Cisco Networkers 2011
May 19, Toronto, Canada

Knowledge Is Power.
Learn. Share. Collaborate.

AnyConnect Secure Mobility

Presented by Tim Davidson

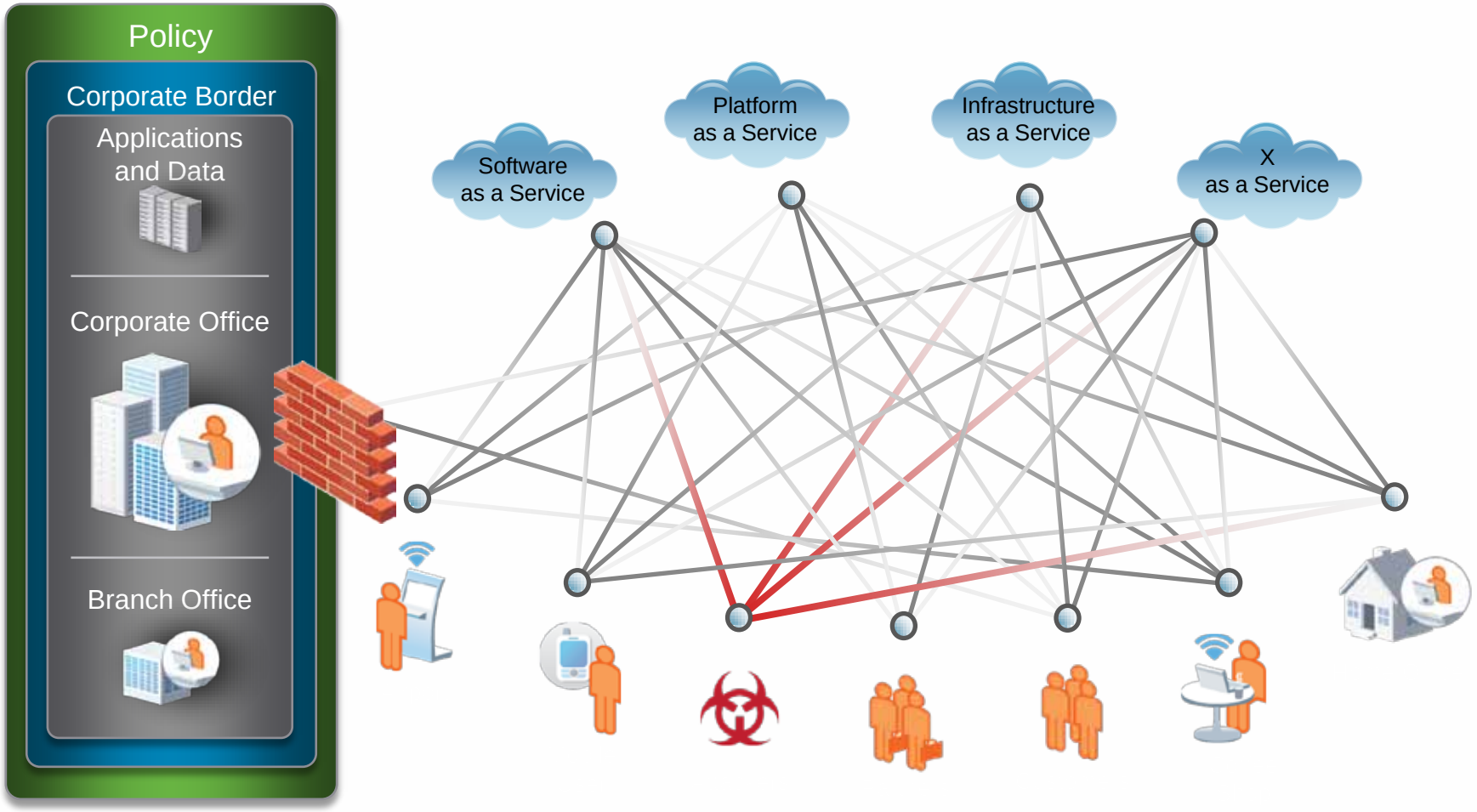
Agenda

- Solution Overview
- Deployment Scenarios
- Feature Highlights
- Q & A
- Wrap Up

Solution Overview

Security in the Borderless World

Knowledge Is Power.
Learn. Share. Collaborate.



Personal Choice vs Corporate Policy

Knowledge Is Power.
Learn. Share. Collaborate.

Traditional Remote Access VPN

Knowledge Is Power.
Learn. Share. Collaborate.

No Security or Visibility

salesforce.com

skype

YouTube

Security

Intranet

Corporate File Sharing

Limited

Predominantly PC-based Client Support

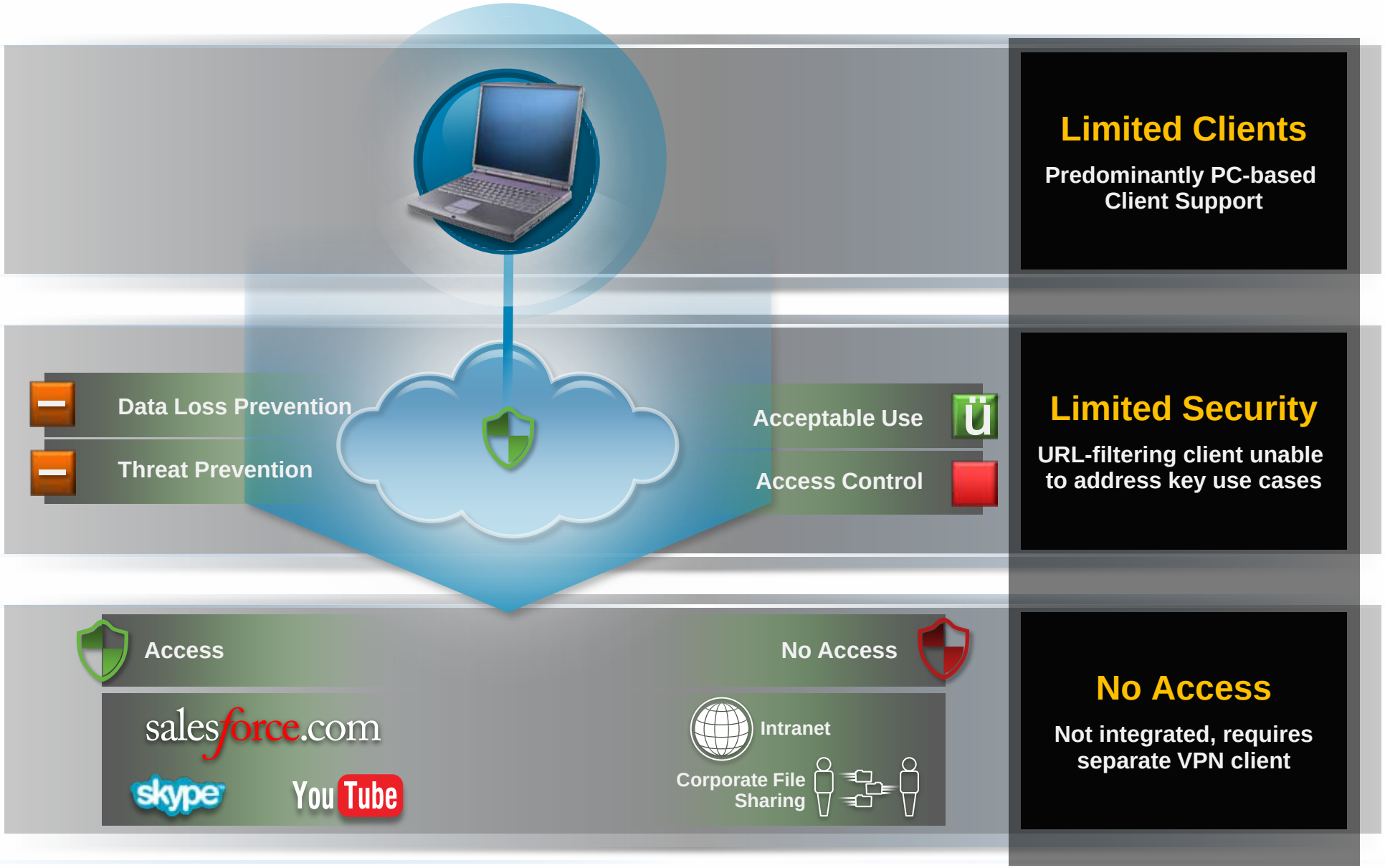
Manual

Numerous “clicks”
Non-persistent Connection

Rarely-On

Only connected if / when absolutely necessary

Traditional Mobile Web Security



Web Security with Next Generation Remote Access

Knowledge Is Power.
Learn. Share. Collaborate.

