

What You Make Possible



CCNP Security: Securing Networks with ASA VPNs - CCNP Security Exam Preparation (VPN 2.0) BRKCRIT-8163

Agenda

- Overview of CCNP Security VPN v2.0 Exam
- VPN v2.0 Topics
 - ASA VPN Architecture and Fundamentals
 - IPsec Fundamentals
 - IPsec Site to Site
 - IPsec Remote Access
 - AnyConnect SSL VPN
 - Advanced VPN Concepts (added for reference at the end of the deck)
 - Clientless SSL VPN (added for reference at the end of the deck)
- Q&A

Overview of the CCNP Security



Disclaimer / Warning

- This session will strictly adhere to Cisco's rules of confidentiality
- We may not be able to address specific questions
- If you have taken the exam please refrain from asking questions from the exam—this is a protection from disqualification
- We will be available after the session to direct you to resources to assist with specific questions or to provide clarification

CCNP Security Certified Means...

- All four CCNP Security exams required. No elective options.
- Some legacy CCSP exams qualify for CCNP Security credit. See FAQ:

<https://learningnetwork.cisco.com/docs/DOC-10424>

Exam No	Exam Name
642-637	Securing Networks with Cisco Routers and Switches (SECURE)
642-627	Implementing Cisco Intrusion Prevention System (IPS)
642-617	Deploying Cisco ASA Firewall Solutions (FIREWALL)
642-648	Deploying Cisco ASA VPN Solutions (VPN)

642-648 VPN v2.0 Exam

- Approximately 90 minute exam
- 60-70 questions
- Register with Pearson Vue
 - <http://www.vue.com/cisco>
- Exam cost is \$200.00 US
 - <https://learningnetwork.cisco.com/docs/DOC-12825>

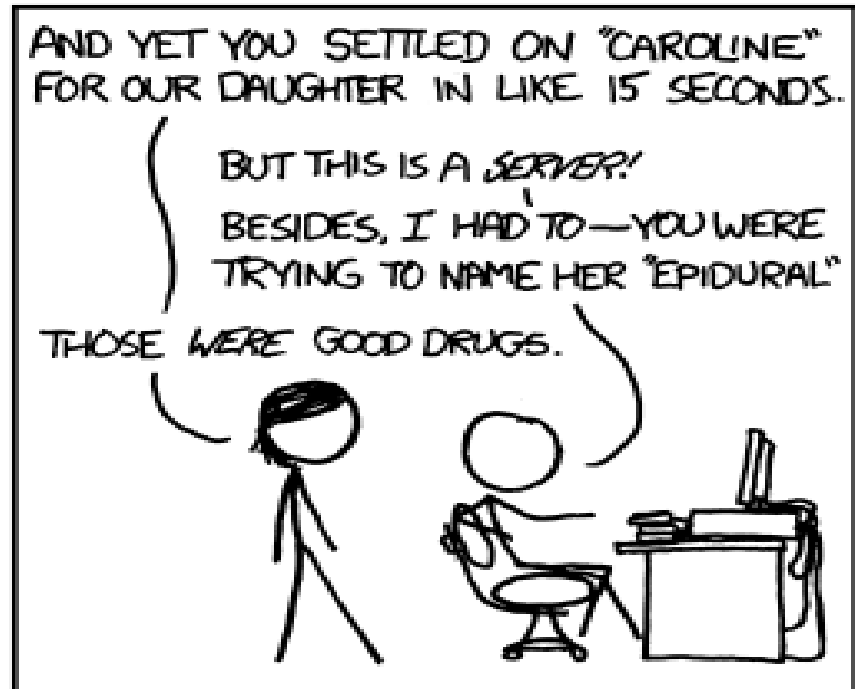
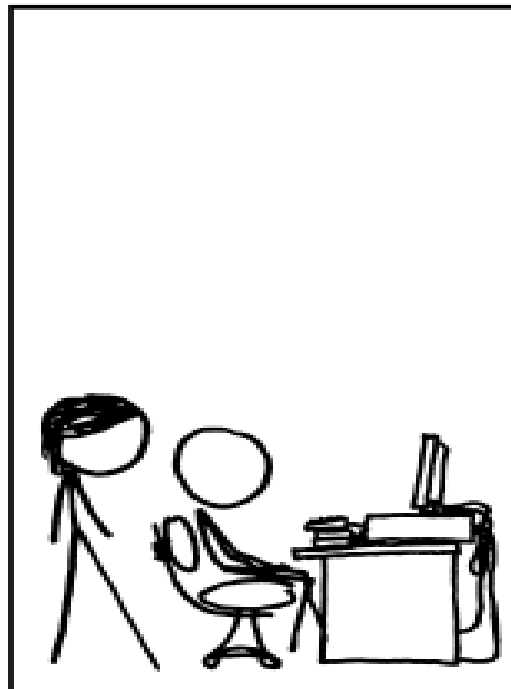
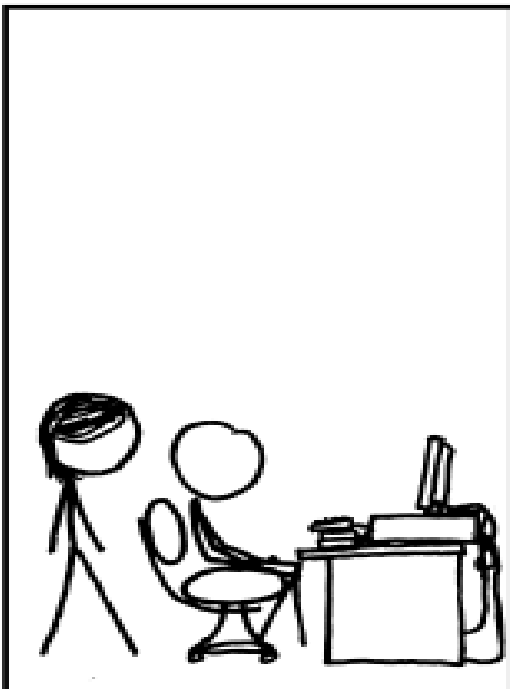
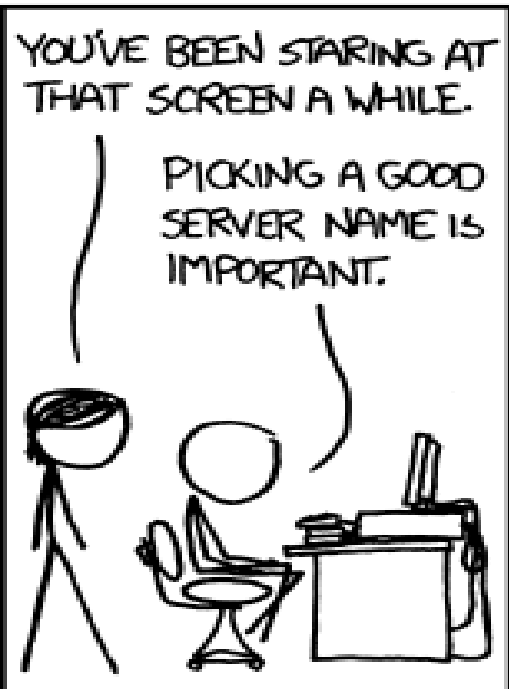
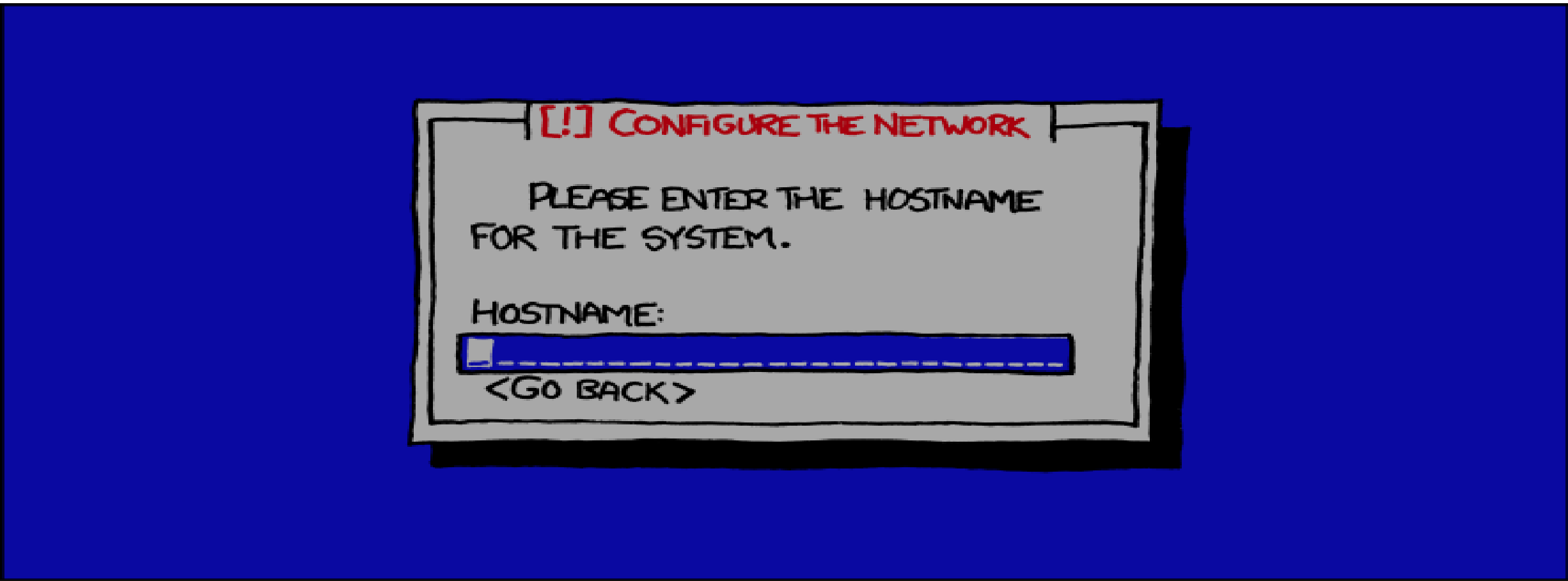
Preparing for the VPN v2.0 Exam

- Recommended reading
 - CCNP Security VPN 642-648 Official Cert Guide (2012)
 - CCSP books in the interim
 - Cisco ASA 8.2 Configuration Guide
- Recommended training via Cisco Learning Partners
 - Deploying Cisco ASA VPN Solutions
- Cisco learning network
 - www.cisco.com/go/learnnetspace
- Practical experience
 - Real equipment
 - ASDM in demo mode

Session Notes

- Session and exam are based on **ASA 8.2 and ASDM 6.2** software even though 8.3 and 8.4 are available on Cisco.com
- This session covers most topics but cannot depth of each topic
- Proper study and preparation is essential
- Spend time with the ASA Security Device Manager (ASDM) demo

Command Line Quiz!



Cisco ASA Architecture and VPN Fundamentals



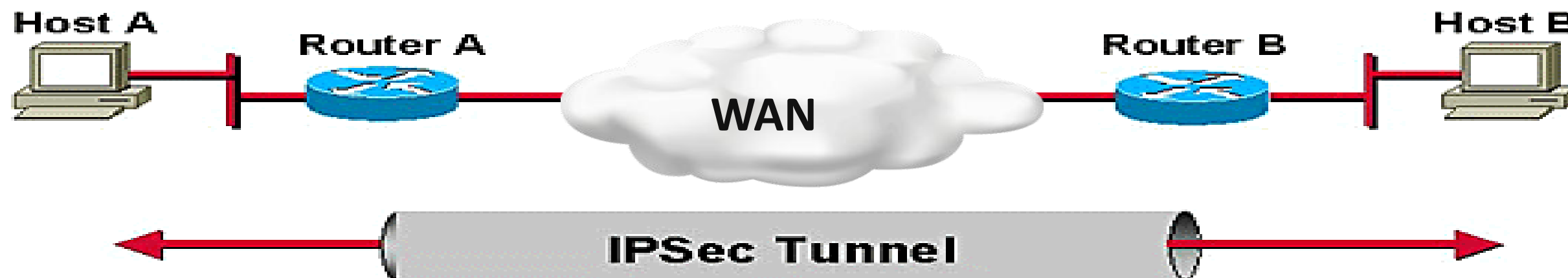
ASA Architecture

- ASA VPN Overview
- ASA Design Considerations
- AAA and PKI Refreshers
- VPN Configuration Basics

Virtual Private Networks (VPNs)

