to applications from unmanaged endpoints

**Client-based SSL or IPsec VPN**



**Day Extenders / Home Office**

Day extenders and mobile employees require consistent LAN-like, full-network access, to corporate resources and applications

# Dynamic Access Policy

Why to use DAP?

- VPN gateways operate in dynamic environments
- Many variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from remote access sites with different configurations and levels of security
- Authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration

# Dynamic Access Policy

## How DAP Works?

- DAP on the security appliance configures authorization that addresses these many variables
- Create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session
- These attributes address issues of multiple group membership and endpoint security
- Security appliance grants access to a particular user for a particular session based on the policies you define

# Dynamic Access Policy

## How DAP Works?

- CSD gives information of the end user machine to the ASA (Adaptive Security Appliance) for evaluation
- ASA selects these DAP records based on the endpoint security information of the remote device and the AAA authorization information for the authenticated user
- It then applies the DAP record to the user session

# Dynamic Access Policy

Support for Remote Access Connection

- Clientless SSL VPN
- Anyconnect Client
- PIX cut-through proxy (posture assessment not available)

# Dynamic Access Policy

## Components of DAP—DAP Selection

### Configuration File

- A text file containing criteria that the security appliance uses for selecting and applying DAP records during session establishment
- Stored on the security appliance. Configurable only through ASDM which applies an XML data format to the ASA
- DAP selection configuration files include all of the attributes that you configure. These can include AAA attributes, endpoint attributes, and access policies as configured in network and web-type ACL filter, port forwarding and URL lists



# Dynamic Access Policy

## Components of DAP—DfltAccessPolicy

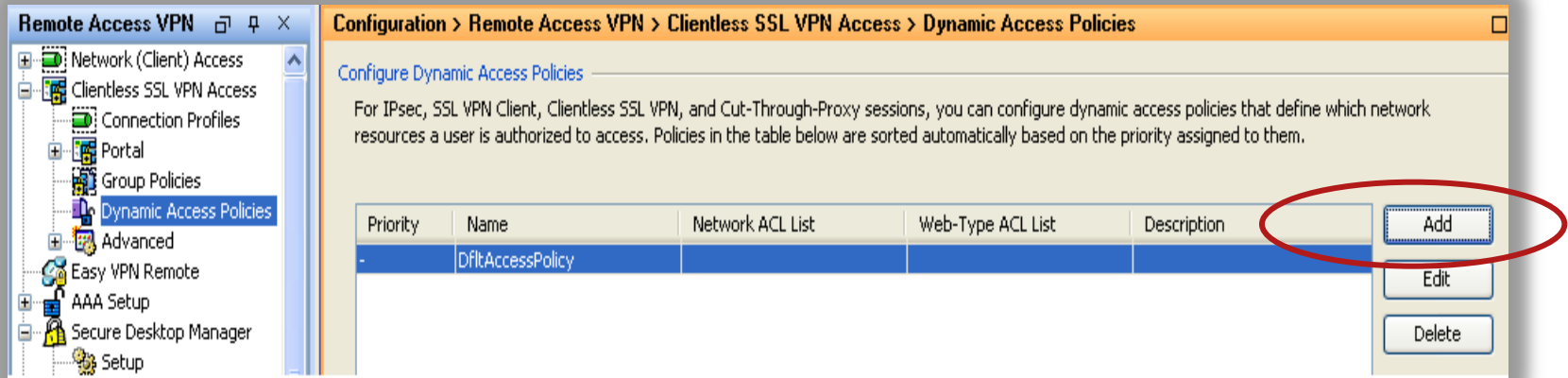
- Always the last entry in the DAP summary table, always with a priority of 0
- Configure Access Policy attributes for the default access policy, but it does not contain—and you cannot configure—AAA or endpoint attributes
- DfltAccessPolicy can not be deleted and it must be the last entry in the summary table

# Dynamic Access Policy

## DAP Configuration on ASDM

- Default action for Default Access Policy is “Continue”
- Add policy with assessments and change Default Policy to include actions for non-complaint end systems or “Terminate”

### ASDM



The screenshot shows the ASDM interface for configuring Dynamic Access Policies. The left pane shows the navigation tree with 'Dynamic Access Policies' selected. The main pane displays the 'Configure Dynamic Access Policies' page, which includes a table of existing policies and three action buttons: 'Add', 'Edit', and 'Delete'. The 'Add' button is circled in red.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies

Configure Dynamic Access Policies

For IPsec, SSL VPN Client, Clientless SSL VPN, and Cut-Through-Proxy sessions, you can configure dynamic access policies that define which network resources a user is authorized to access. Policies in the table below are sorted automatically based on the priority assigned to them.

Priority	Name	Network ACL List	Web-Type ACL List	Description	
-	DfltAccessPolicy				<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

# Dynamic Access Policy

## DAP Configuration on ASDM

ASDM

Policy Name: Networkers2008

Description: Policy applied to all Networkers Attendees

Priority: 90

**Selection Criteria**

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values... (Selected)

User has ALL of the following AAA Attributes values...

User has NONE of the following AAA Attributes values...

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
-------------	----------------------

Buttons: Add, Edit, Delete, Logical Op.

**Advanced**

**Access Policy Attributes**

Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.

Action:  Continue  Terminate

Specify the message that will be displayed when this record is selected.

User Message:

Buttons: OK, Cancel, Help

# Dynamic Access Policy

## DAP Configuration on ASDM

- AAA selection attribute names that are available for DAP use
- The Attribute Name field shows you how to enter each attribute name in a LUA logical expression, which you might do in the Advanced section of the Add/Edit Dynamic Access Policy pane

### ASDM

The screenshot displays the 'Add Dynamic Access Policy' configuration window in ASDM. The main window has the following fields:

- Policy Name: Networkers2008
- Description: Policy for Networkers Attendees
- Priority: 90

The 'Selection Criteria' section includes a dropdown menu set to 'User has ALL of the following AAA Attributes values...' and a table for defining criteria. The 'Advanced' section is currently collapsed.

The 'Access Policy Attributes' section includes tabs for 'Action', 'Network ACL Filters', and 'Web-Type ACL F'. The 'Action' tab is active, showing 'Continue' selected and a 'User Message' field.

The 'Add AAA Attribute' dialog box is open, showing the 'AAA Attribute Type' dropdown menu with 'Cisco' selected. The dialog also includes checkboxes for 'Class', 'IP Address', 'Member-of', 'Tunnel Group', and 'Username', and buttons for 'OK', 'Cancel', and 'Help'.

# Dynamic Access Policy

## DAP—AAA Configuration Attribute Names

Attribute Type	Attribute Name	Source	Value	Max String Length	Description
Cisco	aaa.cisco.memberof	AAA	String	128	Memberof value
	aaa.cisco.username	AAA	String	64	Username value
	aaa.cisco.class	AAA	String	64	Class attribute value
	aaa.cisco.ipaddress	AAA	Number	-	Framed-ip address value
	aaa.cisco.tunnelgroup	AAA	String	64	Tunnel-group name
LDAP	aaa.ldap.<label>	LDAP	String	128	LDAP attribute value pair
RADIUS	aaa.radius.<number>	RADIUS	String	128	Radius attribute value pair

# Dynamic Access Policy

## DAP—Endpoint Assessment

- The security appliance obtains endpoint security attributes by using posture assessment methods. These include Cisco Secure Desktop and NAC
- Endpoint Attribute types such as Anti-spyware, Antivirus, Policy, File, Registry are configured with values for assessment
- Logical Expression can be added along with Endpoint assessments

Endpoint Attribute Type: Anti-Virus

Vendor:

Product Description:

Version:

Please replace character 'x' in Version field with the specific value you want.

Last Update: < days

OK Cancel Help

Endpoint Attribute Type: Anti-Virus

Exists  Does not exist

Vendor: AEC, spol. s r.o.

Product Description:

Version:

Last Update: days

OK Cancel Help

# Dynamic Access Policy

## DAP—Access Policy Attribute Assignment

- After the End point assessment the action to assign the user with the attribute is set
- Assignment of Network ACL filters, Webtype-ACL filters, Functions, Access method, Port Forwarding Lists and URL Lists is done on the access policy attribute section

### ASDM

Access Policy Attributes

Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.

