IPSec and SSL
Remote Access
VPNs

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

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>IPSec</th>
<th>SSL VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost</strong></td>
<td>Free License</td>
<td>Must purchase a license</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Many different types of licenses:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>❖ AnyConnect Essential,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>❖ AnyConnect Premium,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>❖ AnyConnect Mobile,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>❖ SSL Shared Premium</td>
</tr>
<tr>
<td><strong>User Environment</strong></td>
<td>Suited for permanent or full-time telecommuters</td>
<td>Suited for all types of users including contractors, temp workers or even fulltime workers</td>
</tr>
<tr>
<td><strong>Connectivity</strong></td>
<td>Establishes seamless connection to network.</td>
<td>Supports application connectivity through browser portal.</td>
</tr>
<tr>
<td><strong>End-Workstations</strong></td>
<td>Only 32-bit Windows operating systems are supported</td>
<td>32- and 64-bit Windows operating systems are supported</td>
</tr>
</tbody>
</table>
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

IKE

Cisco ASA

Responder

DH key exchange complete, share secret SKEYID derived

HDR, SA_proposal, KE_I, N_I, ID_I, VID_I

HDR, SA_choice, KE_R, N_R, ID_R, VID_R, HASH_R

HDR, HASH_I

IDs are exchanged, HASH is verified for authentication

Phase 1 SA parameter negotiation complete
Phase 1.5 with Pre-Shared Key

VPN Client

Initiator

X-AUTH

Mode-Config

Cisco ASA

Responder

Phase 1.5

HDR, X-Auth Request

HDR, X-Auth Reply

HDR, X-Auth Status Set

HDR, X-Auth Status Set Ack

HDR, Mode-Config Request

HDR, Mode-Config Reply
Phase II Quick Mode Negotiation

- Protected by Phase 1 SA
- Optional DH exchange for Perfect Forward Secrecy (PFS)
- Negotiate IPSec SA parameters, including proxy identities [ID_{CI}, ID_{CR}]
- Two unidirectional IPSec SA established with unique SPI number
Cisco IPSec Remote Access VPN

Configuration Example
Layout

WINS

DNS

ASA

209.165.200.226

10.1.1.0/24

Internet

VPN Client

209.165.201.1

PIX/ASA

209.165.201.2

14.38.1.0/24

14.38.2.0/24

Router

209.165.201.4

209.165.201.0

EasyVPN Clients
Cisco VPN Client to Cisco ASA 8.0 +

no nat-control

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

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

sysopt connection permit-vpn

ip local pool ippool 192.168.1.1-192.168.1.254 mask 255.255.255.0

To bypass NAT. Enabled by default

ISAKMP Policy Defines Phase 1 Parameters

Dynamic crypto map

Static crypto map

Sysopt Command Bypasses Conduits or ACLs Checking for the Inbound VPN Packets after Decryption
username cisco password cisco123
username pix password cisco123

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

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
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
hostname vpn-pix501b
domain-name cisco.com

vpnclient server 209.165.200.226
vpnclient mode network-extension-mode
vpnclient vpn-group 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
[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) + 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**

**Decoding received attributes**

**Received 1st packet from VPN Client**

**Group lookup successful**
Debugs from successful connection

debg crypto isakmp 127
debg 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) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length: 444

[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

[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

Sending 2\textsuperscript{nd} packet of AM

Received 3\textsuperscript{rd} packet of AM

NAT-T Checking
Deubs from successful connection

debug crypto isakmp 127
debug crypto ipsec 127

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

[X-AUTH Status Set & Ack]

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

[IKEv1]: IP = 209.165.201.1, IKE_DECODDE 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

[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!

[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
Debugs from successful connection

debbug crypto isakmp 127
debbug 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, processed

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

debag crypto isakmp 127
debag 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 @ 0xAFA0B580,
SCB: 0xADAC4E88,
Direction: outbound
SPI : 0x7DD8ED8C
Tunnel type: ra
Protocol : esp

[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

[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), VID(Nat-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
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 2nd packet of IKE exchange is decoded by the VPN client

VPN client sends the 3rd 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 209.165.200.226:44
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
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 = MODECFGUNITY_SAVEPWD: , value = 0x00000000

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

44  11:44:48.109 05/17/09  Sev=Info/5  IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFGUNITY_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