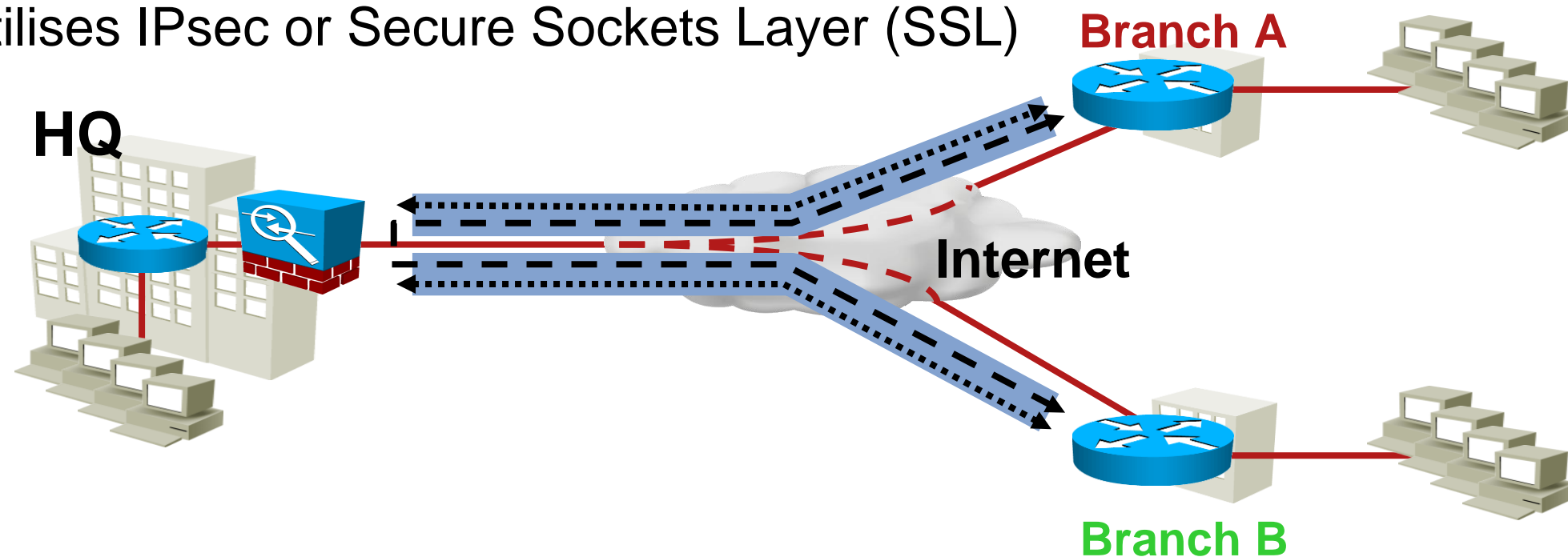
- Virtual Private Networks (VPNs) are a way to establish private connections over another network
- VPN Capabilities

Confidentiality	Prevent others from reading data traffic
Integrity	Ensure data traffic has not been modified
Authentication	Prove identity of remote peer and packets
Anti-replay	Prevent replay of encrypted traffic



ASA Virtual Private Networks (VPNs)

- Site-to-Site VPN
 - Connects two separate networks using two VPN gateway devices such as an ASA
 - Utilises IPsec
- Remote Access VPN
 - Connects single user to a remote network via gateway such as an ASA
 - Utilises IPsec or Secure Sockets Layer (SSL)



Remote-Access VPN

Home Office



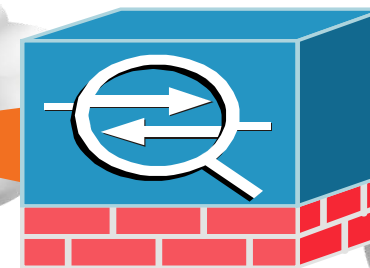
Client Based Tunnel

Computer Kiosk

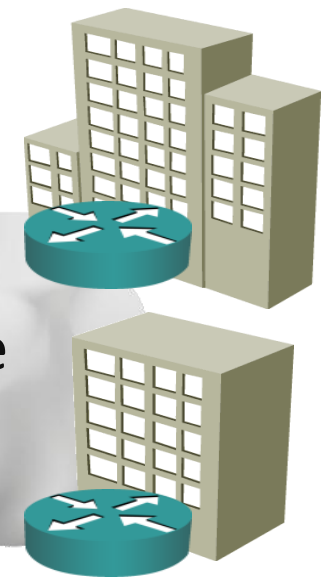


Clientless Tunnel

ISP



Corporate Office



- Client-based VPN

- Remote access using an installed VPN client (VPN Client or AnyConnect)

- Permits “full tunnel” access

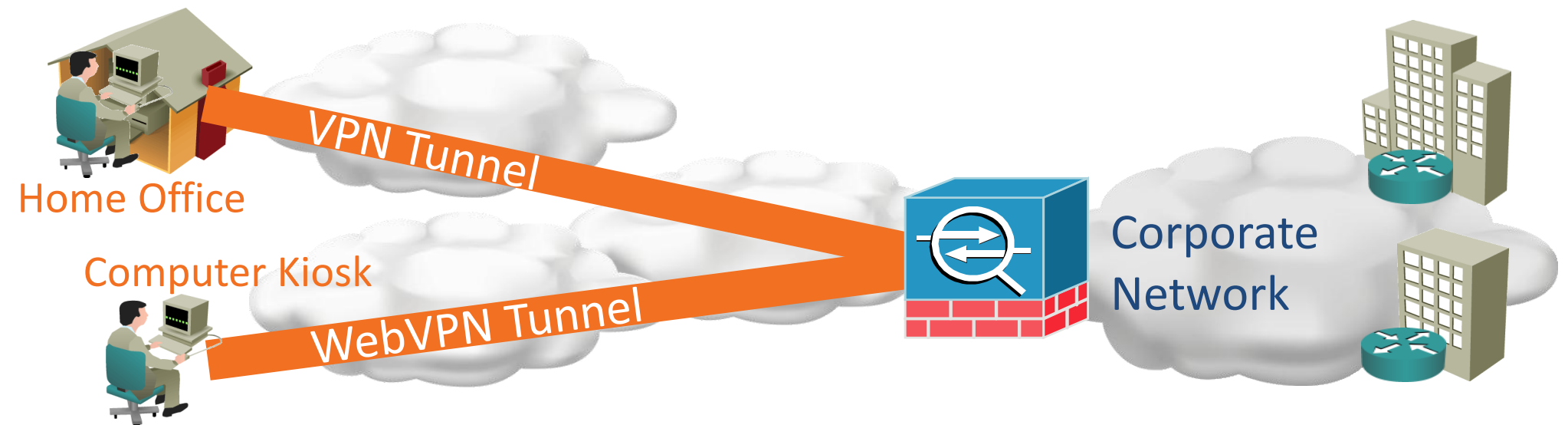
- Clientless VPN

- Remote access through a web browser that leverages the browser’s SSL encryption for protection

- Permits limited access but no footprint required

Choosing Remote Access VPN Method

- IPsec VPN
 - Traditional IPsec access
 - Cisco VPN Client
- AnyConnect SSL VPN
 - Recommended next generation remote access – Windows 7 supported
 - SSL VPN based
 - Full tunnel capabilities similar to IPsec VPN
 - Cisco Secure Desktop
- Clientless SSL VPN (WebVPN)
 - Recommended for thin, flexible access from any computer
 - Web browser based using SSL encryption – no software required
 - Permits network access via HTTP/S, plug-ins, and port forwarding
 - Cisco Secure Desktop



Remote Access VPN Licensing

- IPsec VPNs require no license
- AnyConnect Essentials license
 - Platform license enabling max number of SSL VPN sessions
 - Permits use of AnyConnect full tunnels – not Cisco Secure Desktop (CSD) or Clientless SSL VPN
- AnyConnect Premium license
 - User count based and limited to platform session max
 - Enables all AnyConnect features including full tunnel, CSD, and Clientless
- AnyConnect Mobile license (requires Essentials or Premium)
 - Enables iPhone and Windows Mobile clients
- Advanced Endpoint Assessment (requires Premium)
 - Enables host remediation with Cisco Secure Desktop
- AnyConnect Shared license
 - Enables SSL VPN Premium license pooling amongst multiple ASAs
- AnyConnect Flex license
 - Enables 60-day SSL VPN Premium licenses for business continuity planning
- <http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html>

ASA License Keys

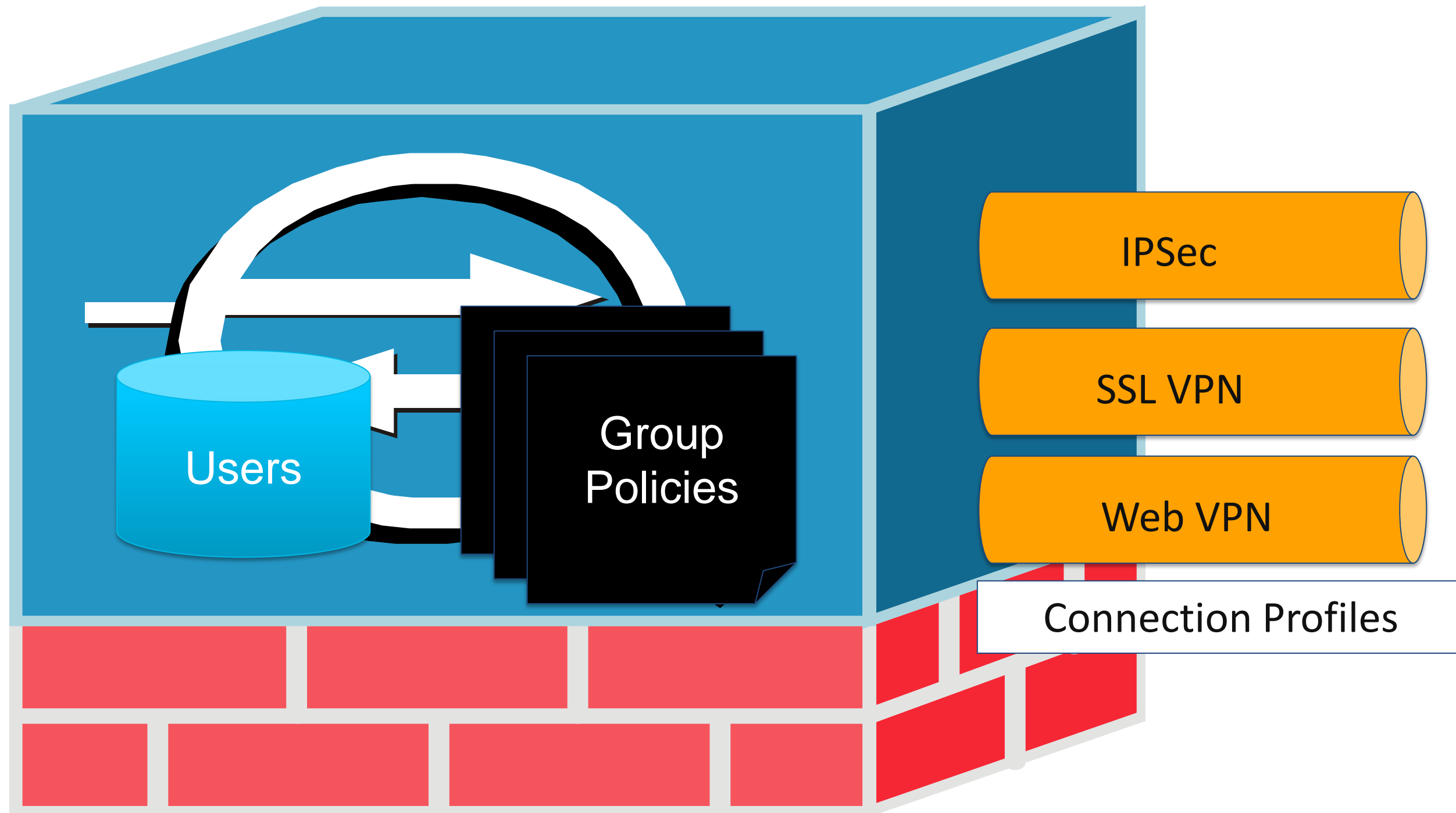
- Two types – Permanent and Temporary
- Three rules to remember
 1. Only one of each type can be active at a time
 2. Higher value from either license is used – NOT combined or additive
 3. Loading a Permanent Key overwrites existing Temporary
 - Re-enter the Temporary Key to activate temporary license features again
- Examples
 - Base license + 25 SSLVPN (P) + 10 SSLVPN (P) = **10 SSLVPN (P)**
 - Base license + 10 SSLVPN (P) + 25 SSLVPN (T) = **25 SSLVPN (T)**
 - Base license + 25 SSLVPN (T) + 10 SSLVPN (P) = **10 SSLVPN (P)**

<http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html>

VPN Configuration



VPN Configuration Components



VPN Configuration Components

- User: Individual that will be instantiating the VPN
- Group Policy: Settings for a group of users
- Connection Profile: Defines a VPN service
- <http://www.cisco.com/en/US/docs/security/asa/asa82/config>

```
group-policy VPN_POLICY internal
group-policy VPN_POLICY attributes
  dns-server value 192.168.1.10
  vpn-filter value VPN_IN_ACL
  ...

tunnel-group VPN_GROUP type remote-access
tunnel-group VPN_GROUP general-attributes
  address-pool VPN_POOL
  authentication-server-group (inside) ACS
  ...
```

VPN Group Policy

- Internal (ASA) or External (RADIUS)
- Sample of various settings:
 - WINS, DNS, DHCP, web proxy settings
 - VPN access hours, idle timeout, network filter, permitted VPN protocols
 - Split tunnelling
- Default Group Policy is called **DfltGrpPolicy**. Can be modified but NOT deleted.
- Settings are inherited:
 - User ==> Connection Profile's Group Policy ==> Default Group Policy

External Group Policy

- Stored on a RADIUS server as a special user account
- RADIUS user includes Vendor-Specific Attributes (VSAs) for Group Policy settings
- Group Policy configuration includes the RADIUS username and password

```
group-policy VPN external server-group ACS password s3cr3t
```

VPN Group Policy

Add Internal Group Policy

General

- Servers
- Advanced
 - Split Tunneling
 - IE Browser Proxy
 - SSL VPN Client
 - Login Setting
 - Key Regeneration
 - Dead Peer Detectio
 - Customization
 - IPsec Client
 - Client Access Rules
 - Client Firewall
 - Hardware Client

Name: GroupPolicy1

Banner: Inherit

Address Pools: Inherit

IPv6 Address Pools: Inherit

More Options

Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec L2TP/IPsec

IPv4 Filter: Inherit

IPv6 Filter: Inherit

NAC Policy: Inherit

Access Hours: Inherit

Simultaneous Logins: Inherit

Restrict access to VLAN: Inherit

Connection Profile (Tunnel Group) Lock: Inherit

Maximum Connect Time: Inherit Unlimited minutes

Idle Timeout: Inherit Unlimited minutes

On smart card removal: Inherit Disconnect Keep the connection

Find:

VPN Connection Profile

- Formerly called Tunnel Group. Command line still uses **tunnel-group** terminology.
- Core VPN Service Attributes
 - VPN Type (IPsec Site-to-Site, IPsec Remote Access, SSL VPN, Clientless)
 - Authentication, authorisation, and accounting servers
 - Default group policy
 - Client address assignment method
 - VPN type specific attributes for IPsec and SSL VPN
- Default Connection Profiles. They can be modified but NOT deleted.
 - DefaultRAGroup – Remote Access connections
 - DefaultWEBVPNGroup – Clientless SSL VPN connections
 - DefaultL2LGroup – IPsec site-to-site connections
- Settings are inherited

VPN Connection Profile

Add SSL VPN Connection Profile

Basic

- Advanced
 - General
 - Client Addressing
 - Authentication
 - Authorization
 - Accounting
 - SSL VPN
 - Secondary Authentication

Name: TunnelGroup1

Aliases:

Authentication

Method: AAA Certificate Both

AAA Server Group: LOCAL

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools:

Client IPv6 Address Pools:

Default Group Policy

Group Policy: DfltGrpPolicy

(Following field is an attribute of the group policy selected above.)