Action Network ACL Filters Web-Type ACL Filters Functions Port Forwarding Lists URL Lists Access Method

Access Method:  Unchanged

AnyConnect Client

Web-Portal

Both-default-Web-Portal

Both-default-AnyConnect Client

# DAP Posture Assessment

## Capability by Connection Protocol

Client Access Method	Host Scan	Vault	NAC Appliance
Cisco VPN Client	No	N/A	Yes
Cisco AnyConnect VPN Client	Yes	Yes	Yes
Clientless SSL	Yes	Yes	No



# SSL VPN Case Study

# SSL VPN – Case Study

## Goal 1:

- **Full time employees** using a **corporate PC** should be allowed to access all internal and DMZ resources through Anyconnect client.

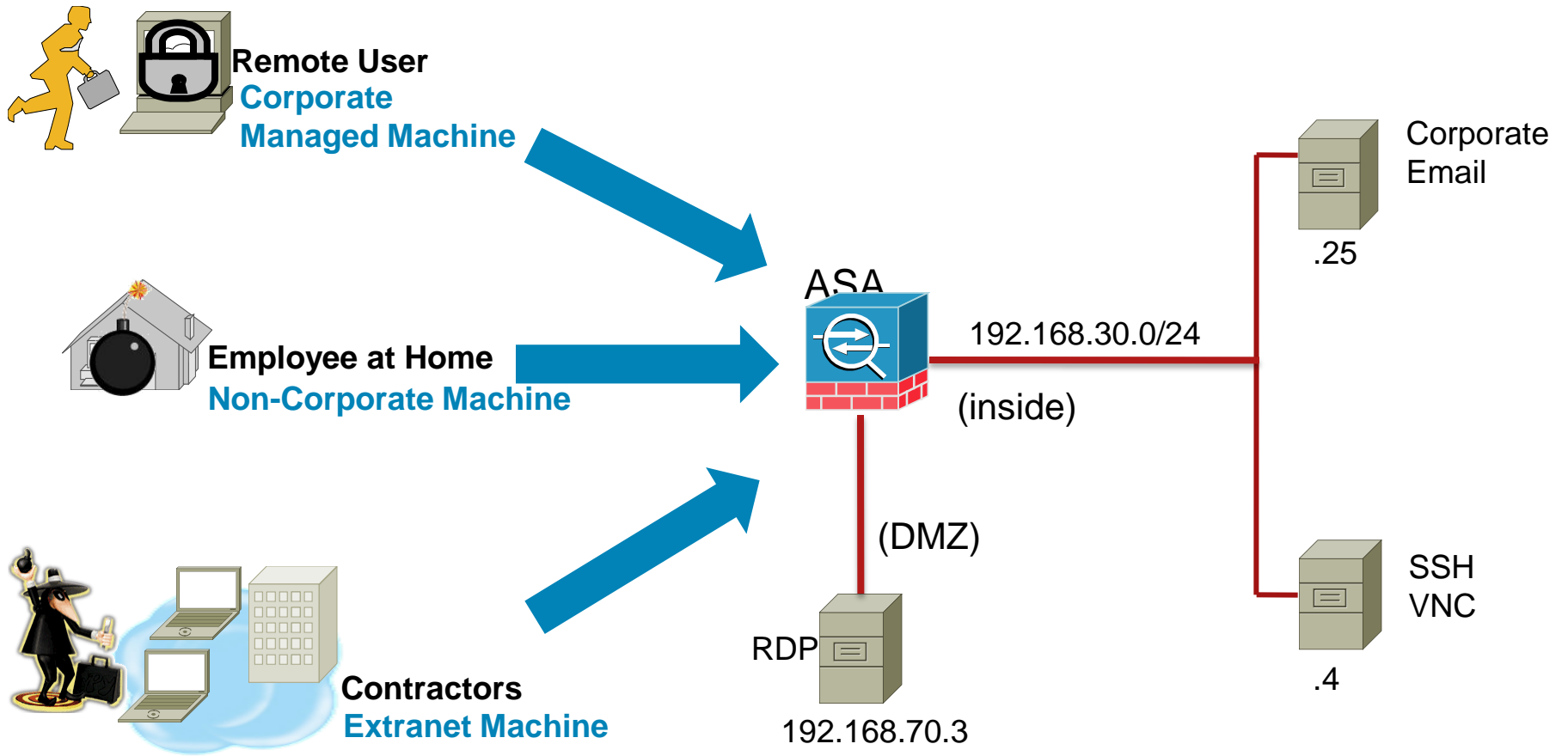
## Goal 2:

- **Full time employees NOT** using a **corporate PC** should be allowed to only access email and main intranet portal using Clientless SSL VPN with CSD.

## Goal 3:

- Allow **contractors** to only access email and some DMZ servers via RDP using Clientless SSL VPN with CSD.

# Topology



# Configuration Steps

1. Configuring tunnel groups and group policies
2. Configuring local users
3. Configuring CSD
4. Configuring DAP

# Configuring Tunnel Groups

The screenshot displays the Cisco ASDM 6.2 for ASA interface. The main window is titled "Add SSL VPN Connection Profile" and shows the configuration for a profile named "Employees". The "Authentication" section is expanded, showing the "Method" set to "AAA" and the "AAA Server Group" set to "LOCAL".

Overlaid on this is the "Configure Group Policies" dialog box. It contains the following text: "Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts." Below this text, there is a red box around the "Add" button and a "Delete" button. A table lists the existing group policies:

Name	Type	Tunneling Protocol	AAA Server Group
DfltGrpPolicy (System Default)	Internal	webvpn	-- N/A --

At the bottom of the dialog are "OK", "Cancel", and "Help" buttons.

# Configuring Tunnel Groups (cont)

The screenshot displays the configuration interface for VPN group policies. The main window is titled "Configure Group Policies" and contains a description of VPN group policies and a list of actions: Add, Edit, and Delete. The "Add" button is highlighted with a red box. Below this, a tree view shows the configuration hierarchy, with "Advanced" expanded to show "Split Tunneling", "IE Browser Proxy", "SSL VPN Client", and "IPsec Client".

The "Add Internal Group Policy" dialog box is open, showing the configuration for a policy named "Employee\_policy". The "Banner" field is checked for inheritance. The "Address Pools" field is unchecked, and the "IPv6 Address Pools" field is checked for inheritance. Two "Select..." buttons are visible, one of which is highlighted with a red box.

The "Select Address Pools" dialog box is also open, showing a table of address pools. The "sslpool" entry is selected and highlighted with a red box. The table has the following data:

Pool Name	Starting Address	Ending Address/Number of Addr...	Subnet Mask/Prefix Len...
sslpool	10.10.10.1	10.10.10.6	255.255.255.0

Below the table, the "Assigned Address Pools" section shows the "sslpool" entry assigned to the policy.

# Configuring Group URLs

Portal Page Customization:

Enable the display of Radius Reject-Message on the login screen when authentication is rejected

Enable the display of SecurId messages on the login screen

Connection Aliases

This SSL VPN access method will present a list of aliases configured for all connection profiles. You must enable the Login Page Setting in the main panel to complete the configuration.

(The table is in-line editable.)

Alias	Enabled

Group URLs

This SSL VPN access method will automatically select the connection profile, without the need for user selection.

(The table is in-line editable.)

URL	Enabled

Do not run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored.)

Find:

URL:

Enabled

# Configuring Local Users

The screenshot displays the Cisco ASDM 6.2 for ASA interface. The main window is titled "Configuration > Remote Access VPN > AAA/Local Users > Local Users". The left sidebar shows the configuration tree with "Local Users" selected. Two "Add User Account" dialog boxes are open. The first dialog shows the "Identity" section with "VPN Policy" selected, and the "Username" field containing "employee1". The "Group Policy" dropdown is set to "Employee\_policy". The second dialog shows the "Employee\_policy" group policy configuration, with "Inherit" checkboxes checked for "Group Policy", "Tunneling Protocols", "IPv4 Filter", "IPv6 Filter", "Connection Profile (Tunnel Group) Lock", "Store Password on Client System", "Access Hours", "Simultaneous Logins", "Maximum Connect Time", and "Idle Timeout".

Configuration > Remote Access VPN > AAA/Local Users > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Authorization](#).

AAA authentication console commands must be enabled in order for certain access restrictions to be enforced. To enable AAA authentication command go to [AAA Authentication Console](#).

**Add User Account**

Identity

- VPN Policy
- Clientless SSL VPN
- SSL VPN Client

Username:

Password:

Confirm Password:

User authenticated using MSCHAPv2

Access Restriction

Select one of the options below to restrict user access to the ASA. Note: All users have network access to the ASA.