Choice

Diverse Endpoint Support for Greater Flexibility

Security

Rich, Granular Security Integrated Into the network

Experience

Always-on Intelligent Connection for Seamless Experience and Performance

AnyConnect Secure Mobility Client

Network and Security Follows User—It Just Works

Knowledge Is Power.
Learn. Share. Collaborate.

Broad Mobile Support

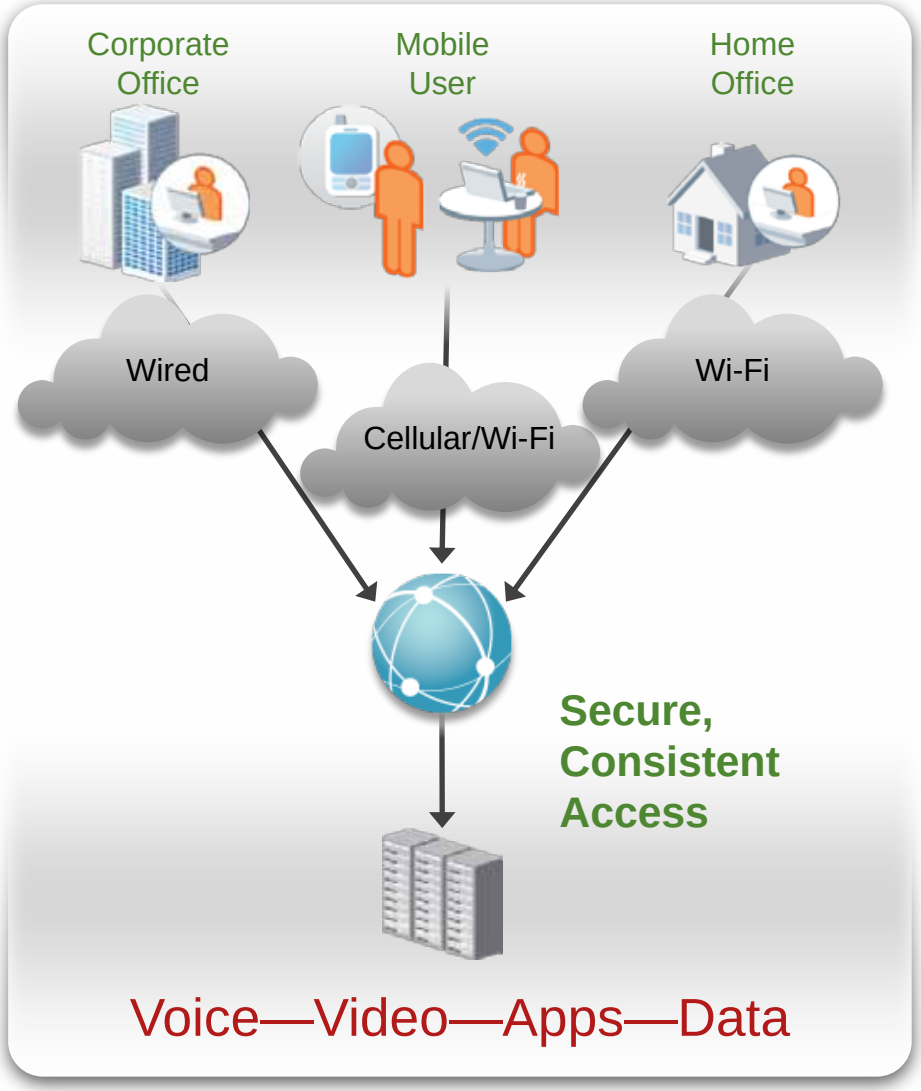
- Fixed and semi-fixed platforms
- Mobile platforms

Persistent Connectivity

- Always-on connectivity
- Optimal gateway selection
- Automatic hotspot negotiation
- Seamless connection hand-offs

Next-Gen Unified Security

- User/device identity
- Posture validation including Managed vs Un Managed Assets
- Integrated web security for always-on security (hybrid)
- Clientless and desktop virtualization