Enable SSL VPN Client protocol

Find:

AAA and PKI Refreshers



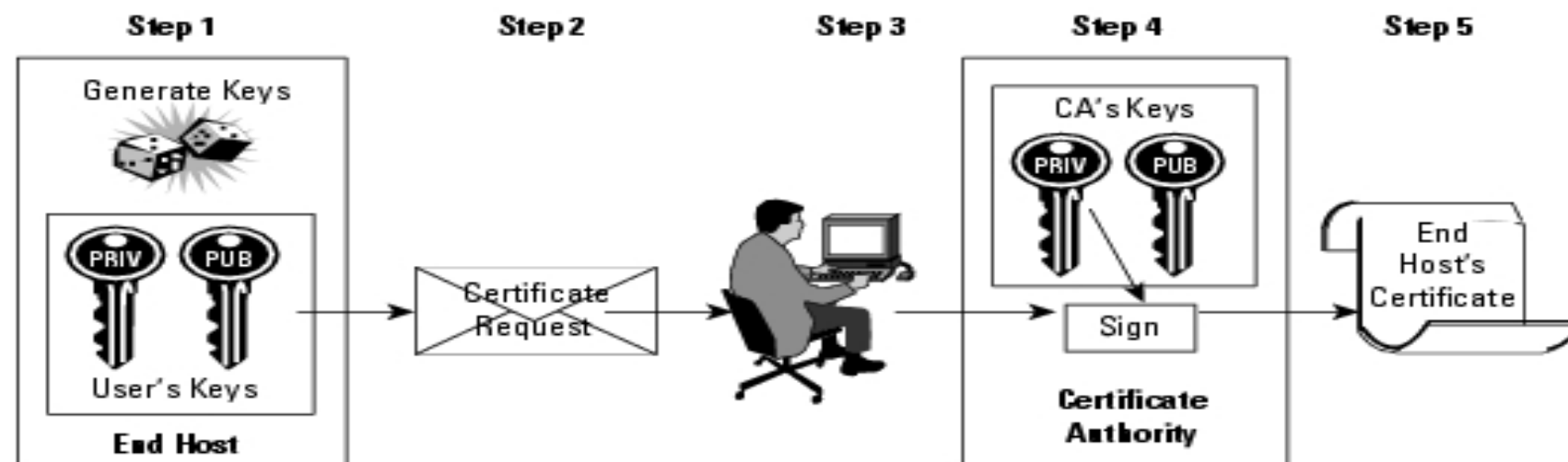
AAA Refresher

- Authentication, Authorisation, and Accounting (AAA)
 - Authentication: Proving the identity of the user
 - Authorisation: Controlling the permissions of the user
 - Accounting: Logging the actions of the user
- AAA servers are used to perform one or more of the AAA functions
 - Supported AAA servers include RADIUS, TACACS+, RSA/SDI, NT, Kerberos, LDAP, HTTP Forms, and LOCAL database

```
aaa authentication http console ACS LOCAL
aaa authentication ssh console LOCAL
aaa authorization exec LOCAL
aaa accounting enable console ACS
aaa accounting ssh console ACS
```

PKI Refresher

- Public Key Infrastructure uses Digital Certificates and public key cryptography
- Encryption with the public key is decrypted with the private key and vice versa
- Each device has a public key, private key, and certificate signed by the Certificate Authority
- **Pre-Shared Key (PSK) deployments do not scale (symmetric keys)**



ASA PKI SCEP Configuration

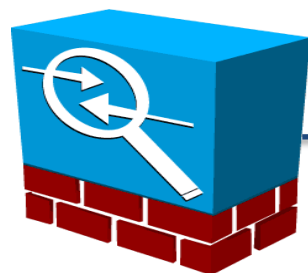
```
domain-name birdland.local

! ---- Create keys
crypto key generate rsa general-keys modulus 2048

! ---- Configure Certificate Authority and SCEP URL
crypto ca trustpoint PKI_CA
  enrollment url http://ca_server:80/certsrv/mscep/mscep.dll

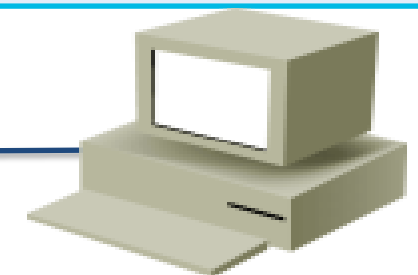
! ---- Retrieve CA certificate
crypto ca authenticate PKI_CA

! ---- Submit certificate request to CA
crypto ca enroll PKI_CA
```



ASA

Simple Certificate Enrollment Protocol



CA

Cisco live!

PKI Refresher

- Validation steps
 - Check validity of the certificate based on **date/time** and certificate attributes
 - Check the certificate using the stored Certificate Authority certificate
 - (optional) Check the Certificate Revocation List (CRL) or
 - Online Certificate Status Protocol (OCSP)
 - to ensure certificate is not revoked
- Enrollment options
 - Manually enroll ASA and endpoints by creating certificates and loading them
 - ASA can also utilise SCEP to enroll directly with the CA
 - **VPN Clients** can enrollment online with the ASA using Simple Certificate Enrollment Protocol (SCEP) proxy
- ASA Certificate Guide
 - http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/cert_cfg.html

Section Quiz - Alphabet Soup!

- Expand these Acronyms!

–ASA

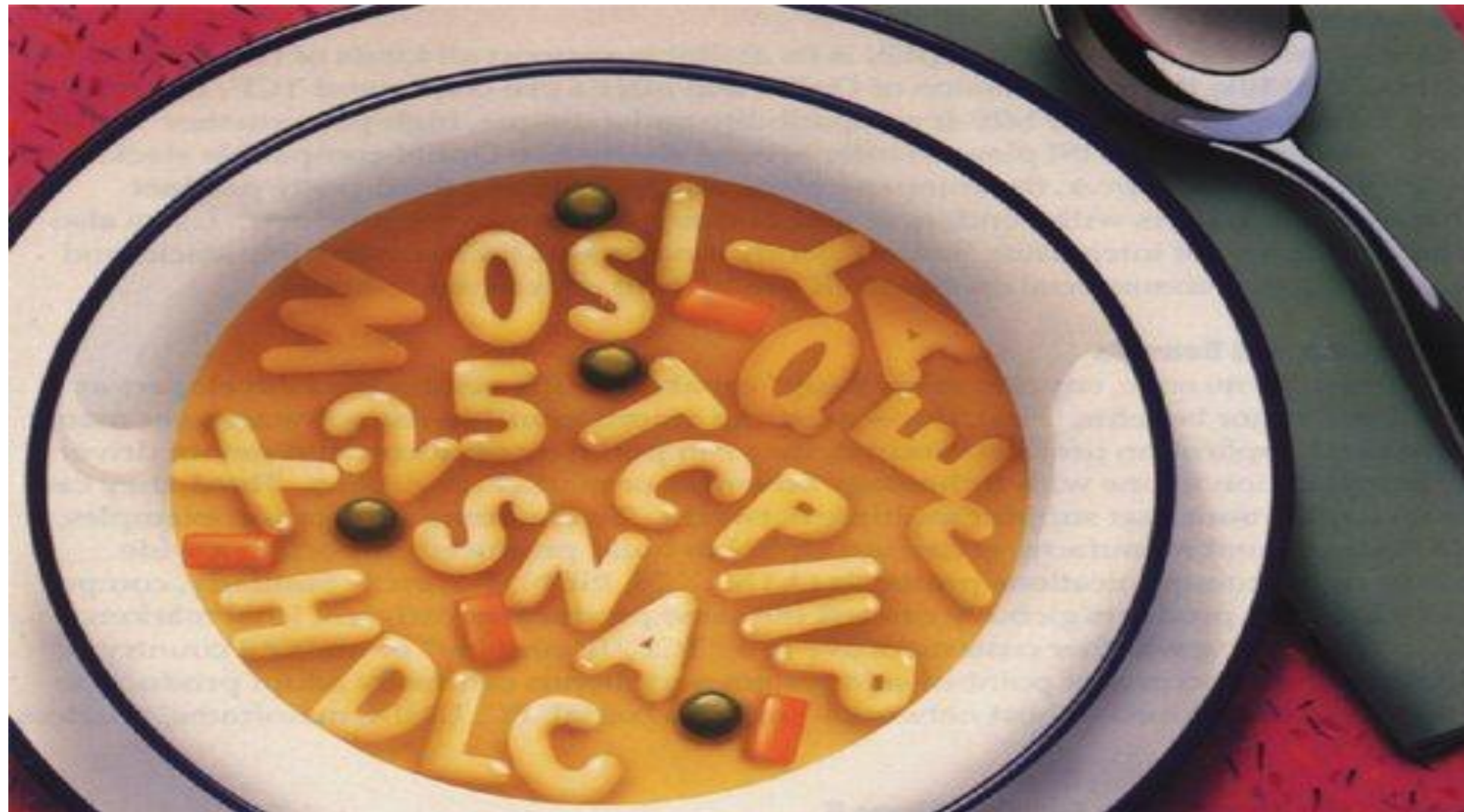
–SSL

–PSK

–PKI

–AAA

–VPN



IPSec Fundamentals



IPsec Connection Overview



1. Interesting Traffic
2. Phase 1 (ISAKMP)
3. Phase 1.5 (ISAKMP)
4. Phase 2 (Ipsec)
5. Data Transfer
6. IPsec Tunnel Termination

IPsec Connection Overview



1. Match Interesting Traffic

Access Control List (ACL) defines matching source/destination addresses to protect

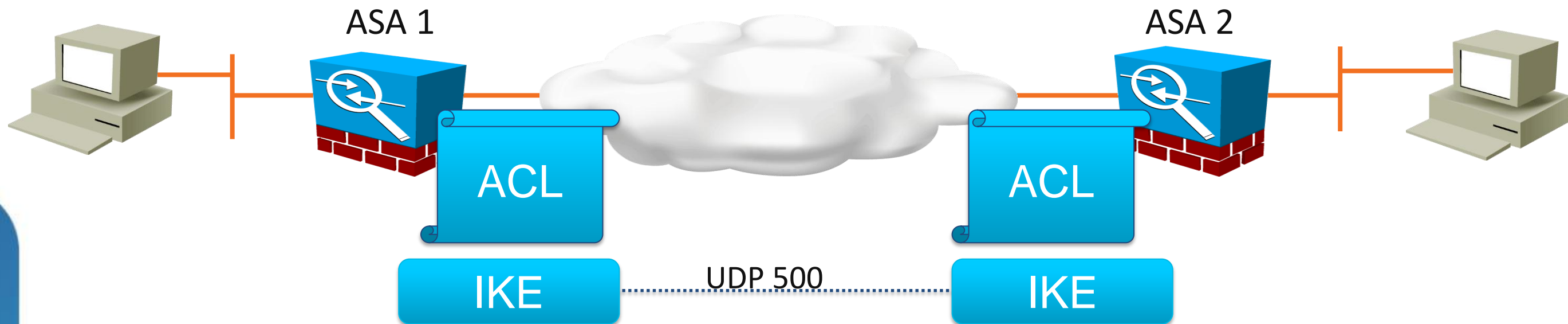
Both sides have mirrored ACLs

IKE kicks off when a packet matches the ACL

```
! ---- Interesting Traffic ACL
access-list VPN_ACL extended permit ip <x.x.x.x> 255.255.255.0 <x.x.x.x.x>
255.255.255.0

! ---- Crypto map creation. Bind crypto settings together.
crypto map VPN_MAP 10 match address VPN_ACL
```