Full access(ASDM, SSH, Telnet)

Privilege level is used with console access.

Privilege Level:

CLI login prompt for SSH, Telnet or Console

This setting is effective only when the user is logging in via the CLI.

No ASDM, SSH, Telnet or Console

This setting is effective only when the user is logging in via the CLI.

Find:

**Add User Account**

Identity

- VPN Policy
- Clientless SSL VPN
- SSL VPN Client

Check an Inherit checkbox to let the corresponding setting take its value from the group policy.

Group Policy:  Inherit  Employee\_policy

Tunneling Protocols:  Inherit  Clientless SSL VPN  SSL VPN Client  II

IPv4 Filter:  Inherit

IPv6 Filter:  Inherit

Connection Profile (Tunnel Group) Lock:  Inherit

Store Password on Client System:  Inherit  Yes  No

Connection Settings

Access Hours:  Inherit

Simultaneous Logins:  Inherit

Maximum Connect Time:  Inherit  Unlimited  Minutes

Idle Timeout:  Inherit  Unlimited  Minutes

Dedicated IP Address (Optional)

IP Address:  Subnet Mask:

Find:

Configuration changes saved successfully.



# Enabling CSD

Cisco ASDM 6.2 for ASA - 172.18.124.224

File View Tools Wizards Window Help Look For: [ ] Go

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN Configuration > Remote Access VPN > Secure Desktop Manager > Setup

Secure Desktop Image

Update Cisco Secure Desktop

Location: disk0:/csd\_3.4.1108.pkg Browse Flash...

Enable Secure Desktop Upload...

Uninstall

Apply Reset

Configuration changes saved successfully. <admin> 15 5/19/09 11:41:26 AM UTC

# Configuring CSD Policies

The screenshot displays the Cisco ASDM 6.2 for ASA interface. The title bar shows the device IP as 172.18.124.224. The breadcrumb navigation path is Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy. The left-hand navigation tree has 'Prelogin Policy' highlighted under the 'Secure Desktop Manager' section. The main configuration area shows a 'Prelogin Policy' diagram with a 'Start' node connected to an 'Employee\_Access' node. A dialog box is open at the bottom, titled 'Select the type of check that you would like to insert'. The 'Check:' dropdown is set to 'Registry Check', and the 'Add' button is highlighted with a red box. The status bar at the bottom indicates the user is logged in as <admin> and the time is 5/19/09 11:48:06 AM UTC.

# Configuring CSD Policies (cont)

The screenshot displays the Cisco ASDM 6.2 for ASA configuration interface. The main window title is "Cisco ASDM 6.2 for ASA - 172.18.124.224". The breadcrumb navigation shows "Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy".

The left sidebar contains a tree view of configuration objects, including "Remote Access VPN", "AAA/Local Users", "Secure Desktop Manager", "Setup", "Global Settings", "Prelogin Policy", "Secure Desktop Customiza", "Employee\_Access", "Host Scan", "Certificate Management", "Language Localization", "Load Balancing", "DHCP Server", "DNS", "Advanced", "Connection Gateway", "SSL Settings", "Certificate to SSL VPN Con", "HTTP Redirect", "Maximum SSL VPN Sessions", and "E-mail Proxy".

The main content area is titled "Prelogin Policy" and contains the following text: "Use the decision tree below to create prelogin policies. Click the + symbol to check for a specific registry key, file, certificate, OS version, or IP address. Click an end node to rename a prelogin policy, change it to a subsequence, or change it to 'Login Denied.'"

The decision tree diagram shows a "Start" node leading to a "Registry Check?" node. From "Registry Check?", a "Success" path leads to an "Employee\_Access" node, and a "Failure" path leads to a "Login Denied" node.

A modal dialog box is open, showing the configuration for the "Registry Check?" node. The "Key Path" is set to "HKEY\_LOCAL\_MACHINE \e\Altiris\Altiris Agent\Enc". The "DWORD value" is set to "1". The "Update" button is highlighted.

At the bottom of the main window, there are "Apply All" and "Reset All" buttons. The status bar at the bottom shows "Device configuration refreshed successfully.", the user "admin", page number "15", and the date/time "5/19/09 2:29:36 PM UTC".

# Configuring CSD Policies (cont)

Cisco ASDM 6.2 for ASA - 172.18.124.224

File View Tools Wizards Window Help Look For: Go

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN Configuration > Remote Access VPN > Secure Desktop Manager > Prelogin Policy

**Prelogin Policy**

Use the decision tree below to create prelogin policies. Click the + symbol to check for a specific registry key, file, certificate, OS version, or IP address. Click an end node to rename a prelogin policy, change it to a subsequence, or change it to "Login Denied."

```
graph LR; Start([Start]) --> Check[Registry Check?]; Check -- Success --> Access[Employee_Access]; Check -- Failure --> Denied[Login Denied];
```

Login Denied  Policy  Subsequence

Label:

Update Cancel

Apply All Reset All

<admin> 15 6/26/09 5:31:03 AM UTC

# Configuring CSD Policies (cont)

The screenshot shows the Cisco ASDM 6.2 for ASA interface. The title bar reads "Cisco ASDM 6.2 for ASA - 172.18.124.224". The breadcrumb navigation is "Configuration > Remote Access VPN > Secure Desktop Manager > Non\_Corp/Contractor\_Access".

The left sidebar shows a tree view of configuration options. The "Non\_Corp/Contractor\_Access" folder is selected and highlighted with a red box. Below it, sub-items like "Cache Cleaner", "Secure Desktop (Vault) Ger", "Secure Desktop (Vault) Set", and "Secure Desktop (Vault) Bro" are visible.

The main content area is titled "Privacy Protection" and contains the following text:

These options protect the remote computer from access to session data after session termination. If you check Secure Desktop (Vault) and it cannot install on the remote device but Cache Cleaner can, Cache Cleaner installs instead. Be sure to inspect both the Cache Cleaner and Secure Desktop (Vault) settings in the subordinate windows if you check Secure Desktop (Vault).

If you uncheck both Secure Desktop (Vault) and Cache Cleaner, the security appliance performs only Host Scan checks.

Install to wipe session data:  Secure Desktop (Vault) or  Cache Cleaner

The "Secure Desktop (Vault)" checkbox is highlighted with a red box. At the bottom of the configuration area, there are "Apply All" and "Reset All" buttons.

The status bar at the bottom shows "<admin> 15" and the date/time "6/26/09 5:47:03 AM UTC".

# Configuring CSD Policies (cont)

The screenshot displays the Cisco ASDM 6.2 for ASA configuration interface. The main window is titled "Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan". The left sidebar shows the configuration tree with "Host Scan" selected under "Secure Desktop Manager". The main content area shows the "Host Scan" configuration page, which includes a table for "Basic Host Scan" and a section for "Host Scan Extensions". A red box highlights the "Add" button and the "Registry Scan..." option in the "Basic Host Scan" section. An "Edit Registry Scan" dialog box is open in the foreground, showing the following fields:

- Endpoint ID: REG
- Entry Path: HKEY\_LOCAL\_MACHINE\ E:\Altiris\Altiris Agent\EnableNotifications

The dialog box has "OK" and "Cancel" buttons. The main window also shows "Apply All" and "Reset All" buttons at the bottom. The status bar at the bottom indicates "Device configuration refreshed successfully." and the user is logged in as "admin" on 5/19/09 2:35:56 PM UTC.

# Configuring DAP

The image shows two overlapping dialog boxes from a network configuration application. The background dialog is titled "Add Dynamic Access Policy" and the foreground dialog is titled "Add Endpoint Attribute".