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

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 =

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

59  11:44:48.234  05/17/09  Sev=Info/5  CVPND/0x63400013
Current Routing Table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Netmask</th>
<th>Gateway</th>
<th>Interface</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>209.165.200.226</td>
<td>209.165.201.1</td>
<td>20</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>255.0.0.0</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>1</td>
</tr>
<tr>
<td>209.165.200.0</td>
<td>255.255.255.0</td>
<td>209.165.201.1</td>
<td>209.165.201.1</td>
<td>20</td>
</tr>
<tr>
<td>209.165.200.255</td>
<td>255.255.255.255</td>
<td>209.165.201.1</td>
<td>209.165.201.1</td>
<td>20</td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>209.165.201.1</td>
<td>209.165.201.1</td>
<td>20</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>255.255.255.255</td>
<td>209.165.201.1</td>
<td>209.165.201.1</td>
<td>1</td>
</tr>
</tbody>
</table>
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=

<table>
<thead>
<tr>
<th>Destination</th>
<th>Netmask</th>
<th>Gateway</th>
<th>Interface</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>209.165.200.226</td>
<td>209.165.201.1</td>
<td>20</td>
</tr>
<tr>
<td>14.0.0.0</td>
<td>255.0.0.0</td>
<td>192.168.1.10</td>
<td>192.168.1.10</td>
<td>20</td>
</tr>
<tr>
<td>192.168.1.10</td>
<td>255.255.255.255</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>20</td>
</tr>
<tr>
<td>14.255.255.255</td>
<td>255.255.255.255</td>
<td>192.168.1.10</td>
<td>192.168.1.10</td>
<td>20</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>255.0.0.0</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>1</td>
</tr>
<tr>
<td>209.165.200.0</td>
<td>255.255.255.0</td>
<td>209.165.201.1</td>
<td>209.165.201.1</td>
<td>20</td>
</tr>
<tr>
<td>209.165.201.1</td>
<td>255.255.255.255</td>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>20</td>
</tr>
<tr>
<td>209.165.200.255</td>
<td>255.255.255.255</td>
<td>209.165.201.1</td>
<td>209.165.201.1</td>
<td>20</td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>192.168.1.10</td>
<td>192.168.1.10</td>
<td>20</td>
</tr>
<tr>
<td>224.0.0.0</td>
<td>240.0.0.0</td>
<td>209.165.201.1</td>
<td>209.165.201.1</td>
<td>20</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>255.255.255.255</td>
<td>192.168.1.10</td>
<td>192.168.1.10</td>
<td>1</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>255.255.255.255</td>
<td>209.165.201.1</td>
<td>209.165.201.1</td>
<td>1</td>
</tr>
</tbody>
</table>

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

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/PIX 7.0, 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`

C advisoryon 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`
debus crypto ipsec enabled at level 127
debus crypto isakmp enabled at level 127
## Show Commands

```
show crypto protocol statistics all
```

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Encrypt packet requests</th>
<th>Encapsulate packet requests</th>
<th>Decrypt packet requests</th>
<th>Decapsulate packet requests</th>
<th>HMAC calculation requests</th>
<th>SA creation requests</th>
<th>SA rekey requests</th>
<th>SA deletion requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKEv1</td>
<td>198</td>
<td>198</td>
<td>198</td>
<td>198</td>
<td>234</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>IPsec</td>
<td>27</td>
<td>27</td>
<td>27</td>
<td>27</td>
<td>27</td>
<td>4</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

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:

1. Buy a bigger box (such as ASA 5540) and replace it with 5520
2. Buy another ASA 5520 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
```

---

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-zonealarmpro 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.

```plaintext
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:

- IP addresses:
  - 192.168.60.0/24
  - 192.168.40.0/24
  - 209.165.202.129
  - 209.165.201.10
  - 209.165.202.129

- Network devices:
  - Syslog server (192.168.60.150)
  - AAA Server (192.168.60.160)
  - Router1 (192.168.40.1)
  - Brussels
  - User1 (209.165.201.10)
  - www.cisco.com

- Traffic types:
  - Encrypted Traffic
  - IPSec tunnel
  - Clear-text Traffic
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
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

Customizable Banner Graphic

Customizable Access Methods

Customizable Banner Message

Customizable Links, Network Resource Access

Customizable Colors and Sections

Localisation

Advanced 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**
  
  Citrix 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

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.
SSL VPN Wizard (Cont.)

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

Connection Name: myclientlessvpn
SSL VPN Interface: outside

Digital Certificate
When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.
Certificate: -- None --

Connection Group Settings

Connection Group Alias/URL: vpn
Display Group Alias list at the login page

Information
URL to access SSL VPN Service:
https://209.165.201.1
https://209.165.201.1/vpn
https://209.165.201.1/admin
SSL VPN Wizard (Cont.)