IPsec Connection Overview

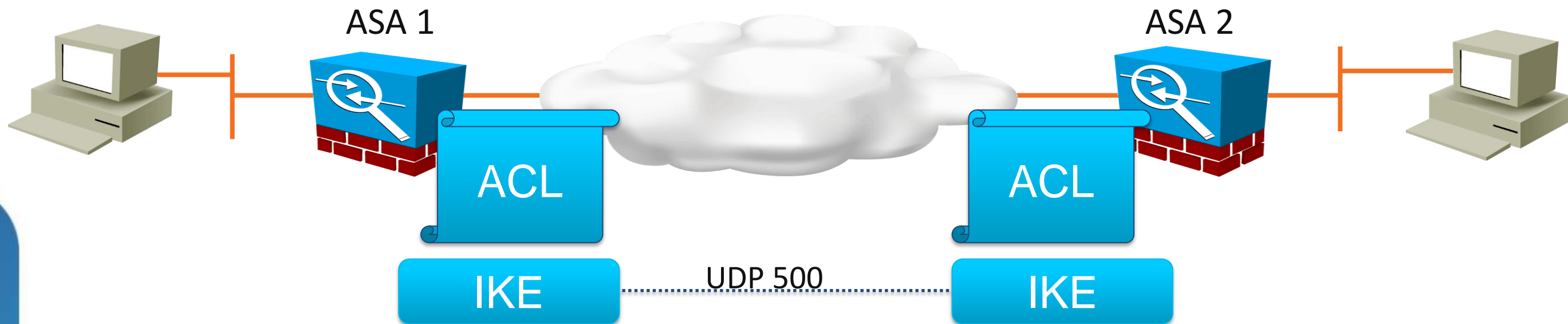


2. Phase 1 – ISAKMP

- Main Mode or Aggressive Mode exchange
- ISAKMP policies matched
- Diffie-Hellman exchange – Creates shared key
- Identities exchanged and authenticated
- ISAKMP Security Association (SA) created
- Negotiate Phase 2 parameters

```
crypto isakmp policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
```

IPsec Connection Overview



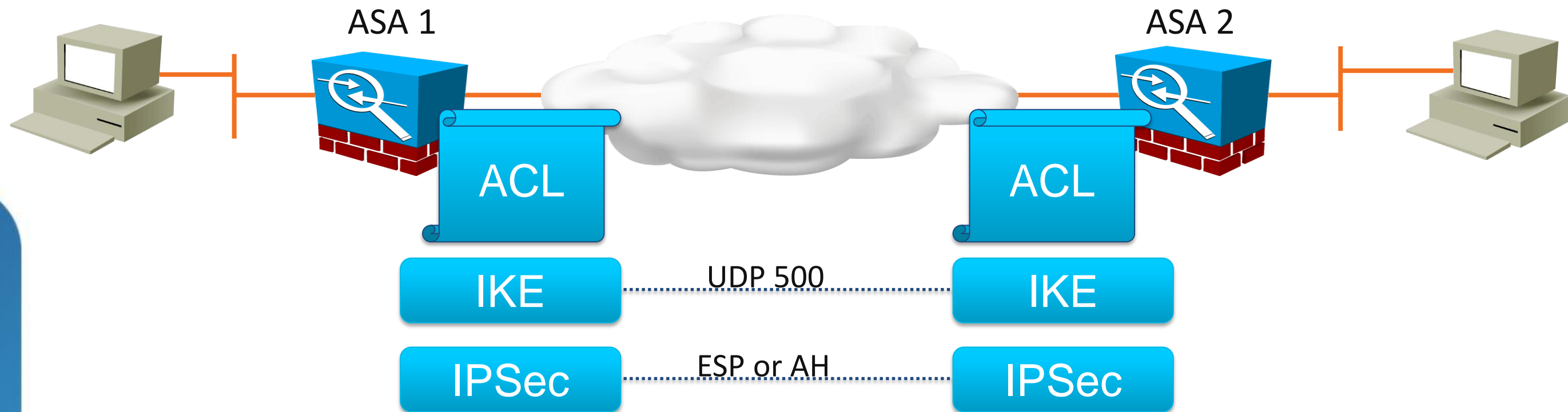
3. Phase 1.5 – Xauth and mode config

Additional user authentication

Client configuration – IP Address, DNS Server, etc

```
tunnel-group VPN_REMOTE_ACCESS general-attributes
! ---- Phase 1.5 Xauth
      authentication-server-group ACS
! ---- Phase 1.5 mode config
      address-pool clientpool
      default-group-policy VPN_GROUP_POLICY
```

IPsec Connection Overview



4. Phase 2 – IPsec Security Associations (SA)

SA is a unidirectional data channel

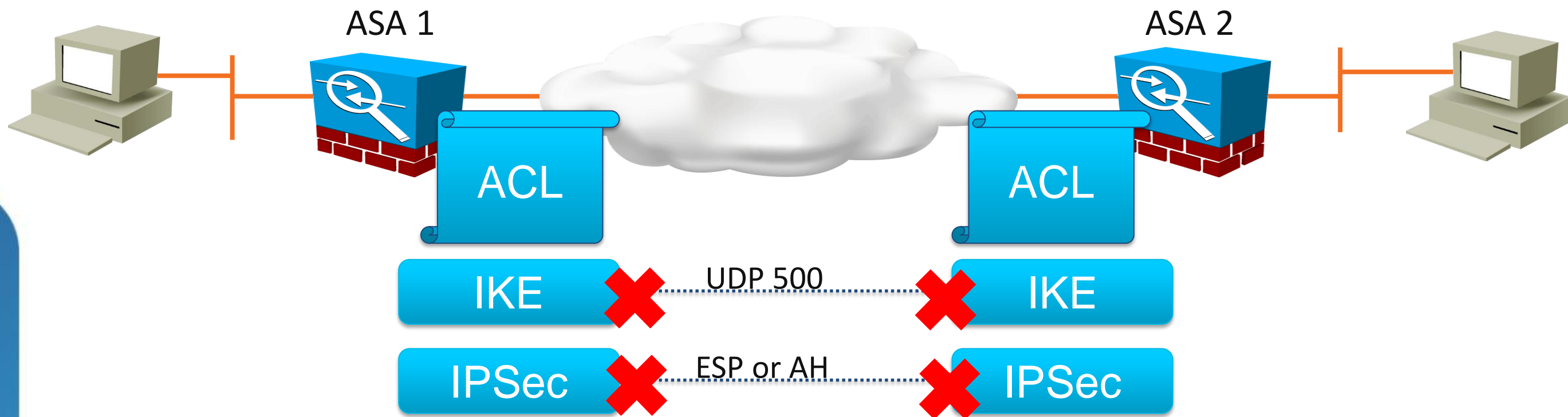
Negotiated encryption and hashing

Re-keyed after time or byte limit

```
! ---- IPsec Transform Set. Encryption and Hashing options.  
crypto ipsec transform-set VPN_PHASE2 esp-des esp-md5-hmac
```

```
! ---- Crypto map creation. Bind crypto settings together.  
crypto map VPN_MAP 10 set transform-set VPN_PHASE2
```

IPsec Connection Overview



5. Data transfer over IPsec SAs

6. Tunnel termination

Lack of interesting traffic

Peer quits responding

Negotiated encryption and hashing

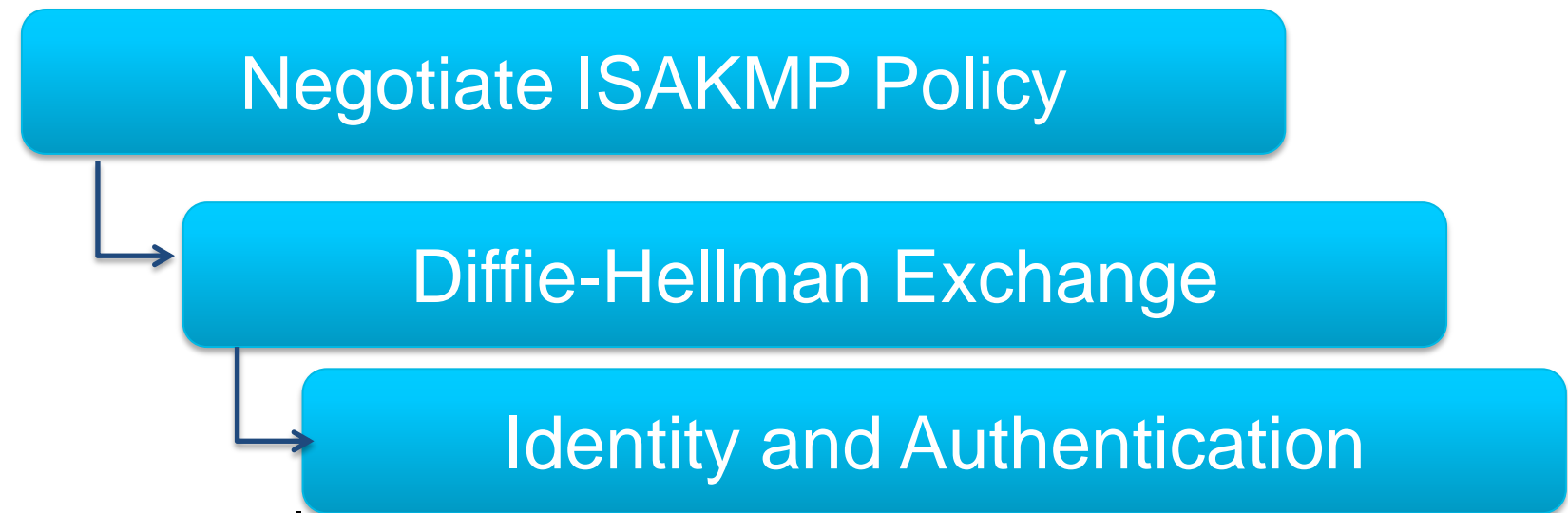
Re-keyed after time or byte limit

```
group-policy DfltGrpPolicy attributes
  vpn-idle-timeout <minutes>
  vpn-session-timeout <minutes>
```

IKE Details

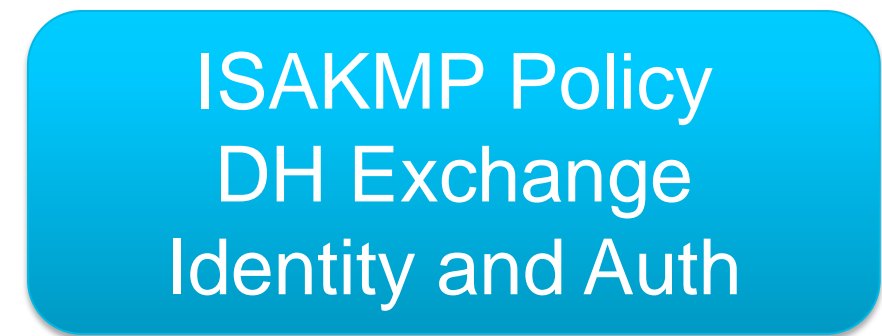
- Main Mode

- Three 2-way exchanges (6 messages) for:
 - ISAKMP policy
 - Diffie-Hellman exchange
 - Verifying the IPSec peer's identity
- Protects identities by exchanging them in secure tunnel



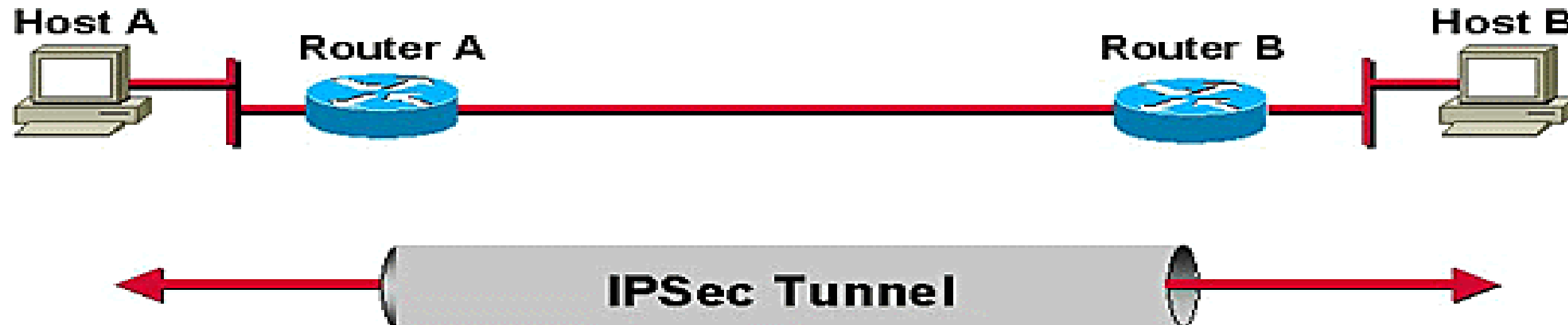
- Aggressive Mode

- Performs the 3 exchanges in a single exchange
- Faster than Main Mode due to less messages (3 total)
- Exposes identities
- 3 total exchanges
- **Required in some cases!** Dynamic peers with Pre-Shared Key (Easy VPN)



IPSec Details

- Phase 2 – Quick Mode
 - Exchange protected by Phase 1 IKE Security Association (SA)
 - Negotiates IPSec SA parameters
 - Creates IPSec SAs
 - Periodically renegotiates the IPSec SAs
 - (optional) Performs Diffie-Hellman exchange for Perfect Forward Secrecy (PFS)



IPSec Ports and Protocols

Protocol	Port	Purpose
Internet Key Exchange (IKE / ISAKMP)	UDP 500	IPSec Phase 1 key negotiation
Encapsulating Security Payload (ESP)	IP Protocol 50	IPSec Phase 2 encrypted payload
Authentication Header (AH)	IP Protocol 51	IPSec Phase 2 authenticated payload
NAT Traversal (NAT-T)	UDP 4500	Phase 1 and 2 UDP encapsulation when NAT is present
IPSec over TCP IPSec over UDP	TCP and UDP 10000	Used to bypass 3 rd party network issues with IKE, ESP, and AH by encapsulating IPSec in UDP or TCP packets
SSL VPN	TCP and UDP 443	Secure Sockets Layer (SSL) and Transport Layer Security (TLS) VPNs. DTLS uses UDP.