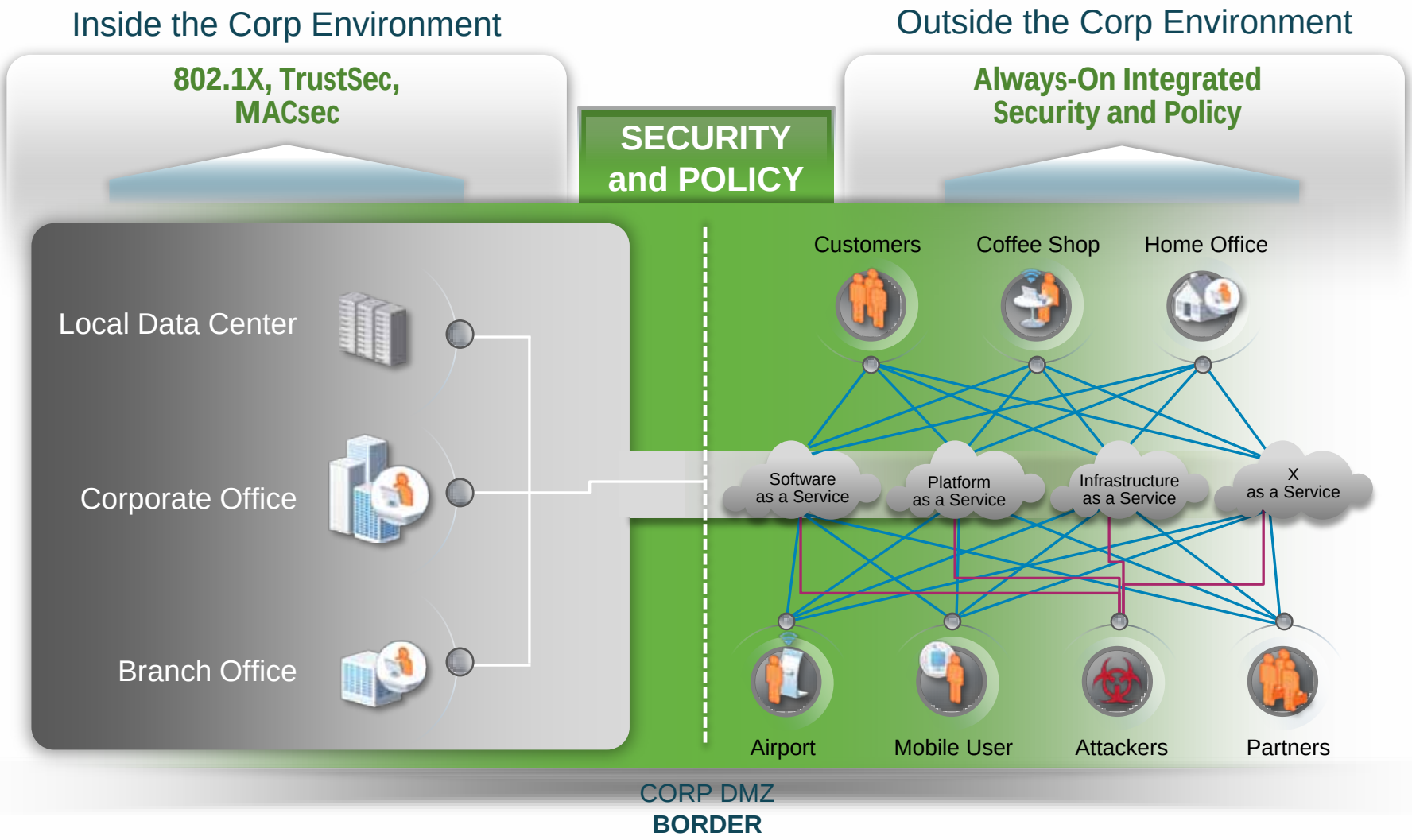


Enabling the New Borderless Organization

Securely, Reliably, Seamlessly

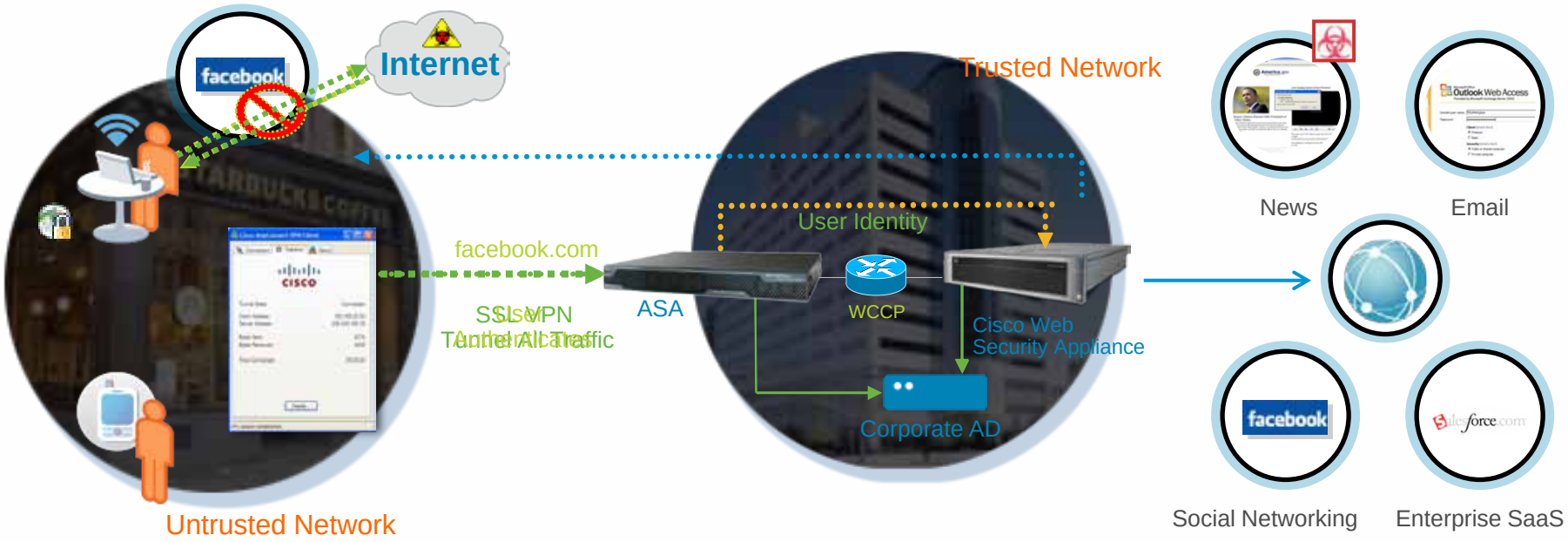
Secure Borderless Network Architecture Enabling Mobility, Extending Security

Knowledge Is Power.
Learn. Share. Collaborate.



Deployment Scenarios

Cisco AnyConnect Secure Mobility with Web Security Appliance



AnyConnect

- Always-on VPN (admin configurable)
- Optimal head end auto-detect
- Transparent auth (certificate)

ASA à WSA

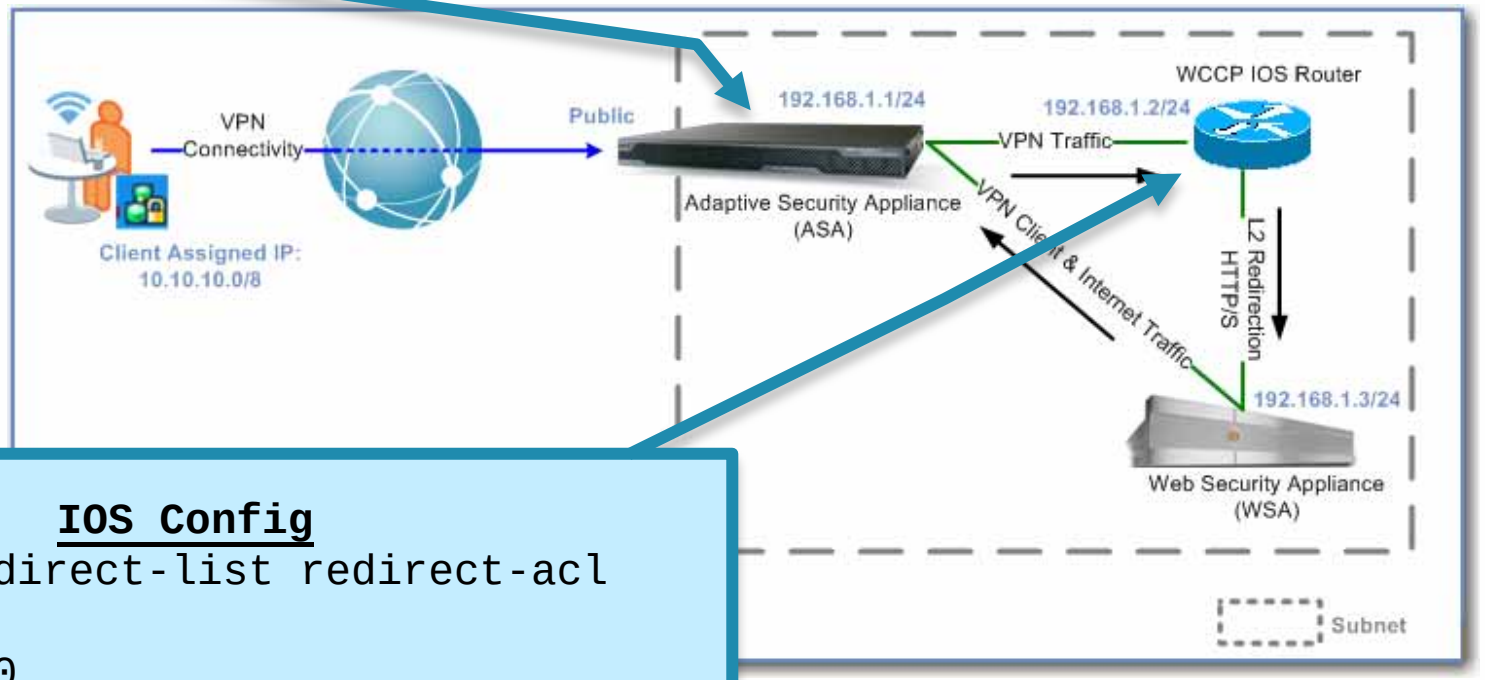
- Authentication handoff (SSO)
- Identity and location aware policy enforcement
- Location-aware reporting

Transparent Redirection – Single ASA
(WCCP on Router)

Knowledge Is Power.
Learn. Share. Collaborate.