**Add Dynamic Access Policy Dialog:**

- Policy Name: Employee\_corp
- Description: Policy for employees connecting with a corporate asset
- ACL Priority: 5
- Selection Criteria:** Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.
- Criteria: User has ANY of the following AAA Attributes values... (dropdown)
- AAA Attribute Table:

AAA Attribute	Operation/Value
cisco.tunnelgroup	= Employees
- Buttons: Add, Edit, Delete
- Advanced:** and the following endpoint attributes are satisfied.
- Endpoint ID Table:

Endpoint ID	Name/Operation/Value
-------------	----------------------
- Buttons: Add, Edit, Delete
- Access/Authorization Policy Attributes:** Configure access/authorization attributes for this policy. Attribute values specified here will be applied to the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes that are not specified in DAP).
- Action: Network ACL Filters | Web-Type ACL Filters | Functions | Port Forwarding Lists
- Access Method:
  - Unchanged
  - AnyConnect Client
  - Web-Portal
  - Both-default-Web-Portal
  - Both-default-AnyConnect Client

**Add Endpoint Attribute Dialog:**

- Endpoint Attribute Type: Registry
- Exists  Does not exist
- Endpoint ID: REG
- Path: HKEY\_LOCAL\_MACHINE\SOFTWARE\Altiris\Altiris Agent\EnableNotifications
- Value:  dword = 1
- Caseless
- Buttons: OK, Cancel, Help

# Configuring DAP (cont)

**Edit Dynamic Access Policy**

Policy Name: Employees\_no\_corp  
Description: Employees with no corporate assets  
ACL Priority: 10

**Selection Criteria**  
Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values...  
and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value
cisco.tunnelgroup	= Employees

Endpoint ID	Name/Operation/Value
registry.REG	exists = true type = dword value = 0

**Advanced**

**Access/Authorization Policy Attributes**  
Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Action:  Continue  Terminate

Specify the message that will be displayed when this record is selected.

User Message:

OK Cancel Help



# Configuring DAP (cont)

The screenshot displays the Cisco configuration interface for Dynamic Access Policy (DAP). It features three overlapping windows:

- Background Window: Edit Dynamic Access Policy**
  - Policy Name: Contractors
  - Description: Contractor Policy
  - ACL Priority: 15
  - Selection Criteria:**
    - Text: "User has ANY of the following AAA Attributes values..."
    - Table:

AAA Attribute	Operation/Value
cisco.tunnelgroup	= Contractors
  - Access/Authorization Policy Attributes:**
    - Checked:  Enable bookmarks
    - Text: Contractor
    - Button: Manage...
- Foreground Window: Edit Dynamic Access Policy**
  - Policy Name: Contractors
  - Description: Contractor Policy
  - ACL Priority: 15
  - Selection Criteria:**
    - Text: "User has ANY of the following AAA Attributes values..."
    - Table:

AAA Attribute	Operation/Value
cisco.tunnelgroup	= Contractors
  - Access/Authorization Policy Attributes:**
    - Checked:  Enable bookmarks
    - Text: Contractor
    - Button: Manage...
- Pop-up Window: Configure GUI Customization Objects**
  - Text: "Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page."
  - Text: "This parameter is enforced in either a VPN user, a group policy, or a dynamic access policy configuration."
  - Buttons: Add, Edit, Delete, Import, Export
  - Table:

Bookmarks
Template
Employee
Contractor
  - Buttons: OK, Cancel, Help

# Configuring Bookmarks

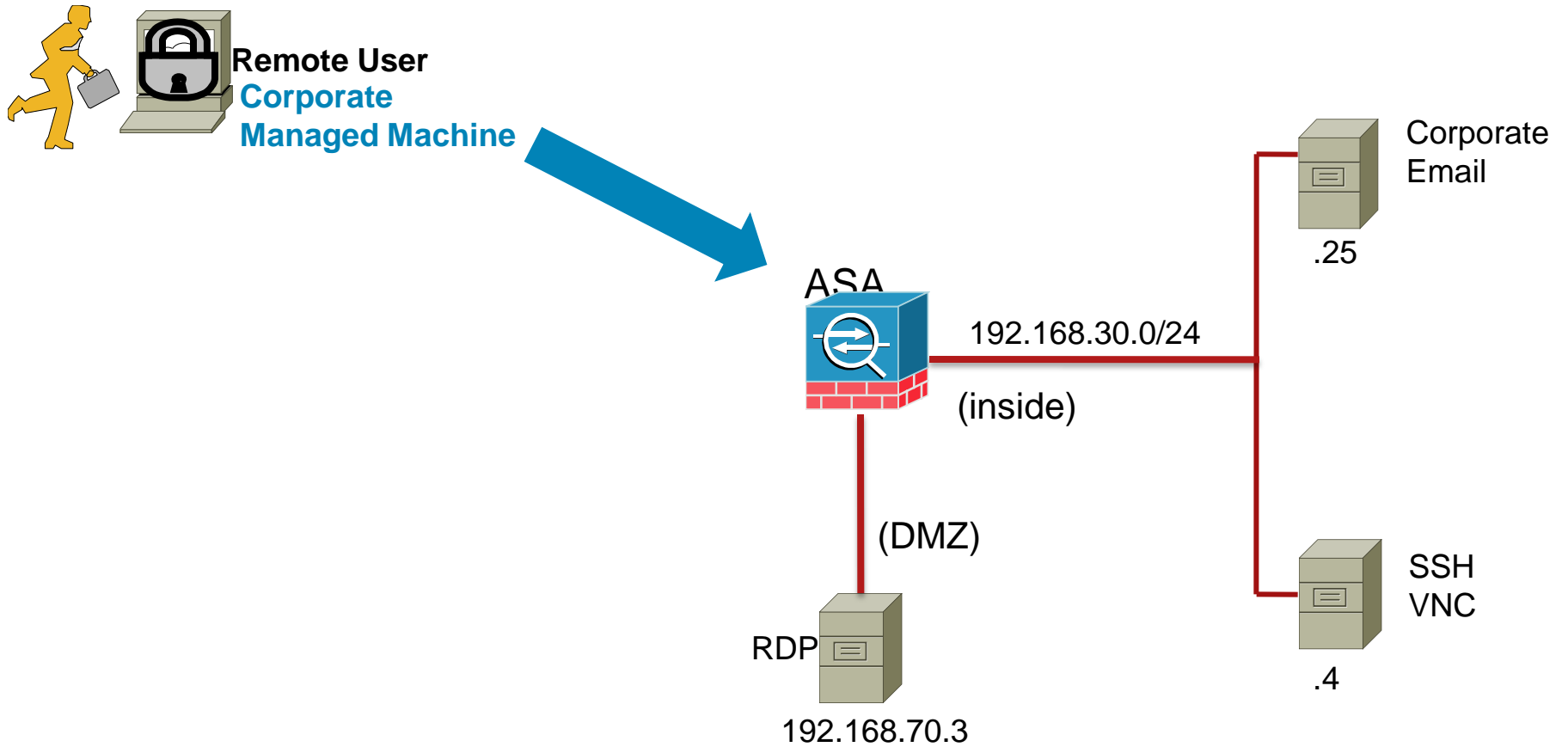
The screenshot shows the Cisco ASDM 6.2 for ASA configuration interface. The main window is titled "Add Dynamic Access Policy" and shows the configuration for a policy named "Contractors". The "Bookmarks" tab is selected, and the "Edit Bookmark List" dialog is open. The dialog shows a table with the following data:

Bookmark Title	URL
Corporate Email Access	https://192.168.30.25
RDP DMZ	rdp://192.168.70.3

The "Edit" button in the dialog is highlighted with a red box. The main window also shows the "Bookmarks" tab with a list of bookmarks: Contractor, Employee, and Template. The "Contractor" bookmark is selected. The "Add Dynamic Access Policy" window also shows the "Bookmarks" tab with a list of bookmarks: Contractor, Employee, and Template. The "Contractor" bookmark is selected. The "Add Dynamic Access Policy" window also shows the "Bookmarks" tab with a list of bookmarks: Contractor, Employee, and Template. The "Contractor" bookmark is selected.