Phase 1 Configuration – Diffie-Hellman

Group	Key Length	Purpose
1	768-bit	Considered weak and no longer recommended.
2 (default)	1024-bit	Minimum strength required by VPN client.
5	1536-bit	Used to support larger key sizes of AES.
7	163-bit Elliptical	Weak algorithm meant for mobile devices. Deprecated.

! ISAKMP Policy Defaults

```
crypto isakmp policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
```

Debugging IPSec Connections

- Debugging commands
 - debug crypto isakmp sa (Phase 1 debugs)
 - debug crypto ipsec (Phase 2 debugs)
- Common IPSec VPN problems
 - http://www.cisco.com/en/US/products/ps6120/products_tech_note09186a00807e0aca.shtml
- IPSec debug guide
 - http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a00800949c5.shtml

IPSec Site-to-Site VPNs



IPSec Site-to-Site VPNs

- Site to Site VPN overview
- Site to Site VPN configuration
- Site to Site debugging

Site to Site VPNs



- Site-to-site VPNs are used to connect two sites together
- They are often used to connect a branch office to the central office

Site-to-Site IPsec Connection Creation

- Three methods for creation
 - Command line
 - ASDM with Connection Profiles and Group Policies
 - ASDM VPN Wizard
- Key configuration choices:
 - Peer IP Address
 - Authentication type (Pre-Shared Key or certificate)
 - IKE Policy (Phase 1)
 - IPsec Policy (Phase 2)
 - Interesting traffic ACL – Local and Remote networks

IPSec Wizard Configuration

The screenshot shows the 'VPN Wizard' window with the title 'VPN Tunnel Type (Step 1 of ...)'. On the left, there is a diagram of a network topology showing a 'Corporate Network' connected to an 'ISP' and a 'Home' network. Below the diagram is a photo of two people looking at a computer. The main area contains the following text and controls:

Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel.

This wizard creates basic tunnel configurations that you can edit later using the ASDM.

VPN Tunnel Type:

- Site-to-Site
- Remote Access

Site-to-Site VPN diagram: A 'Local' router icon is connected to an 'Internet' cloud, which is connected to a 'Remote' router icon.

VPN Remote Access diagram: A 'Local' laptop icon is connected to an 'Internet' cloud, which is connected to a 'Remote' router icon.

VPN Tunnel Interface:

Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Navigation buttons: < Back, Next >, Finish, Cancel, Help

IPSec Manual Configuration

Connection Profile
Group Policy

IPSec Config

Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles

Access Interfaces

Enable interfaces for IPsec access.

Interface	Allow Access
outside	<input type="checkbox"/>
DMZ	<input type="checkbox"/>
Guest	<input type="checkbox"/>
Internal-WLAN	<input type="checkbox"/>

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

+ Add Edit Delete

Name	IPsec Enabled	L2TP/IPsec Enabled	Authentication Server Group
HOME_SSL	<input type="checkbox"/>	<input type="checkbox"/>	LOCAL
DefaultRAGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LOCAL
Client-Anyconnect	<input type="checkbox"/>	<input type="checkbox"/>	LOCAL
SSLVPN	<input type="checkbox"/>	<input type="checkbox"/>	LOCAL
DefaultWEBVPGGroup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LOCAL

Apply Reset

mabernar 15 5/26/11 8:27:13 PM EDT



Site-to-Site VPN Configuration

1. Create interesting traffic ACL
2. Define an **ipsec-l2l** Connection Profile named as peer address
 - Set pre-shared key in **ipsec-attributes**
3. Create IKE policy with encryption, hashing, and authentication options
4. Create IPsec transform-set with encryption and hashing options
5. Create crypto map and associate with ACL, transform-set, and peer
6. Associate crypto map with outside interface
7. Configure NAT exemption for interesting traffic
8. Enable IKE on outside interface
9. Allow IPSec traffic in outside interface with **sysopt** command

Phase 1 Configuration – IKE / ISAKMP

```
! ---- Enable IKE on the outside interface
crypto isakmp enable outside

! ---- Create ISAKMP policy for Site-to-Site
crypto isakmp policy 10
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
```

Phase 2 Configuration – IPsec

```
! ---- Interesting Traffic ACL
access-list VPN_ACL extended permit ip <x.x.x.x> 255.255.255.0 <x.x.x.x.x> 255.255.255.0

! ---- IPsec Transform Set.  Encryption and Hashing options.
crypto ipsec transform-set VPN_PHASE2 esp-des esp-md5-hmac

! ---- Crypto map creation.  Bind crypto settings together.
crypto map VPN_MAP 10 match address VPN_ACL
crypto map VPN_MAP 10 set transform-set VPN_PHASE2
crypto map VPN_MAP 10 set peer <x.x.x.x>
crypto map VPN_MAP interface outside

! ---- Tunnel Group (aka Connection Profile) configuration
tunnel-group <x.x.x.x> type ipsec-l2l
tunnel-group <x.x.x.x> general-attributes
    ...
tunnel-group <x.x.x.x> ipsec-attributes
    pre-shared-key *

! ---- NAT Exemption NOT shown but is usually required

! ---- Allow IPsec traffic in without specifying in outside interface ACL
sysopt connection permit-ipsec
```

Debugging Site-to-Site Connections

- Ensure Phase 1 (ISAKMP) Policies match
- Ensure Phase 2 (IPSec) Transforms match
- Ensure crypto Access Control Lists match
- Ensure Pre-Shared Keys Match or Certificates are valid
 - **Ensure clocks are synchronised if using certificates**
- Ensure IPSec traffic can reach the ASA (**sysopt** command or ACL)
- Debugging commands
 - debug crypto isakmp sa (Phase 1 debugs)
 - debug crypto ipsec (Phase 2 debugs)

IPSec Remote Access VPN



IPSec Remote Access VPN

- Easy VPN Basics
- Easy VPN Certificate Authentication example
- Deploying Easy VPN Hardware Clients
- Deploying Easy VPN Server
- Easy VPN Debugging

Easy VPN Remote Access VPN

Home Office



IPsec Tunnel

Broadband
Provider

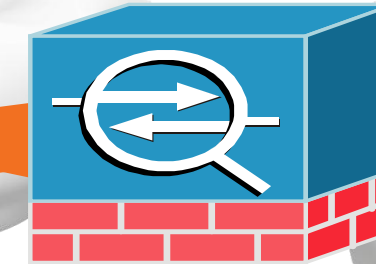
Wireless Hotspot



IPsec Tunnel

Wireless
Provider

ISP



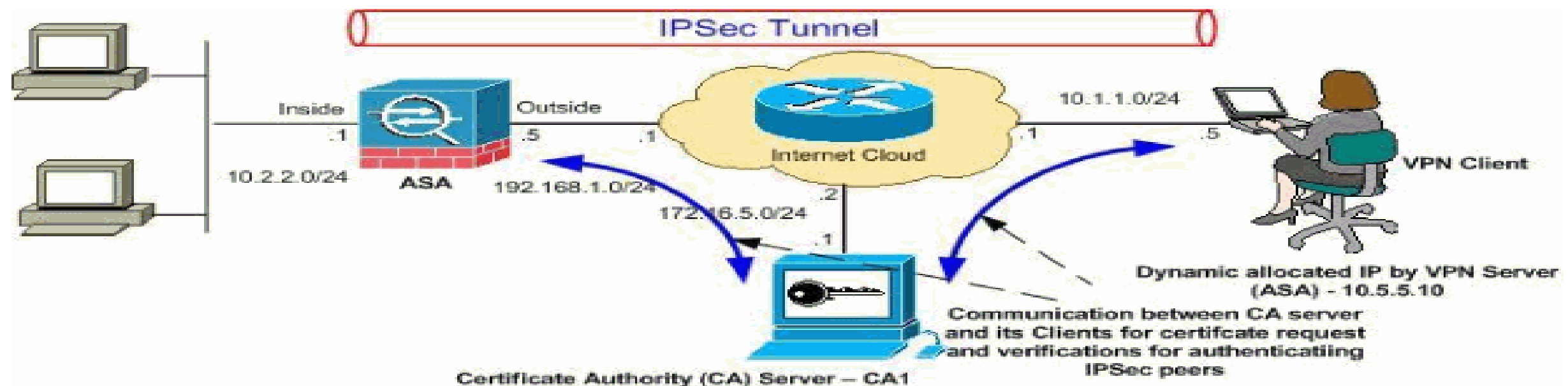
Central
Office



- Traditional IPsec VPN utilising client software on the endpoint
- Minimal client configuration for simplified deployment
- Also works with hardware clients such as an ASA or Cisco router
- Traffic can be tunneled over UDP or TCP for easier firewall and NAT traversal
- Numerous authentication options. PSK, username/password, certificates, and combinations.

Certificate Authentication Example

- Requires a working Public Key Infrastructure
- 2 authentications: IKE Policy (Group) and Connection Profile (User)
- Prepare ASA with trustpoint, certificate, and date/time
- Hybrid authentication example uses IKE certificate (Phase 1) and User password authentication (Phase 1.5 Xauth)



Certificate Authentication - Client Config

1. Obtain CA certificate and load into the VPN Client
2. Obtain User certificate from CA and load into VPN Client
3. Create a new connection. Provide connection name and ASA IP address.
4. Instead of “Group Authentication” for PSK, use “Certificate Authentication”
 - Select user certificate in drop-down

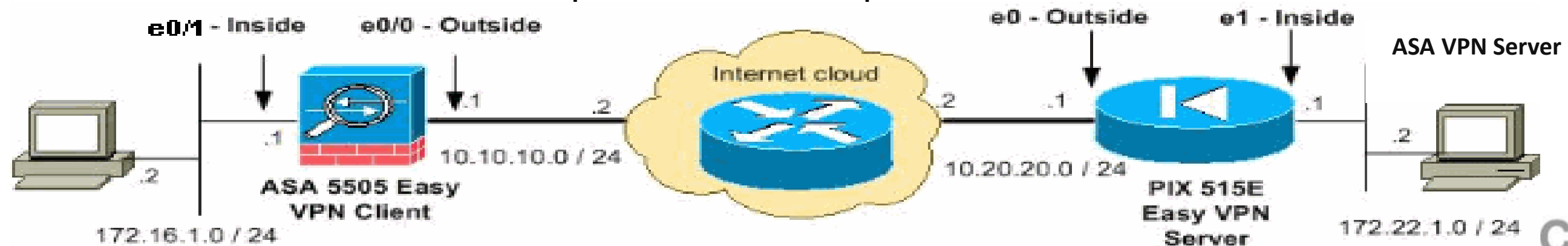
Certificate Authentication for Easy VPN

- Full configuration example:
 - http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080930f21.shtml

The screenshot shows the 'VPN Client | Create New VPN Connection Entry' dialog box. The 'Connection Entry' field contains 'vpnuser'. The 'Host' field contains '192.168.1.5'. The 'Authentication' tab is selected, and 'Certificate Authentication' is chosen. The 'Name' dropdown is set to 'D - Users + vpnuser (Microsoft)'. The 'Save' button is highlighted.