ASA Config

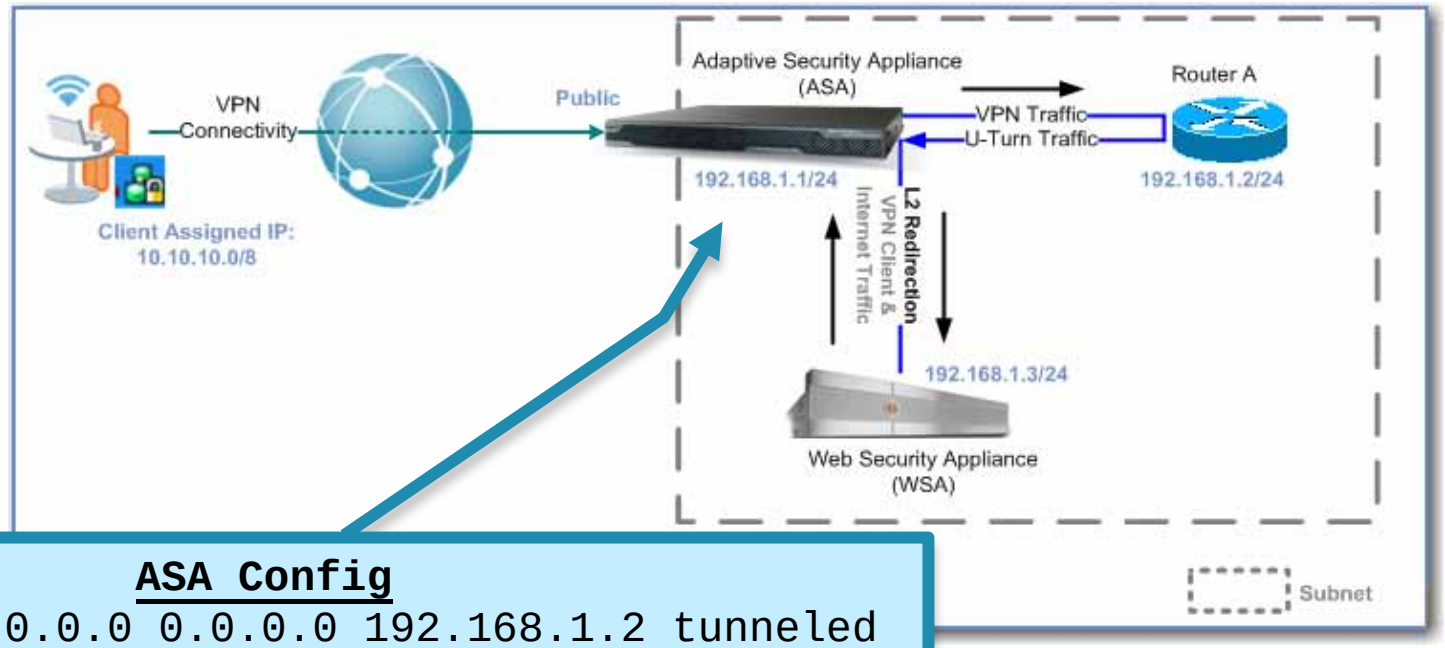
```
route inside 0.0.0.0 0.0.0.0 192.168.1.2 tunneled
route inside 10.10.10.0 255.0.0.0 192.168.1.2
```



IOS Config

```
ip wccp 80 redirect-list redirect-acl

interface eth0
        ip wccp 80 redirect in
```

Transparent Redirection – Single ASA
(WCCP on ASA)



ASA Config

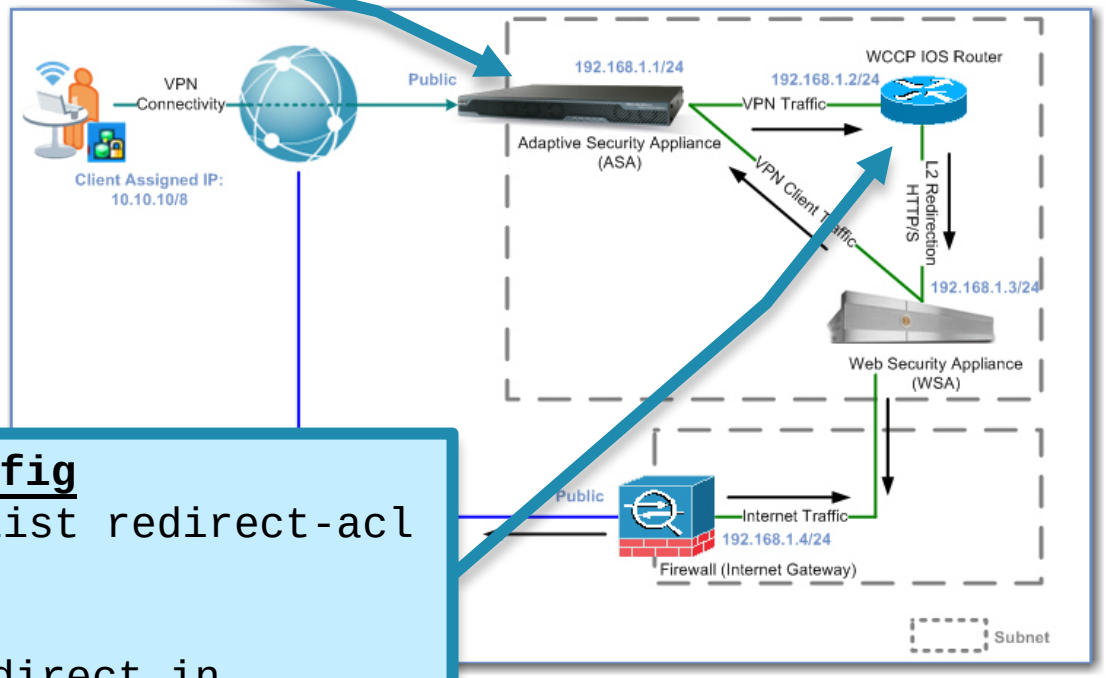
```
route inside 0.0.0.0 0.0.0.0 192.168.1.2 tunneled
route inside 10.10.10.0 255.0.0.0 192.168.1.2

wccp 80 redirect-list redirect-acl
wcpp iterface inside 80 redirect in
```

Transparent Redirection
(Alternate Egress)

Knowledge Is Power.
Learn. Share. Collaborate.