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
A New Group Policy Is Created Called myclientlessgroup.

A Group Policy Is a Collection of User Attributes and Value Pairs.
SSL VPN Wizard (Cont.)

Configure a list of group intranet websites that appears in the portal page as links that Clientless users can navigate to.

1. **Manage**

2. **Add**

3. **Bookmark List Name**: Intranet Sites

4. **Bookmark Title**: Main Employee Intranet Site
   **URL Value**: http://intranetsite.cisco.com
SSL VPN Wizard (Cont.)

**CLI Configuration**

```shell
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
```
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


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

New in 8.2.
General Authentication Problems

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: 57442D62F3BO29AE4FDCE5BA6BC86186
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

Using the CLI:

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

You Can Combine the Debridgs Listed Above with the `debug webvpn`, when Troubleshooting Clientless Authentication Problems.
# Clientless SSL VPN Debugs

<table>
<thead>
<tr>
<th>Problem</th>
<th>Debug Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessing CIFS Shares</td>
<td>debug webvpn cifs (1-255)</td>
</tr>
<tr>
<td>Accessing NFS Shares</td>
<td>debug webvpn nfs(1-255)</td>
</tr>
<tr>
<td>Citrix Connection Problems</td>
<td>debug webvpn citrix (1-255)</td>
</tr>
<tr>
<td>Javascript Mangling Problems (User Specific)</td>
<td>debug webvpn javascript trace user user1</td>
</tr>
</tbody>
</table>
Useful Show Commands

**show webvpn statistics**

```plaintext
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**

```plaintext
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 **Export** Button Saves the Information on the **Details** Screen, Along with Other Connection Information, to a Text File for Troubleshooting
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
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.tmpl
- On non-Windows machines the location will be:
  /opt/cisco/vpn/profile/AnyConnectProfile.tmpl
- 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

- 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
Event Viewer

An Example of How Windows Event Viewer Looks
# Show Commands

ciscoasa# **show vpn-sessiondb summary**

Active Session Summary

<table>
<thead>
<tr>
<th>Sessions</th>
<th>Active</th>
<th>Cumulative</th>
<th>Peak Concurrent</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebVPN</td>
<td>2</td>
<td>13</td>
<td>7</td>
</tr>
<tr>
<td>SSL VPN Client</td>
<td>1</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Email Proxy</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPSec LAN-to-LAN</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPSec Remote Access</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>3</td>
<td>17</td>
<td></td>
</tr>
</tbody>
</table>

License Information:

<table>
<thead>
<tr>
<th>IPSec</th>
<th>Configured</th>
<th>Active</th>
<th>Load</th>
</tr>
</thead>
<tbody>
<tr>
<td>250</td>
<td>250</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>WebVPN</td>
<td>250</td>
<td>2</td>
<td>1%</td>
</tr>
<tr>
<td>Total</td>
<td>500</td>
<td>2</td>
<td>0%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Active</th>
<th>Cumulative</th>
<th>Peak Concurrent</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WebVPN</td>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td>Totals</td>
<td>2</td>
<td>13</td>
</tr>
</tbody>
</table>

Tunnels:

<table>
<thead>
<tr>
<th>WebVPN</th>
<th>Active</th>
<th>Cumulative</th>
<th>Peak Concurrent</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>13</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>SSL-Tunnel</td>
<td>1</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Totals</td>
<td>3</td>
<td>17</td>
<td></td>
</tr>
</tbody>
</table>
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.

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 can't 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

<table>
<thead>
<tr>
<th>Installation Method</th>
<th>Remote User Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active X</td>
<td>Admin Privileges (privi.)</td>
</tr>
<tr>
<td>Microsoft Java VM*</td>
<td>Power-User Privi.</td>
</tr>
<tr>
<td>Sun Java VM*</td>
<td>Any User</td>
</tr>
<tr>
<td>Exe</td>
<td>Any User with Execution Privi.</td>
</tr>
</tbody>
</table>

* VM = Virtual Machine
Cisco Secure Desktop
Installation of CSD on ASA

[Image of a Cisco ASDM 6.2 for ASA interface showing the Secure Desktop Manager: Setup window with fields for Location, Enable Secure Desktop, and an Upload Image window with file paths for Local File Path and Flash File System Path.]
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
To Configure the Flow of CSD Checking
Start by Clicking on the + Sign.
This Will Pull Up a Selection Box.
These Are the Types of Checks CSD will Check for.
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.
CSD Configuration (Cont.)