Deploying an Easy VPN Hardware Client

- Utilises hardware such as Cisco ASA or Cisco ISR in two modes:
 - Client mode performs Port Address Translation (PAT) for hosts behind client
 - Network Extension Mode (NEM) connects the client network to the head-end
- Authentication options for Phase 1.5 Xauth:
 - No authentication (beyond group authentication during Phase 1)
 - Secure Unit Authentication (SUA): Single user behind Client authenticates once
 - Default Xauth authentication: CLI authentication
 - Individual User Authentication (IUA): Each user behind Client must authenticate
- HTTP redirection intercepts web traffic to permit interactive SUA or IUA



Easy VPN Hardware Client Config

```
! ---- Enable Easy VPN
vpnclient enable

! ---- Configure Easy VPN server
vpnclient server ip_primary [ip_secondary_1 ...]

! ---- Configure Easy VPN Remote mode
vpnclient mode {client-mode | network-extension-mode}

! ---- Configure Easy VPN group name and authentication with PSK:
vpnclient vpngroup group_name password preshared_key
! ---- OR PKI:
vpnclient trustpoint trustpoint_name [chain]

! ---- Configure automatic Xauth authentication (if required)
vpnclient username xauth_username password xauth password

! ---- Split tunneling (if required)
vpnclient nem-st-autoconnect

! ---- Configure remote management.
! ---- Tunneled over IPsec or over the clear network.
vpnclient management [ clear | tunnel management_ip management_mask ]
```

Deploying an Easy VPN Server

- Uses a Dynamic Crypto Map
 - Only IPsec Transform set defined
 - Peers are unknown due to Remote Access clients with dynamic addresses
- Easy VPN attributes are stored in the Group Policy and User attributes
- Sample Group Policy settings
 - Enable/disable NEM: **nem**
 - Secure Unit Authentication: **secure-unit-authentication**
 - Split Tunnel ACL: **split-tunnel-network-list**
 - Split Tunnel Policy: **split-tunnel-policy** [**excludespecified** | **tunnelall** | **tunnelspecified**]
 - VPN Filter: **vpn-filter**

Easy VPN Server Configuration

1. Define a Group Policy
 - DNS server
 - Default domain
2. Define a Connection Profile
 - Link to Group Policy created
 - Specify address pool
 - Specify IKE Pre-Shared Key or use certificates for authentication (Xauth)
3. Create IKE policy with encryption, hashing, and authentication options
4. Create IPsec transform-set with encryption and hashing options
5. Create dynamic crypto map and associate with transform-set
6. Associate crypto map with outside interface
7. Configure NAT exemption for client address space
8. Enable IKE on outside interface
9. Permit IPSec traffic through outside ACL with **sysopt** command

Phase 2 Configuration – IPsec

```
! ---- IPsec Transform Set.  Encryption and Hashing options.
crypto ipsec transform-set VPN_PHASE2 esp-des esp-md5-hmac

! ---- Dynamic Crypto map creation.  Only transform set.  No ACL or Peer.
crypto dynamic-map VPN_DYN_MAP 10 set transform-set VPN_PHASE2

! ---- Crypto map creation.
crypto map VPN_MAP 10 ipsec-isakmp dynamic VPN_DYN_MAP
crypto map VPN_MAP interface outside

! ---- Tunnel Group (aka Connection Profile) configuration
tunnel-group VPN_REMOTE_ACCESS type ipsec-ra
tunnel-group VPN_REMOTE_ACCESS general-attributes
! ---- Phase 1.5 Xauth and mode config
    authentication-server-group ACS
    address-pool clientpool
    default-group-policy VPN_GROUP_POLICY
tunnel-group VPN_REMOTE_ACCESS ipsec-attributes
    pre-shared-key *

! ---- NAT Exemption NOT shown but is usually required

! ---- Allow IPsec traffic in without specifying in outside interface ACL
sysopt connection permit-ipsec
```

Debugging Remote Access Connections

- Ensure Phase 1 (IKE / ISAKMP) policies match
- Ensure Phase 2 (IPSec) Transforms match
- Ensure address pools are valid and not exhausted
- Ensure Pre-Shared Keys Match or Certificates are valid
 - **Ensure clocks are synchronised if using certificates**
- Ensure AAA servers are reachable and functional
- Utilise ASDM Monitoring VPN functionality
- Ensure connections are mapping to correct group policy and connection profile
- Debugging commands
 - debug crypto isakmp sa (Phase 1 and 1.5 debugs)
 - debug crypto ipsec (Phase 2 debugs)
 - debug aaa
 - debug radius

Section Quiz – 30 Points

- Name two Phase 2 encryption options
- Name two Phase 2 hashing options

```
crypto ipsec transform-set VPN_PHASE2 . . .
```

AnyConnect SSL VPN



AnyConnect SSL VPN

- AnyConnect Overview
- AnyConnect Configuration
- AnyConnect Profiles
- AnyConnect Advanced Deployment
- Creating Users in Local User Database

AnyConnect Remote Access Overview

- Provides full tunnel access similar to IPsec remote access
- AnyConnect Profiles allow client settings pushed from head-end
- Provides extra security with Cisco Secure Desktop functionality
- Requires the use of AnyConnect client
- Client can be pre-loaded or downloaded from the ASA using WebVPN
- Actual protocol is Transport Layer Security (TLS v1.0) or Datagram Transport Layer Security (DTLS)
- TLS uses TCP 443, DTLS uses UDP 443
- DTLS functions over UDP to provide better performance for real-time applications (voice) that are sensitive to packet delays and jitter
 - Uses TLS first to negotiate and establish DTLS connection
 - Uses DTLS to transmit datagrams

AnyConnect SSL VPN Configuration

- Three methods for creation
 - Command line
 - ASDM with Connection Profiles and Group Policies
 - ASDM AnyConnect VPN Wizard
- Key design and configuration choices:
 - Client deployment: pre-deploy and/or web deployment
 - Authentication type: password, one-time-password, certificate, or two methods
 - Split tunnelling policy
 - Cisco Secure Desktop requirements
 - AnyConnect Profile options

AnyConnect SSL VPN Configuration

- AnyConnect ASDM Configuration
 1. Upload AnyConnect clients from Cisco.com to the ASA using TFTP or ASDM
 2. Configure AAA servers for required user authentication methods
 3. Install an SSL certificate on the ASA for secure remote connections
 4. Configure Trustpoint if needed for client certificate authentication
 5. Create address pool for users
 6. Create Group Policy
 - DNS and WINS server
 - Default domain
 7. Create Connection Profile
 - User authentication type
 - Associate Group Policy
 - Address pool
 8. Configure NAT exemption for address pool to internal network

AnyConnect SSL VPN Configuration

```
! ---- Global webvpn config
webvpn
  enable outside
  svc image anyconnect-win-2.3.0254-k9.pkg 1
  svc enable

! ---- Tunnel group config
tunnel-group AC_VPN type remote-access
tunnel-group AC_VPN general-attributes
  address-pool VPN_POOL
  authentication-server-group (inside) ACS LOCAL
  default-group-policy AC_POLICY
tunnel-group AC_VPN webvpn-attributes
  group-alias AC_VPN enable

! ---- Group Policy webvpn settings
group-policy AC_POLICY internal
group-policy AC_POLICY attributes
  webvpn
    svc keep-installer installed none
```

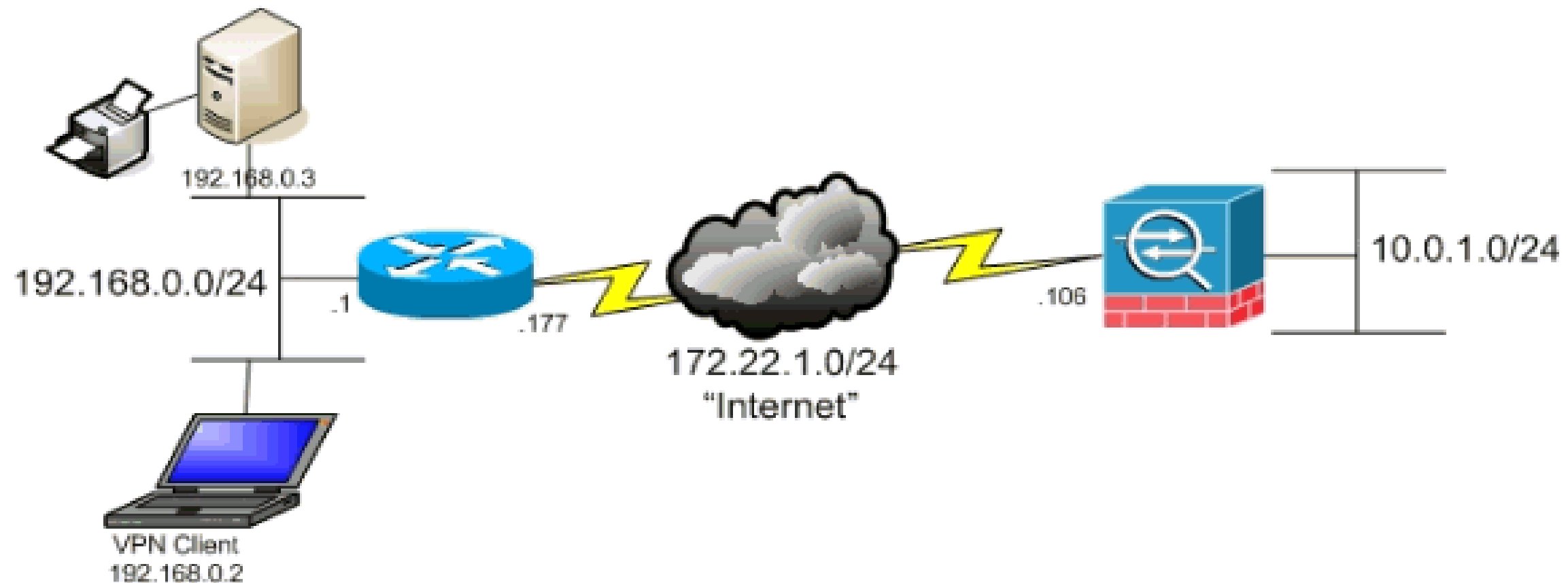
AnyConnect Profiles

- Profiles are XML files stored on the ASA flash and pushed to clients
- Profile settings configure the client to simplify user interaction
- Profiles are edited using a text editor and uploaded to the ASA in 8.2
- Sample profile settings

ASA VPN hostname or IP address	Enable Start Before Logon for Windows users
VPN Server Selection	Auto Reconnect
Backup Server list	Auto Update
Certificate selection	Active SSL VPN Prior to login

- Load uploaded profiles for user with Group Policies
 - `svc profiles name flash_path`

Example of AnyConnect Full Tunnel SSL VPN Solution



Reference

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080702999.shtml

Troubleshooting AnyConnect Client

The screenshot shows the 'Statistics' tab of the AnyConnect Client interface. It is divided into two main columns: 'Connection Information' and 'Address Information'. Callout 'A' points to the 'State' field in the 'Connection Information' section, which is 'Connected'. Callout 'B' points to the 'Client' IP address '10.82.161.31' in the 'Address Information' section. Callout 'C' points to the 'Server' IP address '64.102.252.9' in the same section. The interface also includes sections for 'Bytes', 'Frames', 'Control Frames', 'Transport Information', 'Feature Configuration', and 'Secure Mobility Solution'. At the bottom, there are 'Reset' and 'Export Stats...' buttons.

Connection Information		Address Information	
State:	Connected	Client:	10.82.161.31
Mode:	All Traffic	Server:	64.102.252.9
Duration:	00:01:14	Client (IPv6):	Disabled
Bytes		Transport Information	
Sent:	18295	Protocol:	DTLS
Received:	1170	Cipher:	RSA_AES_128_SHA1
Frames		Compression:	None
Sent:	252	Proxy:	No Proxy
Received:	1	Feature Configuration	
Control Frames		FIPS Mode:	Disabled
Sent:	4	Trusted Network Detection:	Enabled
Received:	4	Always On:	Disabled
Secure Mobility Solution		Status:	Not Available
Status:	Not Available	Appliance:	Not Available

Debugging AnyConnect SSL VPN

- Utilise ASDM Monitoring VPN functionality
- Ensure connections are mapping to correct group policy and connection profile
- Debugging commands
 - show webvpn ?
 - debug webvpn ?
 - debug aaa
 - debug radius

Q & A



Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm



Cisco *live!* 365

Don't forget to activate your Cisco Live 365 account for access to all session material,

communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.

www.ciscoliveaustralia.com/portal/login.wv

Cisco *live!*



Appendix



Test Tips

- Question Types
 - Multiple-choice single answer
 - Multiple-choice multiple answer
 - Drag-and-drop
 - Testlet / Simlet / Simulations
- Narrow it down
- Look for subtle keys
- Look for the **best** answer when multiple exist
- Don't waste too much time

Site-to-Site Design Considerations

- How many sites?
 - If numerous, how will the ASAs be managed?
- What do optimal traffic flow patterns look like?
 - Full mesh network? How many tunnels and how much configuration per ASA?
 - Hub and spoke? How large does hub need to be? Backup hub?
 - How will routes be distributed?
- How will ASAs authentication sessions?
 - Pre-shared key (PSK) or certificate?
 - If PSK, how often will they key be updated?
 - If certificate, does a Public Key Infrastructure exist?
- What level of High Availability is needed?
 - Active / Standby hub?

Remote Access Design Considerations

- Which remote access method?
 - IPsec, SSL VPN full tunnel, or Clientless SSL VPN?
 - Do you have proper licensing?
 - Will endpoints use clients or clientless access?
 - How many users?
- How will clients be loaded on endpoints?
 - Do users have administrative permissions?
 - Will be clients be pushed by other means?
- How will users be authenticated?
 - ACS, RADIUS, LDAP, Active Directory, One Time Password, certificate, 2-factor?
- What additional security is required for remote connections?
 - Cisco Secure Desktop Host scan, Vault, Endpoint Assessment?
- What level of High Availability is needed?
 - Multiple remote access ASA gateways?
 - Active / Standby pair?

LDAP Attributes Example

Edit LDAP Attribute Map

Name:

Mapping of Attribute Name | Mapping of Attribute Value

LDAP Attribute Name	Cisco Attribute Name
bookmarks	WebVPN-URL-List

LDAP Attribute Name:

Cisco Attribute Name:

- Allow-Network-Extension-Mode
- Access-Hours
- Allow-Network-Extension-Mode
- Auth-Service-Type
- Authenticated-User-Idle-Timeout
- Authorization-Required
- Authorization-Type
- Banner1
- Banner2

Buttons: Add >>, << Remove, OK, Cancel, Help



Clientless Portal Configuration

Add SSL VPN Connection Profile

Basic
+ Advanced

Name: Contractor

Aliases:

Authentication

Method: AAA Certificate Both

AAA Server Group: TAC_SERVER Manage...

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers: 10.10.10.224

Client Address Pools: pool-2 Select...

Default Group Policy

Group Policy: DfltGrpPolicy Manage...

(Following field is an attribute of the group policy selected above.)

Enable SSL VPN Client protocol

Find: Next Previous

OK Cancel Help

Clientless Portal Configuration

Add SSL VPN Connection Profile

Basic
+ Advanced

Name: Contractor
Aliases:

Authentication
Method: AAA Certificate Both
AAA Server Group: TAC_SERVER
 Use LOCAL if Server Group fails

Client Address Assignment
DHCP Servers: 10.10.10.224
Client Address Pools: pool-2

Default Group Policy
Group Policy: DfltGrpPolicy
(Following field is an attribute of the...)
 Enable SSL VPN Client protocol

Find: [] Next Previous

OK Cancel Help

Login

Please enter your username and password.