# Example 1: Employee Access with Corporate PC

# Topology



# Employee Access – Corporate PC

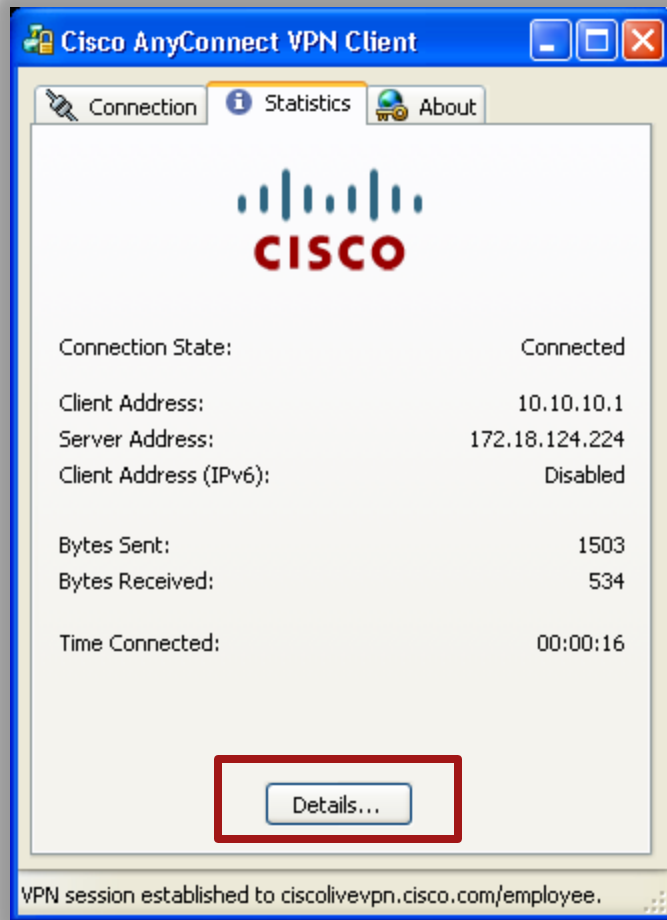
The image displays three sequential screenshots of the Cisco AnyConnect VPN Client interface:

- Left Screenshot:** Shows the main interface with the Cisco logo and a "Connect to:" dropdown menu. The selected profile is "evpn.cisco.com/employee". A blue callout box contains the text "ciscolivevpn.cisco.com/employee" with an arrow pointing to the dropdown menu. A "Select" button is visible at the bottom.
- Middle Screenshot:** Shows the same interface, but the "Connect to:" dropdown is now set to "ciscolivevpn.cisco.com/er". A "Posture Assessment: Initiating..." message is visible at the bottom.
- Right Screenshot:** Shows the login screen with the "Connect to:" dropdown set to "ciscolivevpn.cisco.com/er". The "Username:" field contains "employee1" and the "Password:" field contains "\*\*\*\*\*". A "Connect" button is visible at the bottom. A "Please enter your username and password." message is visible at the bottom.

Red arrows point from the "Select" button in the first screenshot to the "Posture Assessment" message in the second, and from the "Connect" button in the second screenshot to the login screen in the third.



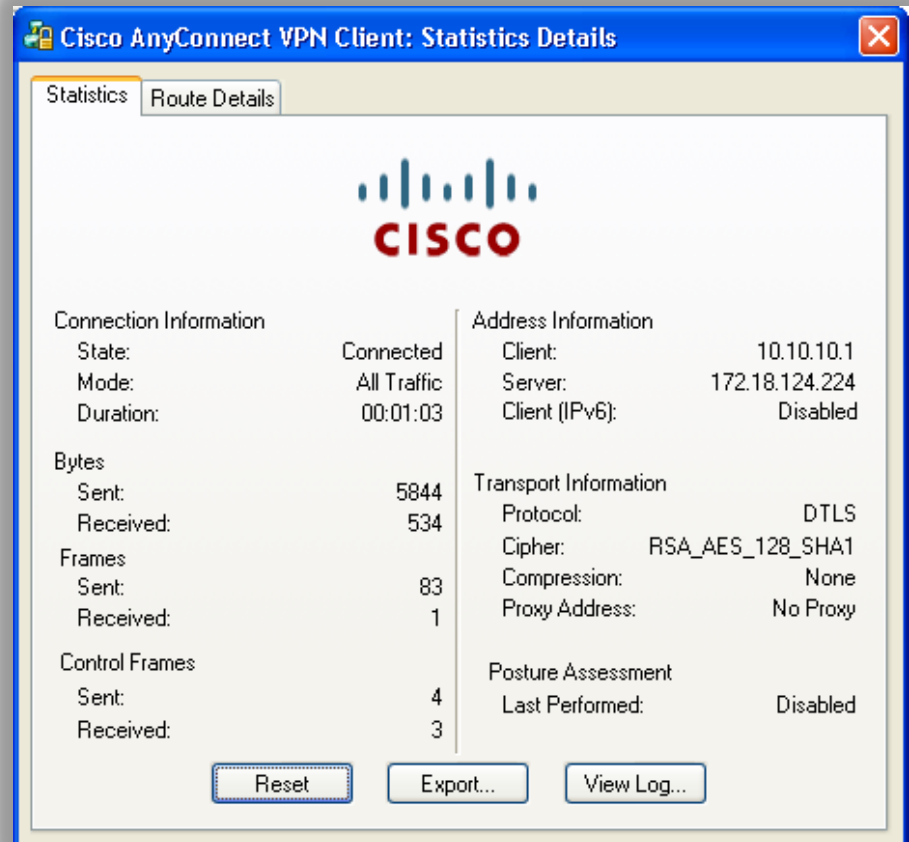
# Employee Access – Corporate PC



The screenshot shows the main window of the Cisco AnyConnect VPN Client. The title bar reads "Cisco AnyConnect VPN Client". There are three tabs: "Connection", "Statistics", and "About". The "Connection" tab is active. The Cisco logo is prominently displayed. Below the logo, the following information is shown:

Connection State:	Connected
Client Address:	10.10.10.1
Server Address:	172.18.124.224
Client Address (IPv6):	Disabled
Bytes Sent:	1503
Bytes Received:	534
Time Connected:	00:00:16

A "Details..." button is highlighted with a red rectangle at the bottom of the window. At the very bottom of the window, a status bar reads: "VPN session established to ciscolivevpn.cisco.com/employee."



The screenshot shows the "Statistics Details" window of the Cisco AnyConnect VPN Client. The title bar reads "Cisco AnyConnect VPN Client: Statistics Details". There are two tabs: "Statistics" and "Route Details". The "Statistics" tab is active. The Cisco logo is prominently displayed. Below the logo, the following information is shown:

Connection Information		Address Information	
State:	Connected	Client:	10.10.10.1
Mode:	All Traffic	Server:	172.18.124.224
Duration:	00:01:03	Client (IPv6):	Disabled
Bytes		Transport Information	
Sent:	5844	Protocol:	DTLS
Received:	534	Cipher:	RSA_AES_128_SHA1
Frames		Compression:	None
Sent:	83	Proxy Address:	No Proxy
Received:	1	Posture Assessment	
Control Frames		Last Performed:	Disabled
Sent:	4		
Received:	3		

At the bottom of the window, there are three buttons: "Reset", "Export...", and "View Log..."

# Debugs enabled on ASA

**debug webvpn 200**

**debug webvpn svc 200**

**debug dap trace**

**debug dap events**

# Employee Access – Corporate PC

webvpn\_auth.c:http\_webvpn\_pre\_authentication[2327]

WebVPN: calling AAA with ewsContext (-1275712960) and nh (-1300499416)!

webvpn\_auth.c:webvpn\_add\_auth\_handle[5118]

WebVPN: started user authentication...

webvpn\_auth.c:webvpn\_aaa\_callback[5158]

WebVPN: AAA status = (ACCEPT)

ewaFormSubmit\_webvpn\_login: tgCookie = 0Employees

ewaFormSubmit\_webvpn\_login: cookie = 1

ewaFormSubmit\_webvpn\_login: tgCookieSet = 0

ewaFormSubmit\_webvpn\_login: tgroup = Employees

DAP\_TRACE: dap\_add\_to\_lua\_tree:aaa["cisco"]["grouppolicy"] = "Employee\_policy";


DAP\_TRACE: dap\_add\_to\_lua\_tree:aaa["cisco"]["class"] = "Employee\_policy";

DAP\_TRACE: dap\_add\_to\_lua\_tree:aaa["cisco"]["username"] = "employee1";


DAP\_TRACE: dap\_add\_to\_lua\_tree:aaa["cisco"]["tunnelgroup"] = "Employees";

DAP\_TRACE: dap\_add\_to\_lua\_tree:endpoint["application"]["clienttype"] = "AnyConnect";

User Authentication  
Accepted



User info collected  
through DAP





# Employee Access – Corporate PC


```
endpoint.os.version = "Windows XP";  
endpoint.os.servicepack = "3";  
endpoint.policy.location = "Employee_Access";  
endpoint.device.protection = "cache cleaner";  
endpoint.device.hostname = "ggilbert-wxp02.cisco.com";  
endpoint.device.protection_version = "3.4.1108.0";  
endpoint.device.protection_extension = "2.5.16.1";
```