ASA-1 Config

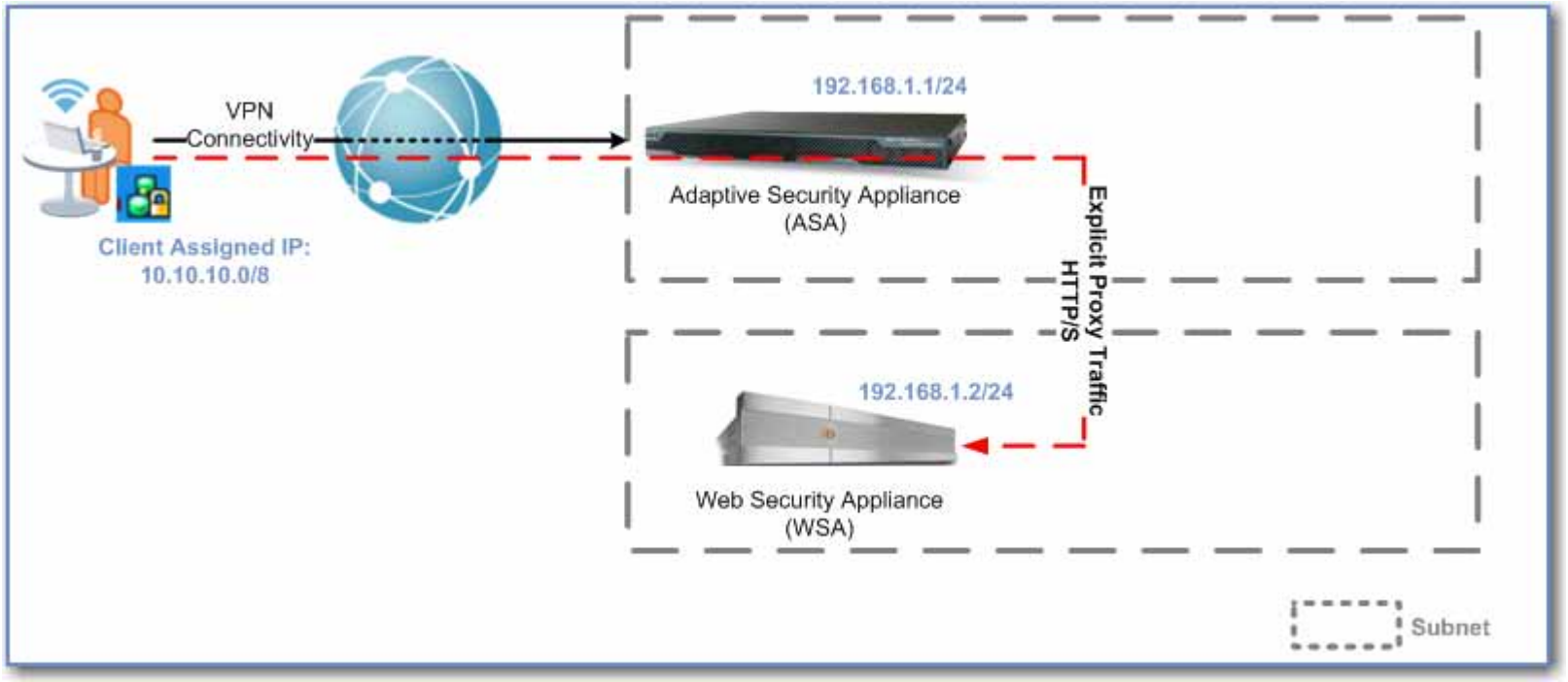
```
route inside 0.0.0.0 0.0.0.0 192.168.1.2 tunneled
route inside 10.10.10.0 255.0.0.0 192.168.1.2
```



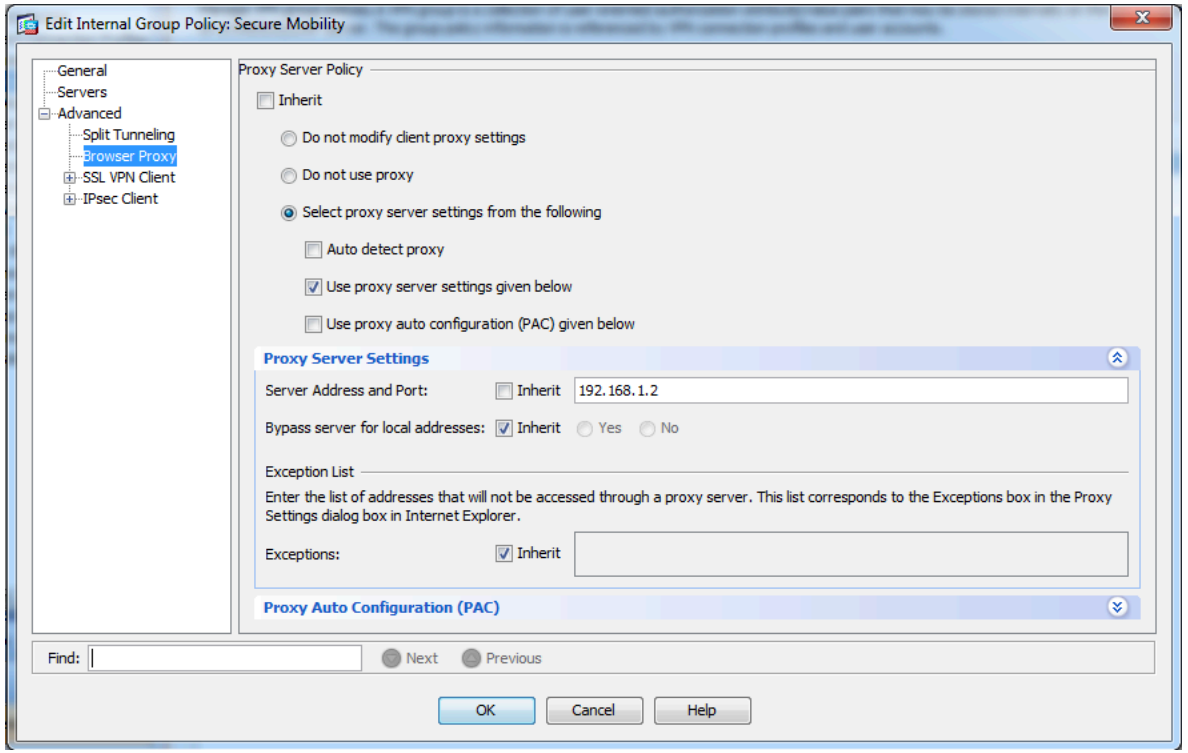
IOS Config

```
ip wccp 80 redirect-list redirect-acl

interface eth0
        ip wccp 80 redirect in
```