GROUP: contractor
USERNAME:
PASSWORD:

Login

Clientless SSL VPN



Clientless SSL VPN

- Clientless VPN Overview
- Clientless Capabilities
 - Application access
 - Smart Tunnels
 - Plug-ins
- Troubleshooting Clientless SSL VPNs
- Advanced Authentication and Single Sign-On in a Clientless SSL VPN
- Customising the Portal

Clientless SSL VPN Overview

- Provides network access using a standard web browser. No client.
- Secure access through multiple methods
 - Internal websites – delivering internal websites over HTTPS
 - Windows file shares – web-based file browsing capabilities
 - Plug-ins – Java applets for telnet, SSH, RDP, VNC, and Citrix (ICA)
 - Smart Tunnels – Automatic tunnelling of application traffic through the SSL VPN
 - Port Forwarding – Opening local ports to be forwarded over the SSL VPN
- Provides extra security with Cisco Secure Desktop functionality

Clientless SSL VPN Configuration

- Three methods for creation
 - Command line
 - ASDM with Connection Profiles and Group Policies
 - ASDM VPN Wizard
- Key design and configuration choices:
 - Which access methods to permit (web, file browsing, plug-ins, etc)
 - Bookmarks for users
 - Different web portals for different groups
 - Authentication type: password, one-time-password, certificate, or two methods
 - Cisco Secure Desktop requirements

Clientless ASDM Configuration

1. Upload Plug-ins and CSD to flash if needed
2. Configure AAA servers for required user authentication methods
3. Install an SSL certificate on the ASA for secure remote connections
4. Configure Trustpoint if needed for client certificate authentication
5. Create Group Policy
 - Define most of the Clientless options
6. Create Connection Profile
 - User authentication type
 - Associate Group Policy
 - Create Connection Aliases and Group URLs for users to access this Clientless SSL VPN
7. Enable SSL VPN on the appropriate interface

Clientless SSL VPN Configuration

```
! ---- Global webvpn config
webvpn
  enable outside
  tunnel-group-list enable
  port-forward PF_LIST 8080 192.168.1.200 www Intranet web server

! ---- Tunnel group config
tunnel-group CLIENTLESS_VPN type remote-access
tunnel-group CLIENTLESS_VPN general-attributes
  authentication-server-group (inside) ACS LOCAL
  default-group-policy CLIENTLESS
tunnel-group CLIENTLESS_VPN webvpn-attributes
  group-alias CLIENTLESS_VPN enable

! ---- Group Policy webvpn settings
group-policy CLIENTLESS internal
group-policy CLIENTLESS attributes
  vpn-tunnel-protocol ssl-clientless
...
webvpn
  port-forward enable PF_LIST
...
```

Clientless SSL VPN Bookmarks

- Methods for assigning bookmarks
 - Group policy
 - User attributes
 - LDAP or RADIUS attributes
 - Dynamic Access Policy (DAP) result
- URL Variables for Single Sign On
 - CSCO_WEBVPN_USERNAME — User login name
 - CSCO_WEBVPN_PASSWORD — Obtained from user login password
 - CSCO_WEBVPN_INTERNAL_PASSWORD — Obtained from the Internal password field. You can use this field as Domain for Single Sign-on operations.
 - CSCO_WEBVPN_CONNECTION_PROFILE — User login group drop-down
 - CSCO_WEBVPN_MACRO1 — Set via Radius or LDAP vendor specific attribute
 - CSCO_WEBVPN_MACRO2 — Set via Radius or LDAP vendor specific attribute

Bookmark Settings

The screenshot displays the Cisco VPN configuration interface. The main window is titled "Edit User Account" and shows a tree view on the left with "VPN Policy" expanded to "Clientless SSL VPN". The main area contains settings for "Bookmark List", "URL Entry", and "File Access Control".

Overlaid on this is a "Configure GUI Customization Objects" dialog box. It contains the following text:
Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.
This parameter is enforced in either a VPN [user](#), a [group policy](#), or a [dynamic access policy](#) configuration.

Below the text are buttons for "Add", "Edit", "Delete", "Import", and "Export".

A second dialog box, "Edit Bookmark List", is open over the "Configure GUI Customization Objects" dialog. It shows the "Bookmark List Name" as "www.cisco.com" and a table of bookmarks:

Bookmark Title	URL
cisco	http://www.cisco.com
support	http://www.cisco.com/go/sup...
switches	http://www.cisco.com/go/swit...

Buttons for "Add", "Edit", "Delete", "Move Up", and "Move Down" are visible on the right side of the "Edit Bookmark List" dialog.



Clientless Smart Tunnels

- Allows a TCP-based application to tunnel through the clientless VPN
- Benefits
 - Better performance than plug-ins
 - Simplifies user experience compared to forwarding local ports
 - Does not require administrative privileges like port forwarding
- Available for Windows (using Internet Explorer) and Mac
- Configuring Smart Tunnels
 - Under **webvpn** configuration, use the following command:
 - **smart-tunnel list *list application path [platform OS] [hash]***
 - Enable Smart Tunnel access in the Group Policy. Optionally enable auto-start.
smart-tunnel enable *list*
 - **smart-tunnel auto-start *list***

Deploying Advanced Application Access for Clientless SSL VPN

- Configuring Smart Tunnels

The screenshot displays the configuration path: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels**. The main configuration page contains the text: "Configure Smart Tunnel lists for application access. This parameter is enforced in either a VPN [user](#) or [group policy](#) configuration." Below this text are buttons for "Add", "Edit", and "Delete".

Two dialog boxes are overlaid on the main page:

- Add Smart Tunnel List**: This dialog has a "List Name" field containing "Lotus" and a table with columns "Application ID", "Process Name", "OS", and "Hash". An "Add" button is located at the bottom right of the table.
- Add Smart Tunnel Entry**: This dialog has three input fields: "Application ID" with the value "lotusnotes", "Process Name" with the value "notes.exe" (with a note "(e.g. word.exe)" below it), and "Hash (Optional)". At the bottom, there are "OK", "Cancel", and "Help" buttons.

Mid-Section Quis – IP Protocol 17?

What AnyConnect SSL VPN feature provides better performance for real-time applications like voice?



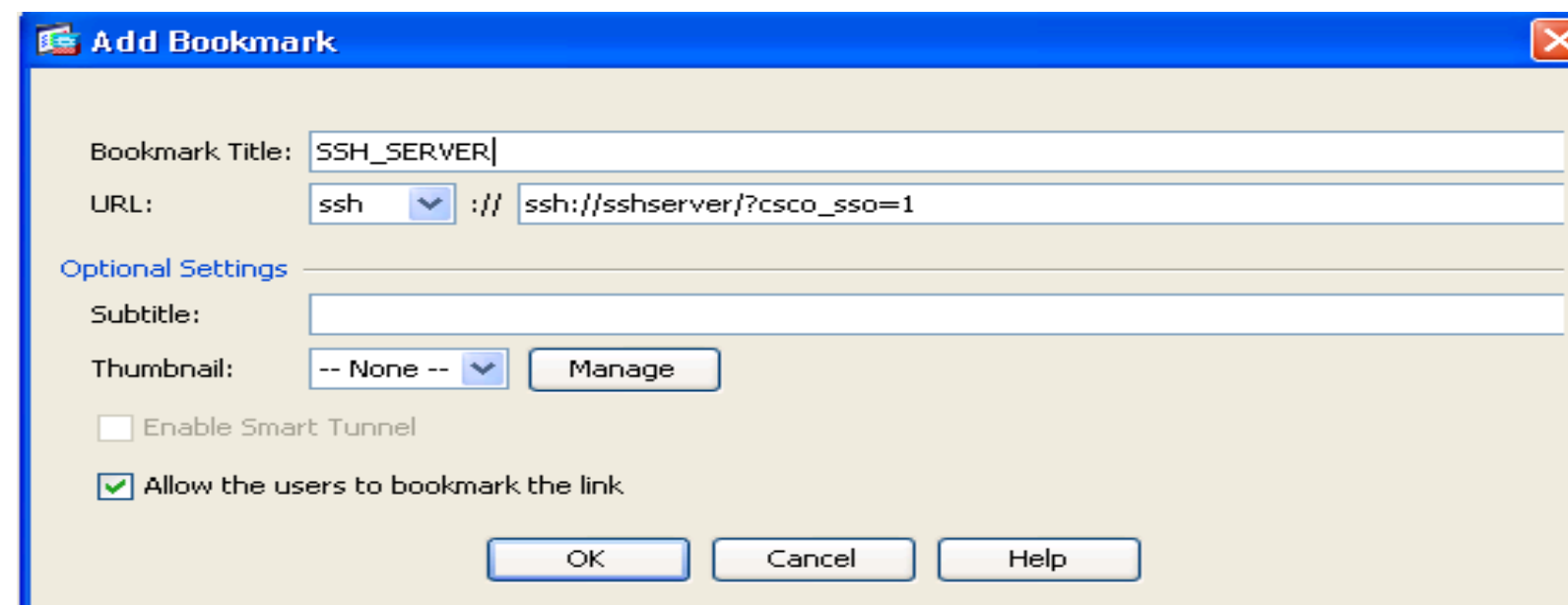
Clientless Plug-ins

- Java applets that enable secure application connectivity through the SSL VPN browser session and enables new URL and bookmark types
 - Citrix Client (ica://)
 - Windows terminal service (rdp://, rdp2://)
 - Shell access (telnet://, ssh://)
 - VNC remote desktop service (vnc://)
- Configuration
 - Load the plug-in files to ASA flash or TFTP server * **Plug-ins DO NOT require administrator privileges on the remote system to run**
 - Issue the privileged exec command to load the plug-in
 - **import webvpn plug-in protocol [rdp | rdp2 | ssh, telnet | vnc] *URL***
 - To remove a plug-in
 - **revert webvpn plug-in protocol [rdp | rdp2 | ssh, telnet | vnc]**

Deploying Single Sign-On for Plug-ins

1. Install the plug-in
2. Add a bookmark entry to display a link to the server
3. Specifying SSO support using the `cisco_sso=1` parameter

- Example:

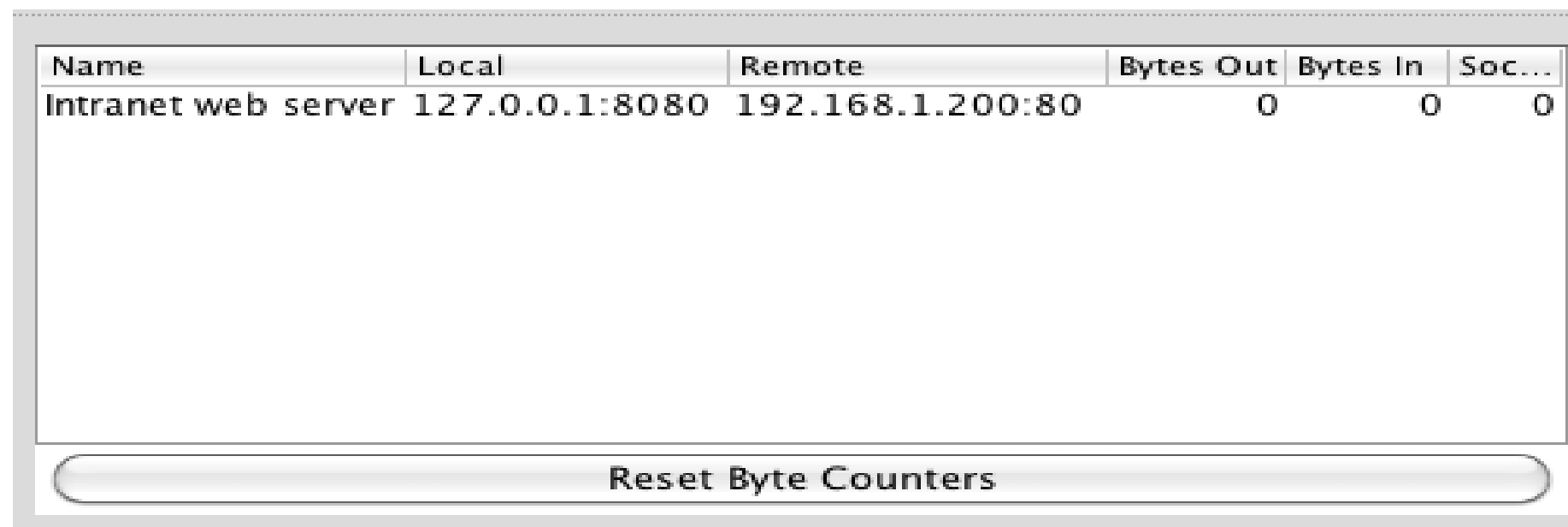


`ssh://sshserver/?cisco_sso=1`

`rdp://rdp-server/?Parameter1=value&Parameter2=value&cisco_sso=1`

Clientless Port Forwarding

- Port forwarding supports TCP applications over the SSL VPN
- Works by opening local ports and forwarding the connection as defined by the port forward configuration
- DNS is intercepted to force applications to connect to the local ports
- Requires administrative rights on the endpoint to function
- Works on Windows, Mac, and Linux



Name	Local	Remote	Bytes Out	Bytes In	Soc...
Intranet web server	127.0.0.1:8080	192.168.1.200:80	0	0	0

Reset Byte Counters

Port Forwarding Configuration

1. Under **webvpn** configuration, define the port forwarding list
 - **port-forward** *{list_name local_port remote_server remote_port description}*
2. Enabled port forwarding list under the Group Policy
 - **port-forward enable** *list_name*
 - **port-forward auto-start** *list_name*

```
webvpn
  port-forward PF_LIST 8080 192.168.1.200 www Intranet web server

group-policy VPN_POLICY attributes
  webvpn
    port-forward enable PF_LIST

hostname maynard
```

Port Forwarding Configuration

The screenshot displays the Cisco VPN configuration interface. On the left is a navigation tree with 'Remote Access VPN' selected. The main window shows the 'Port Forwarding' configuration page under 'Clientless SSL VPN Access > Portal > Port Forwarding'. It includes a table for 'Port Forwarding Lists' and two modal dialog boxes: 'Add Port Forwarding List' and 'Add Port Forwarding Entry'.