CSD Policy applied  
for user



```
endpoint.registry["REG"] = {};  
endpoint.registry["REG"].exists = "true";  
endpoint.registry["REG"].path = "HKEY_LOCAL_MACHINE\\SOFTWARE\\Altiris\\Altiris  
Agent\\EnableNotifications";  
endpoint.registry["REG"].type = "dword";  
endpoint.registry["REG"].value = "1";
```

Endpoint Registry  
check



# Employee Access – Corporate PC

```
endpoint.as["McAfeeAS"].exists = "true";  
endpoint.as["McAfeeAS"].description = "McAfee Anti-Spyware Enterprise Module";  
endpoint.as["McAfeeAS"].version = "8.0.0.989";  
endpoint.as["McAfeeAS"].activescan = "ok";  
endpoint.as["McAfeeAS"].lastupdate = "214691";  
endpoint.as["McAfeeAS"].timestamp = "1245643200";  
endpoint.av["WmiAV"] = {};  
endpoint.av["WmiAV"].exists = "true";  
endpoint.av["WmiAV"].description = "Cisco unknown product";  
endpoint.av["WmiAV"].version = "V6.0.0.220";  
endpoint.av["WmiAV"].activescan = "ok";
```

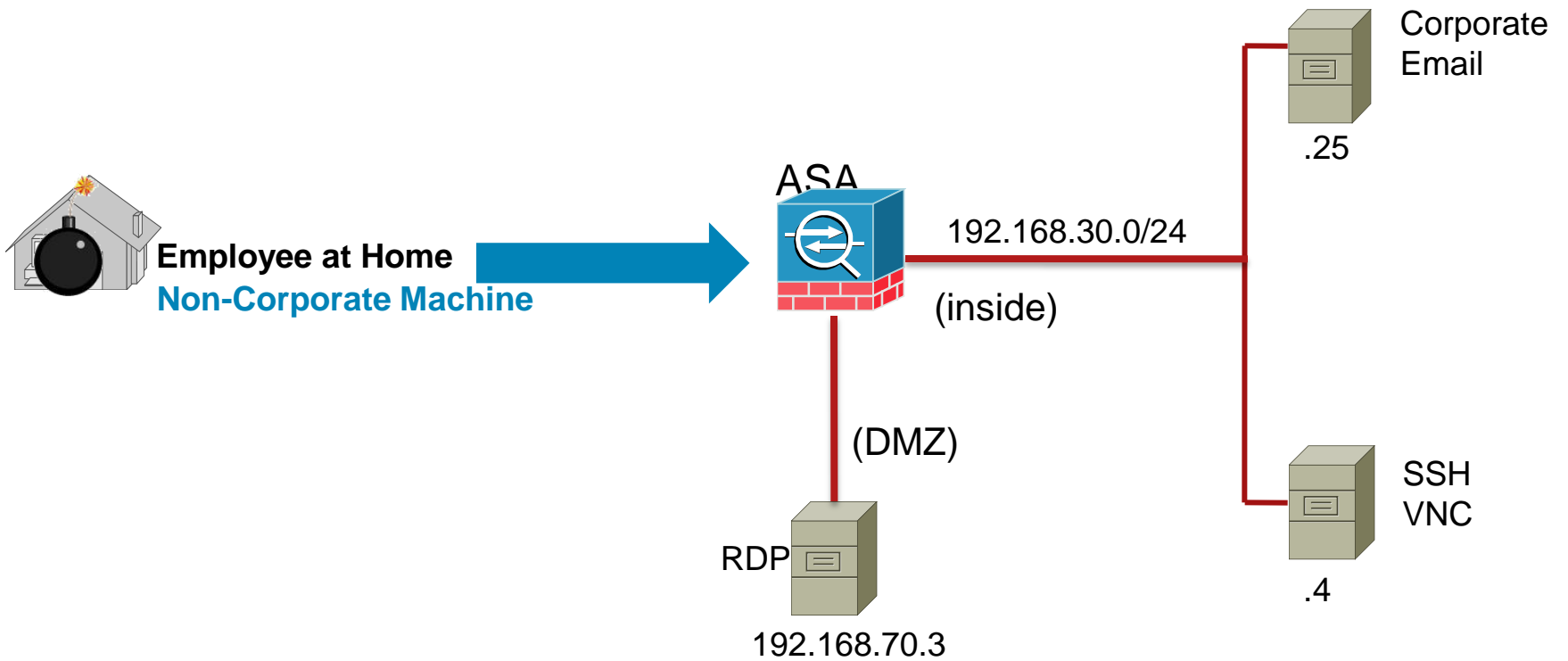
AV identified through  
Host Scan process

```
DAP_TRACE: Username: employee1, Selected DAPs: ,Employee_corp  
DAP_TRACE: dap_request: memory usage = 40%  
DAP_TRACE: dap_process_selected_daps: selected 1 records  
DAP_TRACE: Username: employee1, dap_aggregate_attr: rec_count = 1  
CSTP state = CONNECTED
```

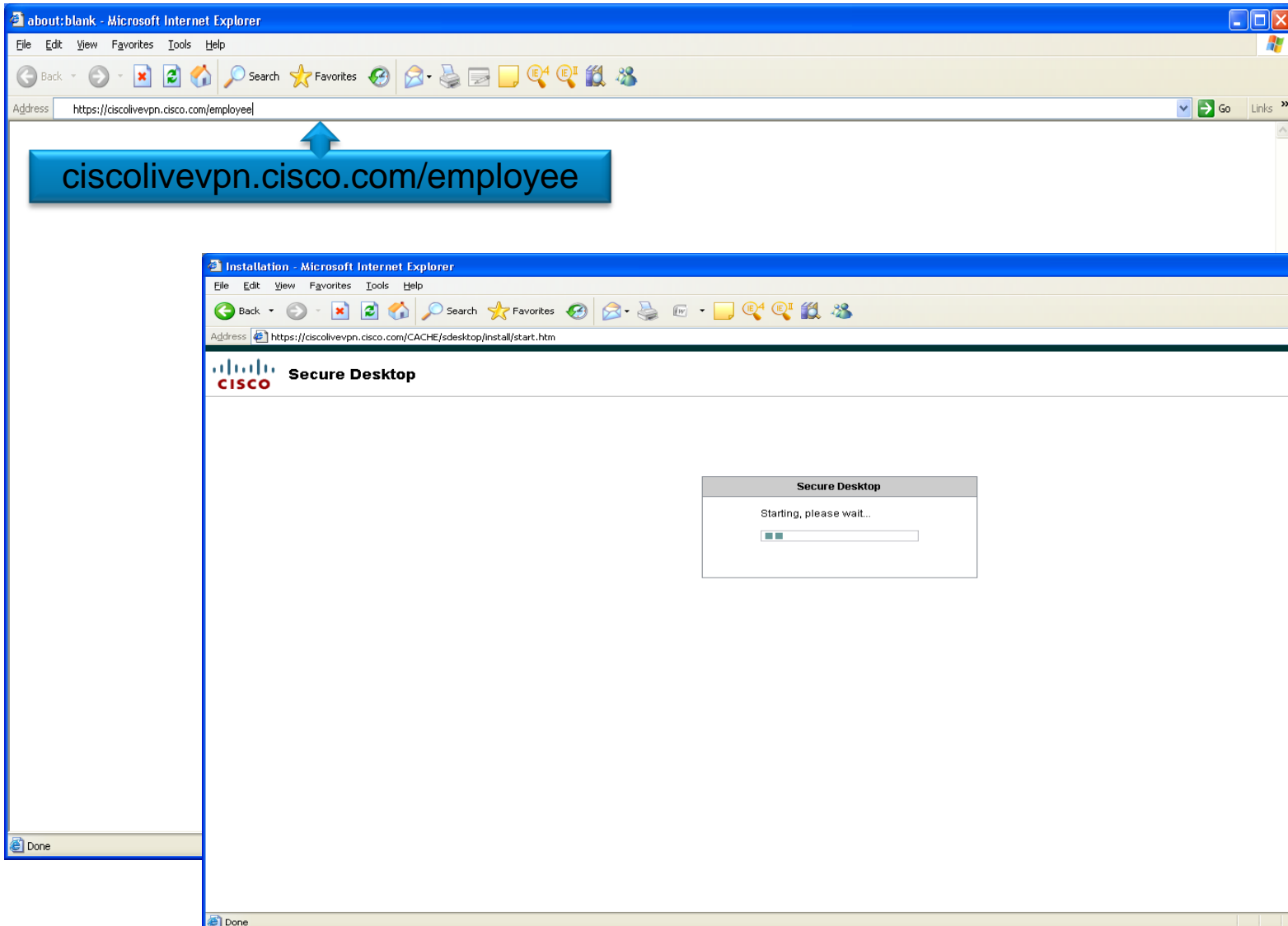
DAP record selected  
for the user

## Example 2: Employee Access with Non-corporate PC

# Topology



# Employee Access – Non-corporate PC



# Employee Access – Non-corporate PC

The screenshot displays a Windows XP desktop environment. The desktop background is light blue. On the left side, there is a vertical taskbar with icons for 'My Documents', 'My Computer', 'My Network Places', 'Recycle Bin', 'Internet Explorer', 'Microsoft Office Outlook', and 'csd\_contrac...'. The taskbar at the bottom features the 'start' button, several application icons, and a system tray with a clock showing '8:55 AM' and the text 'Local intranet'.