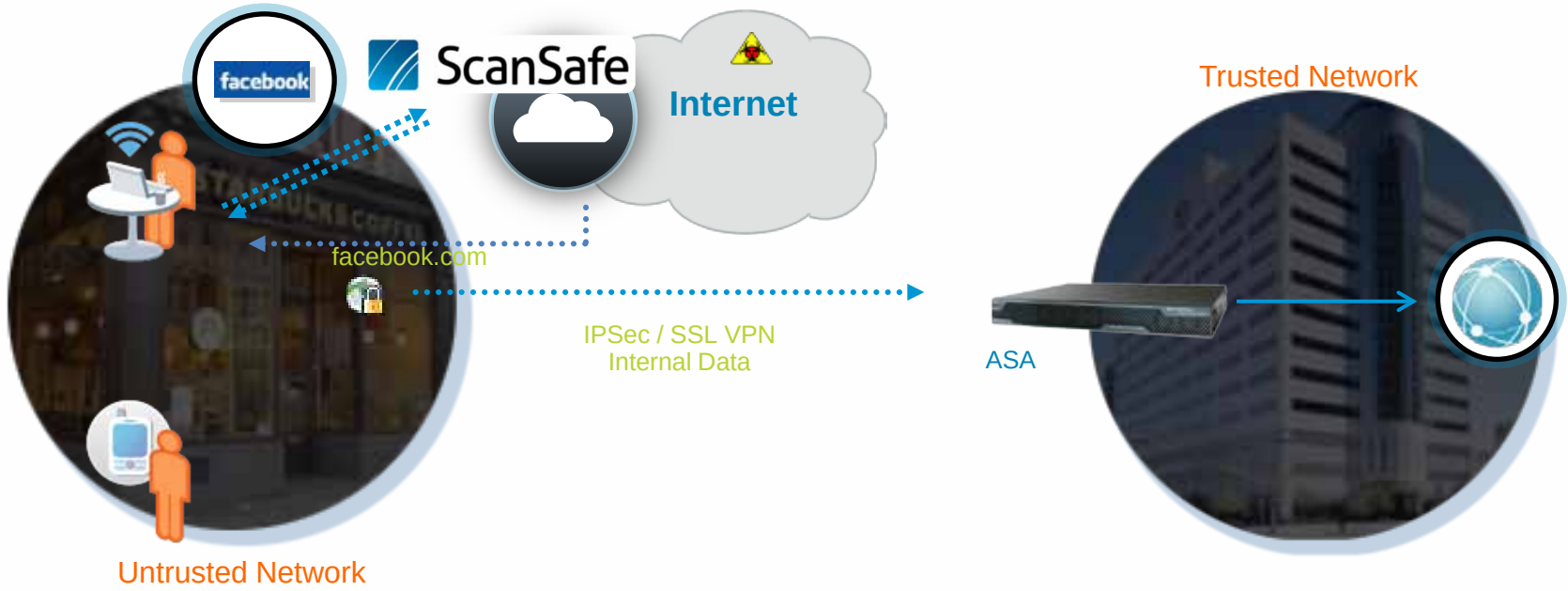
Explicit Proxy Redirection



Explicit Proxy Redirection



Cisco AnyConnect Secure Mobility with Cloud Web Security



AnyConnect

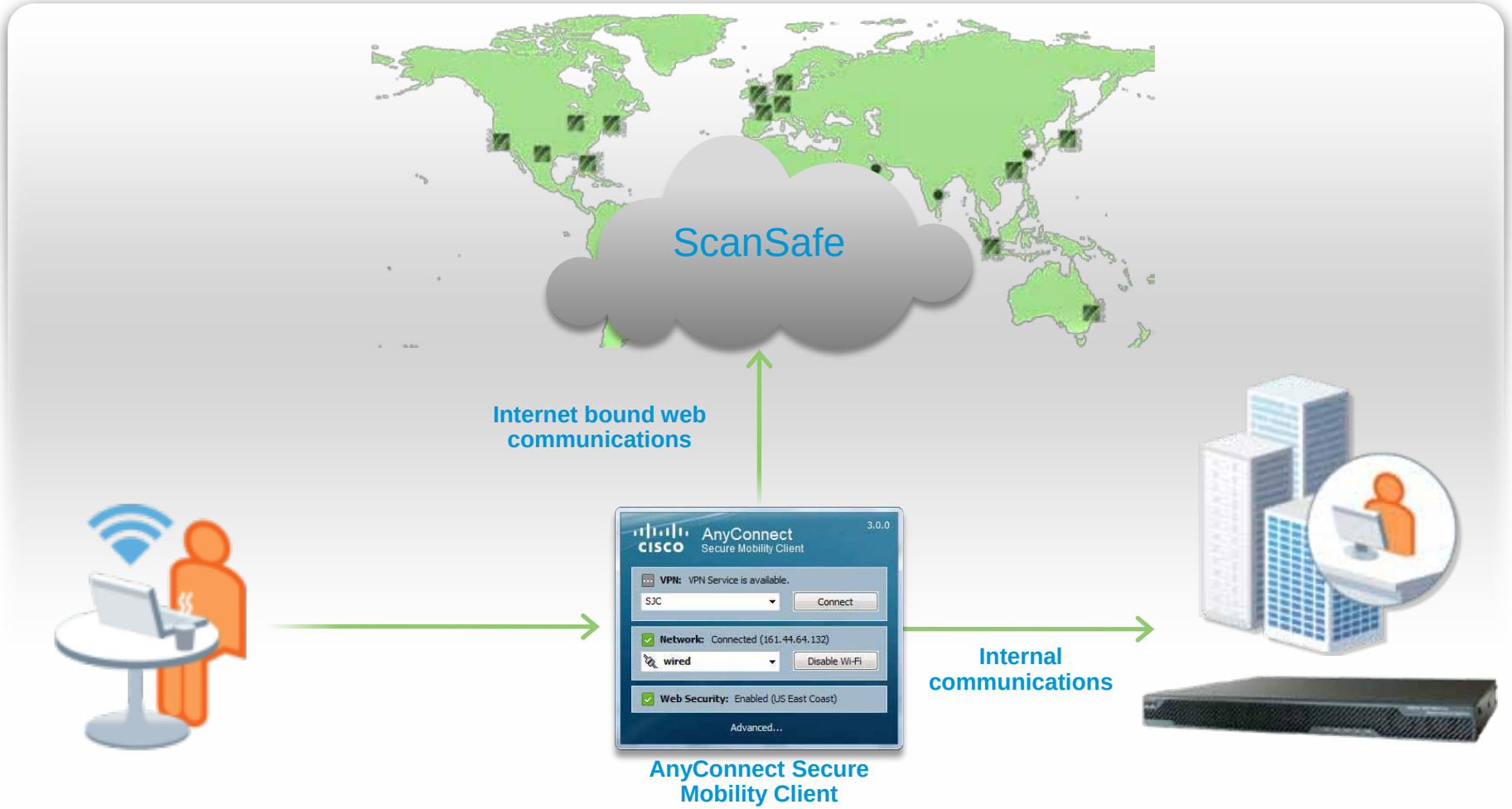
- Always-on VPN (admin configurable)
- Optimal head end auto-detect
- Transparent auth (certificate)

ScanSafe

- Web 2.0 Content Control
- Dynamic Web Classification
- Search Ahead
- Outbreak Intelligence

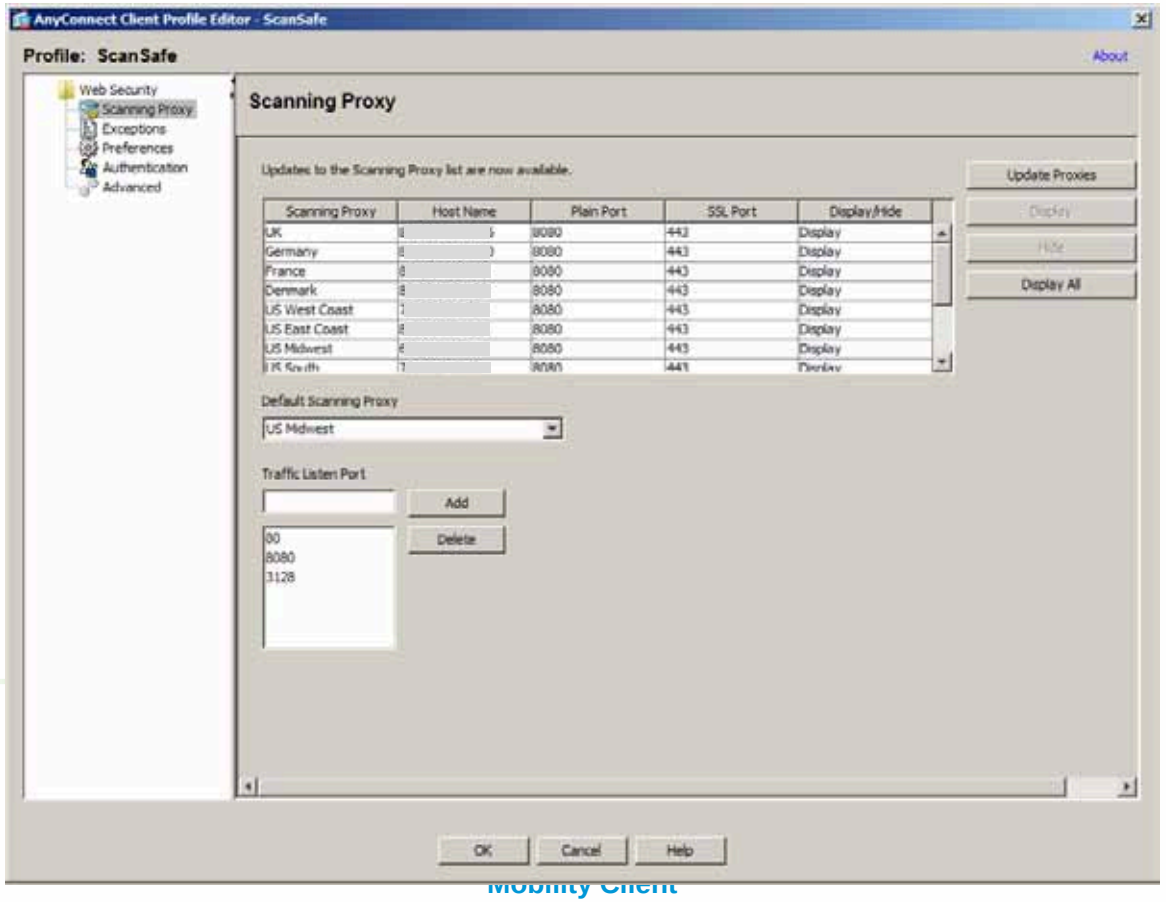
AnyConnect 3.0
Web Security with ScanSafe

Knowledge Is Power.
Learn. Share. Collaborate.