Create a Registry Check for a Unique Value.
Create a Subsequence if Different Requirements Are Needed for Multiple Groups/Departments.
Make Sure the Default Success Value of a Subsequence Is Changed to Reflect the Correct Value. If not the Login Will Fail.
Notice that when the value is changed to a location the value is added to location settings. Make sure the location settings are configured.
CSD Configuration (Cont.)

ASDM

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
- Default

Keystroke Logger & Safety Checks

- [ ] Check for keystroke loggers

List of Safe Modules:

- [ ] Check for tool simulations

Apply All  Reset All
CSD Configuration (Cont.)

ASDM

Remote Access VPN

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

Cache Cleaner

- Launch hidden URL after installation
- Show success message at the end of successful installation
- Launch cleanup upon timeout based on inactivity
- 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)
CSD Configuration (Cont.)

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:
CSD Configuration (Cont.)

**ASDM**

- Secure Desktop General
  - Secure Desktop Settings
    - 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
CSD Configuration (Cont.)
CSD Configuration (Cont.)

ASDM

Remote Access VPN
- 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

Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Secure Desktop Manager > Mac and Linux...

Mac and Linux Cache Cleaner

- 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)

Apply All  Reset All
The Configurations Above Are the Three Types of Configurable Options—Registry, File, and Process.