The central focus is a Microsoft Internet Explorer browser window titled 'https://ciscolivevpn.cisco.com/+CSCOE+/portal.html - Microsoft Internet Explorer'. The browser's address bar shows the URL 'https://ciscolivevpn.cisco.com/+CSCOE+/portal.html'. The page content includes the Cisco logo and the text 'SSL VPN Service'. A navigation menu on the left lists: Home, Web Applications, Browse Networks, Terminal Servers, VNC Connections, and Telnet/SSH Servers. The main content area is divided into sections: 'Web Bookmarks' with 'Corporate Email Access', 'Terminal Servers Bookmarks' with 'RDP DMZ', 'VNC Bookmarks' with 'VNC Server', and 'Telnet and SSH bookmarks' with 'SSH Linux Box'. A search bar at the top of the page contains 'http://' and a 'Browse' button. A 'Logout' link is visible in the top right corner of the page content.

On the right side of the desktop, there are three red icons: 'Launch Login Page', 'Switch Desktop', and 'Close Desktop'.

# Employee Access – Non-corporate PC

```
webvpn_auth.c:webvpn_add_auth_handle[5118]
```

```
WebVPN: started user authentication...
```

```
WebVPN: AAA status = (ACCEPT)
```

```
webvpn_portal.c:ewaFormSubmit_webvpn_login[2162]
```

```
ewaFormSubmit_webvpn_login: tgCookie = 0Employees
```

```
ewaFormSubmit_webvpn_login: cookie = 1
```

```
ewaFormSubmit_webvpn_login: tgCookieSet = 0
```


```
ewaFormSubmit_webvpn_login: tgroup = NULL
```

```
webvpn_auth.c:http_webvpn_post_authentication[1506]
```

```
WebVPN: user: (employee2) authenticated.
```

```
webvpn_auth.c:http_webvpn_auth_accept[2994]
```

User Authentication Accepted



```
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["grouppolicy"] = "Employee_policy";
```


```
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["class"] = "Employee_policy";
```

```
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] = "employee2";
```

```
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "Employees";
```

```
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]["clienttype"] = "Clientless";
```


User info collected through DAP



# Employee Access – Non-corporate PC


```
endpoint.os.version = "Windows XP";  
endpoint.os.servicepack = "3";  
endpoint.policy.location = "Non_Corp/Contractor_Access";  
endpoint.device.protection = "secure desktop";  
endpoint.device.hostname = "ggilbert-wxp02.cisco.com";  
endpoint.device.protection_version = "3.4.1108.0";  
endpoint.device.protection_extension = "2.5.16.1";
```

CSD policy applied to user



```
endpoint.registry["REG"] = {};  
endpoint.registry["REG"].exists = "true";  
endpoint.registry["REG"].path = "HKEY_LOCAL_MACHINE\\SOFTWARE\\Altiris\\Altiris  
Agent\\EnableNotifications";  
endpoint.registry["REG"].type = "dword";  
endpoint.registry["REG"].value = "0";
```

Endpoint registry check






# Employee Access – Non-corporate PC


```
endpoint.fw["MSWindowsFW"] = {};  
endpoint.fw["MSWindowsFW"].exists = "false";  
endpoint.fw["MSWindowsFW"].description = "Microsoft Windows Firewall";  
endpoint.fw["MSWindowsFW"].version = "XP SP2+";  
endpoint.fw["MSWindowsFW"].enabled = "failed";  
endpoint.av["McAfeeAV"] = {};  
endpoint.av["McAfeeAV"].exists = "true";  
endpoint.av["McAfeeAV"].description = "McAfee VirusScan Enterprise";  
endpoint.av["McAfeeAV"].version = "8.0.0";  
endpoint.av["McAfeeAV"].activescan = "ok";  
endpoint.av["McAfeeAV"].lastupdate = "117998";  
endpoint.av["McAfeeAV"].timestamp = "1242705600";
```

AV/FW information  
collected through host  
scan



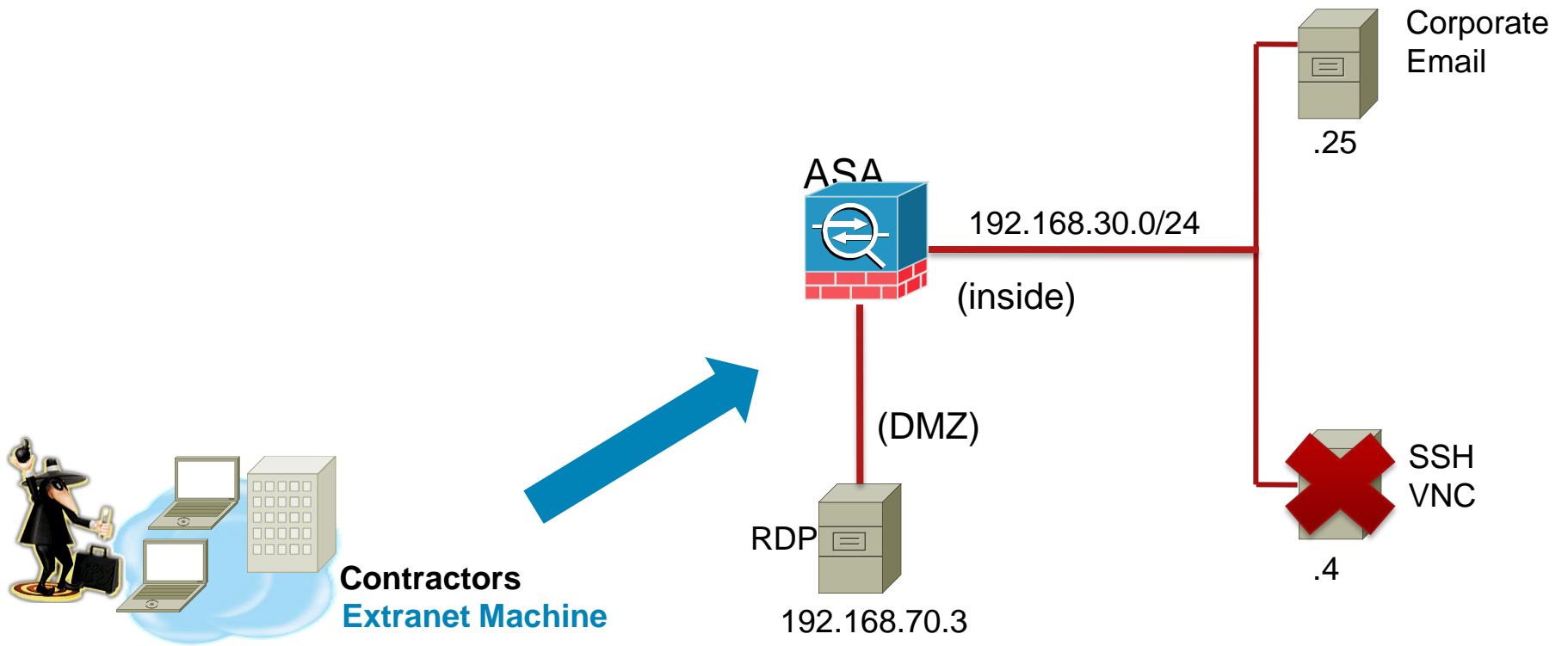
```
DAP_TRACE: Username: employee2, Selected DAPs: ,Employees_no_corp  
DAP_TRACE: dap_request: memory usage = 42%  
DAP_TRACE: dap_process_selected_daps: selected 1 records  
DAP_TRACE: Username: employee2, dap_aggregate_attr: rec_count = 1
```