AnyConnect 3.0
Web Security with ScanSafe

Knowledge Is Power.
Learn. Share. Collaborate.



Mobility Client

Feature Highlights

Cisco AnyConnect Secure Mobility Features

AnyConnect

- Trusted Network Detection
- Session Persistence
- Optimal Gateway Selection
- Always-on VPN
- Enhanced Device Support
- IPSec IKEv2
- Network Access Manager
- Telemetry
- SCEP Enrollment

ASA Firewall

- AnyConnect Secure Mobility Head End Support
- Optimized WSA Traffic handoff
- Simplified Management
- Enterprise firewall
- Remote Access Head End
- BotNet Filter

Web Security Appliance

- Remote Specific Policy
- Application Controls
- SaaS Access Control
- Multi-layer malware defense
- URL filtering & Dynamic Categorization
- Data Security
- Application Visibility and Control

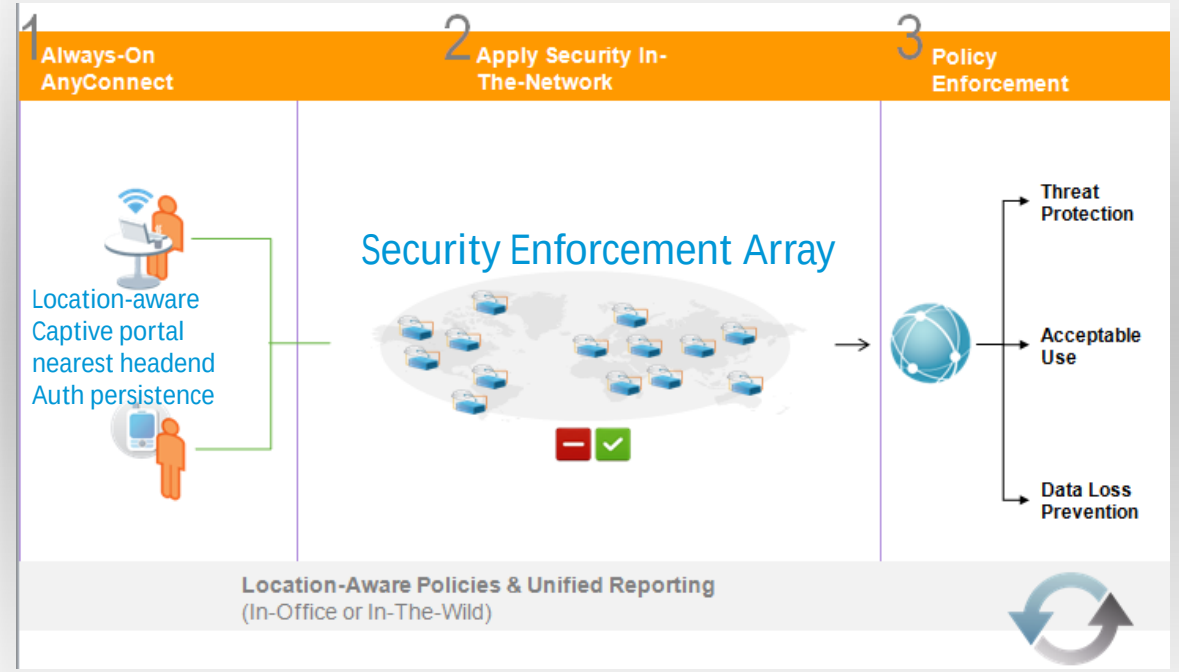
Cloud Web Security

- Web 2.0 Content Control
- Dynamic Web Classification
- HTTP/s Scanning
- Search Ahead
- Outbreak Intelligence
- Real-Time Content Analysis

- Acceptable Use / Control
- Malware Defense

Cisco AnyConnect Secure Mobility Always On

Knowledge Is Power.
Learn. Share. Collaborate.



Security Persistence with Always On VPN (Fail Closed or Fail Open)

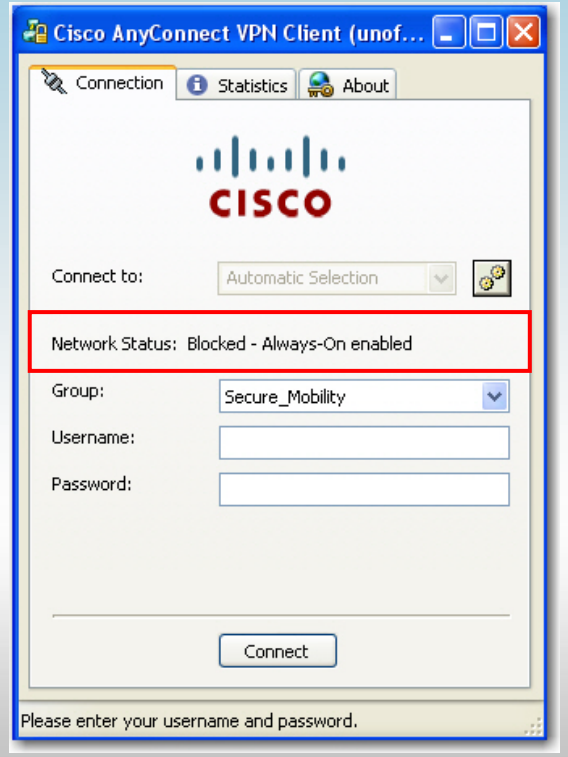
- Always On VPN extends the virtual perimeter to the endpoint
- § Security Persistence and policy are administratively controlled
- § If ASA head-end is unreachable,
  - § fail-open (direct network access)

  or
  - § fail-close (no network access)

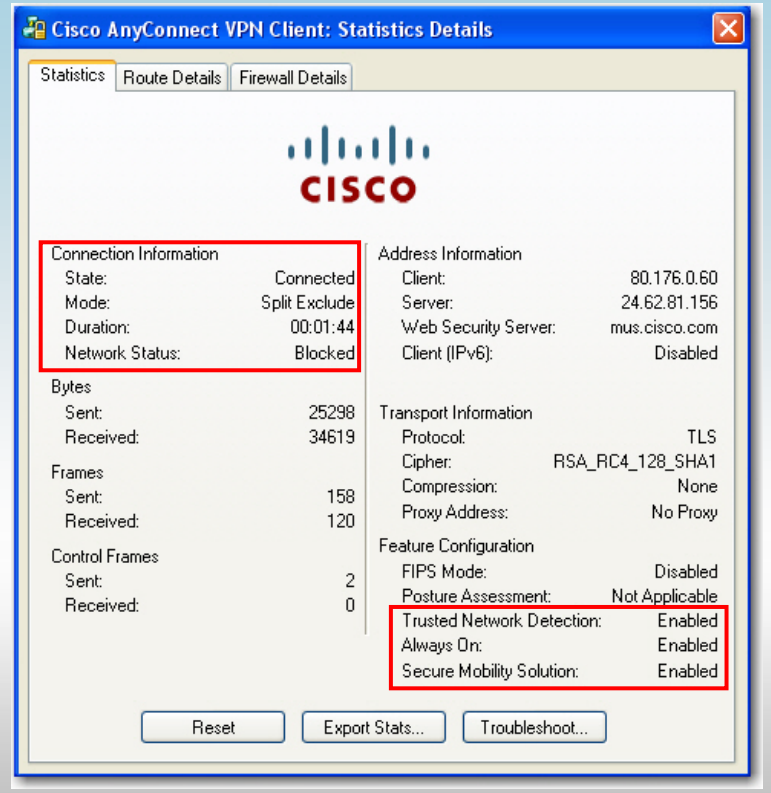
Cisco AnyConnect Secure Mobility Session Persistence

Knowledge Is Power.
Learn. Share. Collaborate.