Endpoint Assessment Gives the Ability to Check/Enforce AV, AS, and Firewall Software for CSD. The Advanced Endpoint Assessment Option Will Be a Licensed Feature for Release.
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
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.)

```javascript
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

- Clientless SSL VPN
  - Controlled access to specific resources and applications

Mobile Workers
- Easy access to corporate network resources

Clientless SSL VPN

Roamers
- Seamless access to applications from unmanaged endpoints

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-compliant end systems or “Terminate”
Dynamic Access Policy

DAP Configuration on ASDM

Add Dynamic Access Policy

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

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

Add | Edit | Delete


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

Action: Continue | Terminate

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

User Message:
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.
## Dynamic Access Policy

### DAP—AAA Configuration Attribute Names

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Attribute Name</th>
<th>Source</th>
<th>Value</th>
<th>Max String Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>aaa.cisco.memberof</td>
<td>AAA</td>
<td>String</td>
<td>128</td>
<td>Memberof value</td>
</tr>
<tr>
<td></td>
<td>aaa.cisco.username</td>
<td>AAA</td>
<td>String</td>
<td>64</td>
<td>Username value</td>
</tr>
<tr>
<td></td>
<td>aaa.cisco.class</td>
<td>AAA</td>
<td>String</td>
<td>64</td>
<td>Class attribute value</td>
</tr>
<tr>
<td></td>
<td>aaa.cisco.ipaddress</td>
<td>AAA</td>
<td>Number</td>
<td>-</td>
<td>Framed-ip address value</td>
</tr>
<tr>
<td></td>
<td>aaa.cisco.tunnelgroup</td>
<td>AAA</td>
<td>String</td>
<td>64</td>
<td>Tunnel-group name</td>
</tr>
<tr>
<td>LDAP</td>
<td>aaa.ldap.&lt;label&gt;</td>
<td>LDAP</td>
<td>String</td>
<td>128</td>
<td>LDAP attribute value pair</td>
</tr>
<tr>
<td>RADIUS</td>
<td>aaa.radius.&lt;number&gt;</td>
<td>RADIUS</td>
<td>String</td>
<td>128</td>
<td>Radius attribute value pair</td>
</tr>
</tbody>
</table>
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
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
## DAP Posture Assessment

### Capability by Connection Protocol

<table>
<thead>
<tr>
<th>Client Access Method</th>
<th>Host Scan</th>
<th>Vault</th>
<th>NAC Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco VPN Client</td>
<td>No</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco AnyConnect VPN Client</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Clientless SSL</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
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

Remote User
Corporate Managed Machine

Employee at Home
Non-Corporate Machine

Contractors
Extranet Machine

ASA (inside)
192.168.30.0/24

ASA (DMZ)
192.168.70.3

Corporate Email
.25

SSH
VNC
.4

RDP

Corporate Managed Machine

Extranet Machine

Employee at Home

Remote User
Configuration Steps

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

A VPN group is a collection of user-oriented authorization attributes/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.

To define authorization attributes from an LDAP server, you must use an LDAP attribute map.
Configuring Tunnel Groups (cont)
Configuring Group URLs

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.

**Group URLs**

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

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

Use the decision tree below to create prelogin policies. Click the + symbol to check 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."

Select the type of check that you would like to insert:

- Registry Check

Click Add.
Configuring CSD Policies (cont)

Use the decision tree below to create prelogin policies. Click the + symbol to check if 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."

Key Path: \HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CCM Agent\Exe
- Exists
- Does Not Exists
- DWORD value
- String contains
- Case Sensitive

Apply All   Reset All
Configuring CSD Policies (cont)

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."

- Start
- Registry Check
  - Success
    - Employee_Access
  - Failure
    - Login Denied

Label: Non_CorpContractor_Access

Update Cancel

Apply All Reset All
Configuring CSD Policies (cont)

Privacy Protection

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
Configuring CSD Policies (cont)
Configuring DAP

Add Dynamic Access Policy

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.

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

AAA Attribute | Operation/Value
---|---
daas tunnelsgroup | Employees

and the following endpoint attributes are satisfied.

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

Advanced

Access/Authorization Policy Attributes:
Configure/access/authorization attributes for this policy. Attribute values specified here will override settings in the group-policy hierarchy. The resulting VRF authorization policy is an aggregation of DAP attributes that are not specified in DAP.

Add Endpoint Attribute

Endpoint Attribute Type: Registry

- Exists
- Does not exist

Endpoint ID: REG
HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Altiris Agent\EnableNotifications

- Value: dword = 1
- Caseless

OK Cancel Help
Configuring DAP (cont)

The image shows a configuration screen for a Dynamic Access Policy (DAP) policy. The policy is named `Employees_no_corp` and has a description indicating it is for employees with no corporate assets. The ACL Priority is set to 16.

### Selection Criteria

- **AAA Attribute**:
  - `cisco.tunnelgroup` is selected with a value of `Employees`.

- **Endpoint ID**:
  - `registry.REG` is selected with the following attributes:
    - `exists = true`
    - `type = dword`
    - `value = 0`

### Access/Authorization Policy Attributes

The page provides options for actions and user messages. The actions are `Continue` and `Terminate`. The user message field is empty.

- **Action**:
  - Options: `Continue`, `Terminate`.

- **User Message**:
  - The message field is empty.

The screen also includes an `Advanced` section, which is not detailed in the image.
Configuring DAP (cont)
Configuring Bookmarks
Example 1: Employee Access with Corporate PC
Topography

Remote User
Corporate Managed Machine

ASA

192.168.30.0/24
(inside)

(RDP)

192.168.70.3

(inside)

192.168.30.0/24

SSH VNC

Corporate Email

.25

.4
Employee Access – Corporate PC

ciscolivevpn.cisco.com/employee

Username: employee1
Password: **********
Employee Access – Corporate PC

[Image of Cisco AnyConnect VPN Client window showing connection details and statistics]

- Connection State: Connected
- Client Address: 10.10.10.1
- Server Address: 172.18.124.224
- Client Address (IPv6): Disabled
- Time Connected: 00:00:16

[Image of Cisco AnyConnect VPN Client: Statistics Details window]

- Connected
- All Traffic
- 00:01:03
- 5844
- 534
- 83
- 1
- 4
- 3

VPN session established to ciscollivevpn.cisco.com/employee.
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

```javascript
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";

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";
```

CSD Policy applied for user

Endpoint Registry check
Employee Access – Corporate PC

```javascript
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";
```

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

AV identified through Host Scan process
DAP record selected for the user
Example 2: Employee Access with Non-corporate PC
Employee at Home
Non-Corporate Machine

Corporate Email
.25

SSH
VNC
.4

ASA
192.168.30.0/24
(inside)

(DMZ)

RDP
192.168.70.3

192.168.168.70.
3

© 2009 Cisco Systems, Inc. All rights reserved.
Employee Access – Non-corporate PC

ciscolivevpn.cisco.com/employee
Employee Access – Non-corporate PC
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 = 0
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]

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 Authentication Accepted

User info collected through DAP
Employee Access – Non-corporate PC

```javascript
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";

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";
```
Employee Access – Non-corporate PC

```javascript
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";
```

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
Example 3: Contractor Access
Topology

Contractors
Extranet Machine

ASA
192.168.30.0/24
(inside)

DMZ
192.168.70.3

RDP

Corporate Email
.25

SSH
VNC
.4
Contractor Access

ciscollivevpn.cisco.com/contractors
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 = 0
  Contractors
  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";
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

```javascript
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";
```

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

AV/FW information collected through host scan

DAP record applied to user
Q&A