DAP record applied to  
user

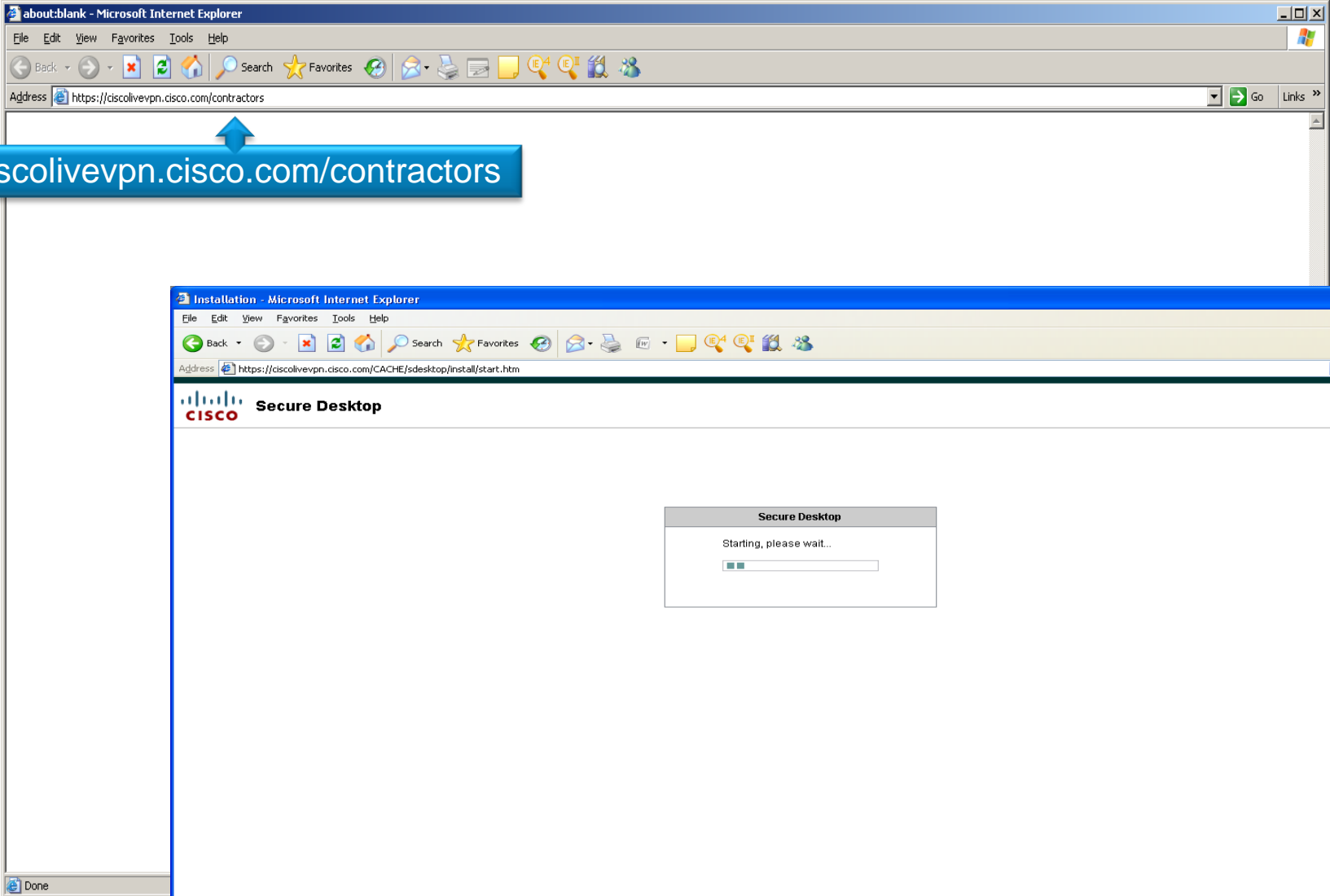


# Example 3: Contractor Access

# Topology



# Contractor Access



# Contractor Access

The screenshot displays a Windows XP desktop environment. A Microsoft Internet Explorer browser window is open, showing the Cisco SSL VPN Service portal. The browser's address bar contains the URL `https://ciscolvevpn.cisco.com/+CSCOE+/portal.html`. The page title is "CISCO SSL VPN Service". On the left side of the browser window, there is a navigation menu with the following items: Home, Web Applications, Browse Networks, Terminal Servers, VNC Connections, and Telnet/SSH Servers. The main content area of the browser window features a search bar with the text "http://", a "Browse" button, and a "Logout" button. Below the search bar, there are two bookmark sections: "Web Bookmarks" with a link to "Corporate Email Access" and "Terminal Servers Bookmarks" with a link to "RDP DMZ". The desktop background is light blue. On the left side of the desktop, there are several icons: My Documents, My Computer, My Network Places, Recycle Bin, Internet Explorer, Microsoft Office Outlook, and a file named "csd\_contrac...". The bottom taskbar shows the Start button, several application icons, and the system tray with the time 8:55 AM and date 8/15/2009. In the bottom right corner of the desktop, there are three icons: "Launch Login Page", "Switch Desktop", and "Close Desktop".

# Contractor Access

```
webvpn_auth.c:webvpn_add_auth_handle[5118]
```

```
WebVPN: started user authentication...
```

```
webvpn_auth.c:webvpn_aaa_callback[5158]
```

```
WebVPN: AAA status = (ACCEPT)
```

```
webvpn_portal.c:ewaFormSubmit_webvpn_login[2162]
```

```
ewaFormSubmit_webvpn_login: tgCookie = 0Contractors
```

```
ewaFormSubmit_webvpn_login: cookie = 1
```

```
ewaFormSubmit_webvpn_login: tgCookieSet = 0
```

```
webvpn_auth.c:http_webvpn_post_authentication[1506]
```

```
WebVPN: user: (contractor1) authenticated.
```

```
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["grouppolicy"] = "Contractors";
```

```
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["class"] = "Contractors";
```

```
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] = "contractor1";
```

```
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "Contractors";
```

```
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]["clienttype"] = "Clientless";
```

User Authentication  
Accepted

User info collected  
through DAP

# Contractor Access

```
endpoint.os.version = "Windows Vista";
endpoint.os.servicepack = "1";
endpoint.policy.location = "Non_Corp/Contractor_Access";
endpoint.device.protection = "secure desktop";
endpoint.device.hostname = "rtpvpn-vista";
endpoint.device.protection_version = "3.4.1108.0";
endpoint.device.protection_extension = "2.5.16.1";
.....
endpoint.os.hotfix["KB960715"] = "true";
endpoint.os.hotfix["KB960803"] = "true";
endpoint.os.hotfix["KB961501"] = "true";
endpoint.os.hotfix["KB963027"] = "true";
endpoint.os.hotfix["KB968537"] = "true";
.....
endpoint.registry["REG"] = {};
endpoint.registry["REG"].exists = "false";
```

← CSD policy applied to user


← Endpoint KB hot fixes found

← Endpoint registry check

# Contractor Access


```
endpoint.fw["MSWindowsFW"] = {};  
endpoint.fw["MSWindowsFW"].exists = "true";  
endpoint.fw["MSWindowsFW"].description = "Microsoft Windows Firewall";  
endpoint.fw["MSWindowsFW"].version = "Vista";  
endpoint.fw["MSWindowsFW"].enabled = "ok";  
endpoint.as["MicrosoftAS"] = {};  
endpoint.as["MicrosoftAS"].exists = "true";  
endpoint.as["MicrosoftAS"].description = "Windows Defender Vista";  
endpoint.as["MicrosoftAS"].version = "1.1.1600.0";  
endpoint.as["MicrosoftAS"].activescan = "ok";  
endpoint.as["MicrosoftAS"].lastupdate = "107997";  
endpoint.as["MicrosoftAS"].timestamp = "1245920100";
```

AV/FW information  
collected through host  
scan



```
DAP_TRACE: Username: contractor1, Selected DAPs: ,Contractors  
DAP_TRACE: dap_request: memory usage = 40%  
DAP_TRACE: dap_process_selected_daps: selected 1 records  
DAP_TRACE: Username: contractor1, dap_aggregate_attr: rec_count = 1
```

DAP record applied to  
user





# Q&A