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Port Forwarding

Configure Port Forwarding Lists that the security appliance uses to grant users access to TCP-based applications over a clientless SSL VPN connection. This parameter is enforced in either a VPN [user](#), a [group policy](#), or a [dynamic access policy](#) configuration.

Table: Port Forwarding Lists

List Name	Local TCP Port	Remote Server	Remote TCP Port	Description
[Empty table body]				

Add Port Forwarding List Dialog:

List Name:

Add Port Forwarding Entry Dialog:

Local TCP Port:

Remote Server:

Remote TCP Port:

Description:

Buttons: Add, Edit, Delete, OK, Cancel, Help, Apply, Reset



Customising the Clientless SSL VPN UI

- Deploying Basic Navigation Customisation
- Deploying Full Portal Customisation
- Deploying Portal Localisation
- Deploying Portal Help Customisation
- Cisco AnyConnect Portal Integration

Customising User Interface and Portal

A

B

C

D

E

F

G

- Home
- Web Applications
- Browse Networks
- AnyConnect
- Application Access
- Telnet/SSH Servers
- VNC Connections
- Terminal Servers

Address http://

EVIA

Customising the SSL Login Page

- Page can be branded with the following options

CISCO SSL VPN Customization Editor

A → Logon page

B → Portal

- Browser Window
- Title Panel
- Toolbar
- Navigation Panel
- Applications
- Home page
- Custom Panes
- Columns

C → Logout page

HOME_SSL_PAGE : Portal > Browser Window

Browser Window

Debugging Clientless SSL VPN

- Utilise ASDM Monitoring VPN functionality
- Ensure connections are mapping to correct group policy and connection profile
- Debugging commands
 - show webvpn ?
 - debug webvpn ?
 - debug aaa
 - debug radius
 - debug dap

Advanced Cisco ASA VPN Solutions



Advanced Cisco ASA VPN Solutions

- Cisco Secure Desktop in SSL VPNs
- Onscreen Keyboard Configuration
- Scan for Key Loggers example
- Dynamic Access Policies
- Selection Hierarchy for SSL Attributes
- WebACL Example
- High Availability Options

Cisco Secure Desktop

- Advanced endpoint analysis, security, and remediation
- Downloaded and executed when AnyConnect or Clientless session is initiated
- Works on Windows, Mac, and Linux (varying capabilities)
- Results of host analysis can be used with Dynamic Access Policies
- Capabilities
 - Host scan – Checks for OS, patch levels, registry entries, processes, and files
 - Endpoint assessment – Checks and remediates Anti-Virus, Anti-Spyware, and Personal Firewall
 - Vault – Secure desktop session
 - Cache cleaner – Securely delete web browsing data remnants
 - Keystroke logger detection
 - Onscreen keyboard – Mitigate keystroke logger threat

Cisco Secure Desktop Setup

- CSD ASDM installation
 1. On CSD Setup page, upload CSD image
 2. Click 'Enable Secure Desktop'
- Enable features needed like pre-login policy, onscreen keyboard, etc

Pre-login Policy Decision Tree

Prelogin Policy

Use the decision tree below to create prelogin policies. Click the + symbol to check for a specific OS version, or IP address. Click an end node to rename a prelogin policy, change it to a subsequent node, or "Login Denied." The policy name can be used as the value for the Policy endpoint selection attribute under the endpoint.

Select the type of check that you would like to insert

Check:

Onscreen Keyboard Configuration

The screenshot shows the configuration page for the Onscreen Keyboard. The breadcrumb trail is: Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization. The page title is "Customization Objects". Below the title, there is a description: "Configure Customization Objects that the security appliance displays as main SSL VPN portal page. This parameter is enforced in either a VPN user, a group policy, or a connection profile configuration." There are buttons for Add, Edit, Delete, Import, and Export. A table lists the customization objects, with "HOME_SSL_PAGE" selected. Below the table, there is a section for "OnScreen Keyboard" with three radio button options: "Do not show OnScreen Keyboard", "Show only for the login page" (which is selected), and "Show for all portal pages requiring authentication".

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization

Customization Objects

Configure Customization Objects that the security appliance displays as main SSL VPN portal page.
This parameter is enforced in either a VPN [user](#), a [group policy](#), or a [connection profile](#) configuration.

+ Add Edit Delete + Import Export

Customization Objects
Template
DfltCustomization
HOME_SSL_PAGE

OnScreen Keyboard

Specify when OnScreen Keyboard

- Do not show OnScreen Keyboard
- Show only for the login page
- Show for all portal pages requiring authentication

Login

Please enter your username and password.

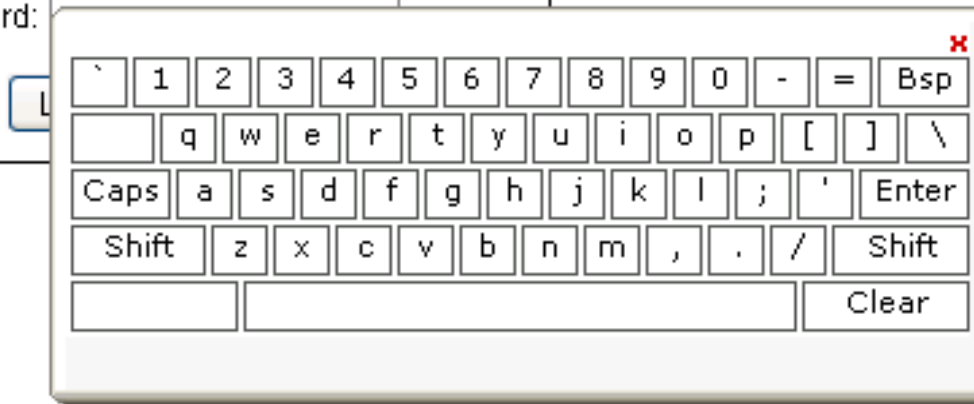
GROUP: HOME_USER

USERNAME: mabernar

PASSWORD:

Internal Password:

This is a private workspace



Scan for Key Loggers example

Configuration > Remote Access VPN > Secure Desktop Manager > Default > Keystroke Logger & Safety Checks

Keystroke Logger & Safety Checks

If you check "Force admin control" and an unapproved keystroke logger is detected, the Cisco Secure Desktop module (that is, Secure Desktop, Cache Cleaner, or Host Scan) does not install on the remote device. Likewise, if you check "Always deny access" and a host emulator is detected, the Cisco Secure Desktop module does not install on the remote device.

Check for keystroke loggers

Force admin control on list of safe modules

List of Safe Modules:

%windir%\system32\keylogger.exe	Add
---------------------------------	-----

Check for host emulation

Always deny access if running within emulation

Apply All Reset All



Note CSD only detects keystroke loggers if the user has administrator privileges. If the user does not, keystroke logger detection does not run.

Dynamic Access Policies

- Use Dynamic Access Policies (DAP) to create powerful rules that enable differentiated remote access
- DAP selection criteria are combined with logical expressions
 - AAA attributes from LDAP or RADIUS
 - Endpoint attributes from Endpoint Assessment and Host Scan
- If criteria met, Access and Authorisation Policies can be set
 - Permit, Quarantine, or Terminate connection and display message to user
 - Apply a Network ACL
 - Apply a Web ACL (clientless)
 - Enable/disable file browsing, file server entry, HTTP proxy, and URL entry (clientless)
 - Enable/disable/auto-start port forwarding lists (clientless)
 - Enable bookmark lists (clientless)
 - Permit or deny access methods such as AnyConnect and/or Clientless

Dynamic Access Policy Creation

Policy Name:

Description: ACL Priority:

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.

AAA Attribute	Operation/Value
ldap.memb...	= FinanceGroup

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
av.SophosAV	lastupdate < 30 activescan = ok

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 Quarantine Terminate

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

User Message:



WebACL Example

The screenshot displays the configuration interface for a Clientless SSL VPN. The main window shows various settings, including 'Web ACL' which is currently set to 'Inherit' and 'None'. Two windows are overlaid on the main interface:

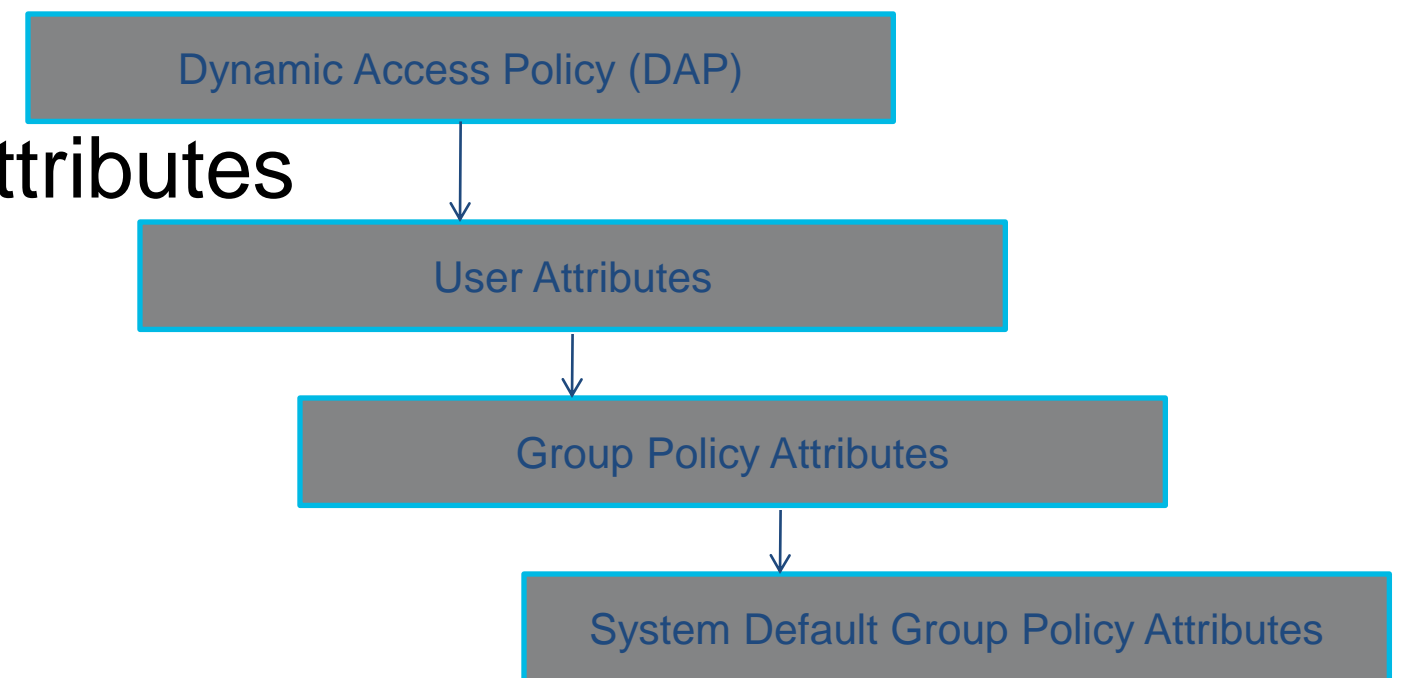
- ACL Manager:** A table showing a single Access Control Entry (ACE) named 'test' with ID '1'. The address is 'http://*f[F]acebook*', the service is 'http', and the action is 'Permit'. The filter is set to 'Both'.
- Edit ACE:** A dialog box for editing the selected ACE. It shows the action is 'Permit', the filter is 'Filter on URL', and the URL pattern is 'http://*f[F]acebook*'. The 'Enable Logging' checkbox is checked, and the logging level is set to 'Default'.

No	Address	Service	Action	Time	Logging
1	http://*f[F]acebook*	http	Permit		



Selection Hierarchy for VPN Attributes

1. Dynamic Access Policy (DAP) attributes
2. User Policy attributes
3. Policy attributes attached to the user profile
4. Policy attributes attached to the connection profile (tunnel group)
5. System Default Group Policy attributes



High Availability Options

- Redundant head-end peering
 - Configure two head-ends with 2 IPsec tunnels
 - Utilise two interfaces with 2 ISPs for additional redundancy
 - Static route tracking is used to switch between ISPs
- Active / Standby chassis redundancy
 - ASA must be in single context and routed mode to support VPNs
 - Configure both Failover link and Stateful link to preserve VPN sessions
- VPN Load Balancing feature
 - Virtual load balancing built into ASA. No external load balancer required.
 - Works with IPsec (remote access), SSL VPN tunnels, and SSL VPN clientless
 - VPN Clustering requires a Unified Client Certificate

Command Line Quiz!