§ Always-On, Failed Closed
§ No Network Access Available
§ Manual URL Entry is not Allowed

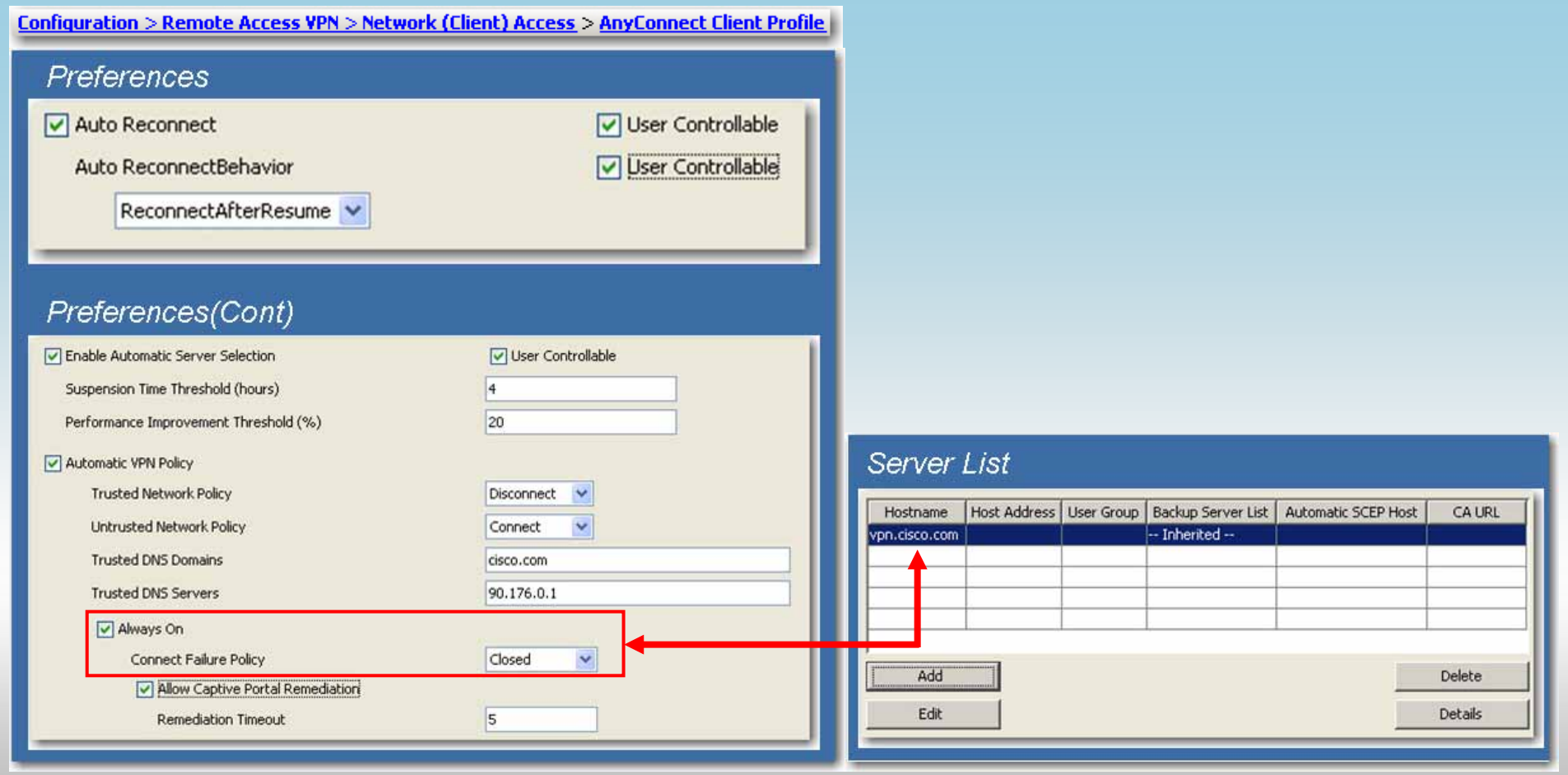


§ Connection Status



AnyConnect Always-On ASDM Profile Configuration

Knowledge Is Power.
Learn. Share. Collaborate.



Trusted Network Detection
Intelligent Mobility

Knowledge Is Power.
Learn. Share. Collaborate.

Trusted Network Detection

In Office

Out of Office

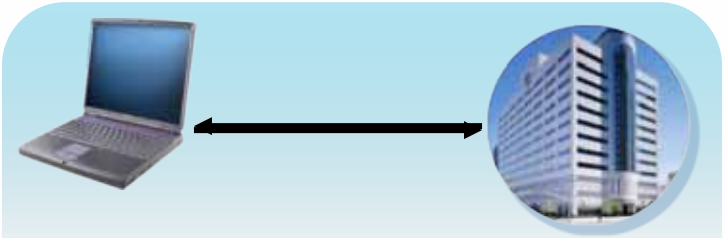
- **Automatically connects or disconnects under the following conditions**:
  - In Office
  - Out of Office
- Location determination made by Default Domain Name or DNS server IP
  - Other checks likely in future
- Certificate authentication for seamless reconnection
- Administratively controlled policy
- Windows XP, Vista, 7 & Mac OS X

Trusted Network Detection

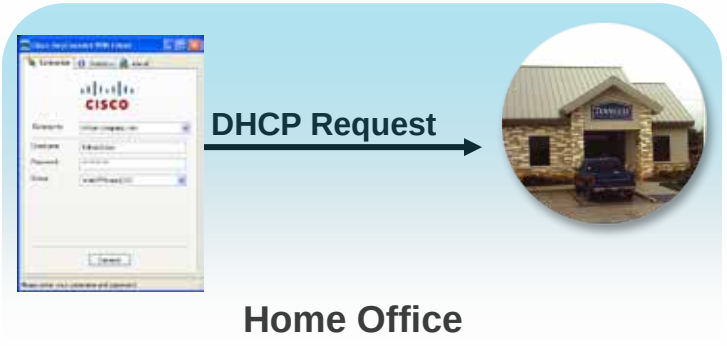
Knowledge Is Power.
Learn. Share. Collaborate.

Detects Trusted or Untrusted Network Infrastructures for Secure Connectivity

- **Trusted Network Detection is Configurable VIA the AnyConnect Profile**
- **Trusted Networks can be Defined as DNS Suffixes or DNS Server IP Addresses**
- **DNS Suffixes and DNS Server IP Addresses must be defined on the Client Workstation Dynamically (DHCP)**
- **If Both the Trusted DNS Suffix and DNS Server IP Address are Defined, the Entries will be ANDed to Determine the Trusted Network**



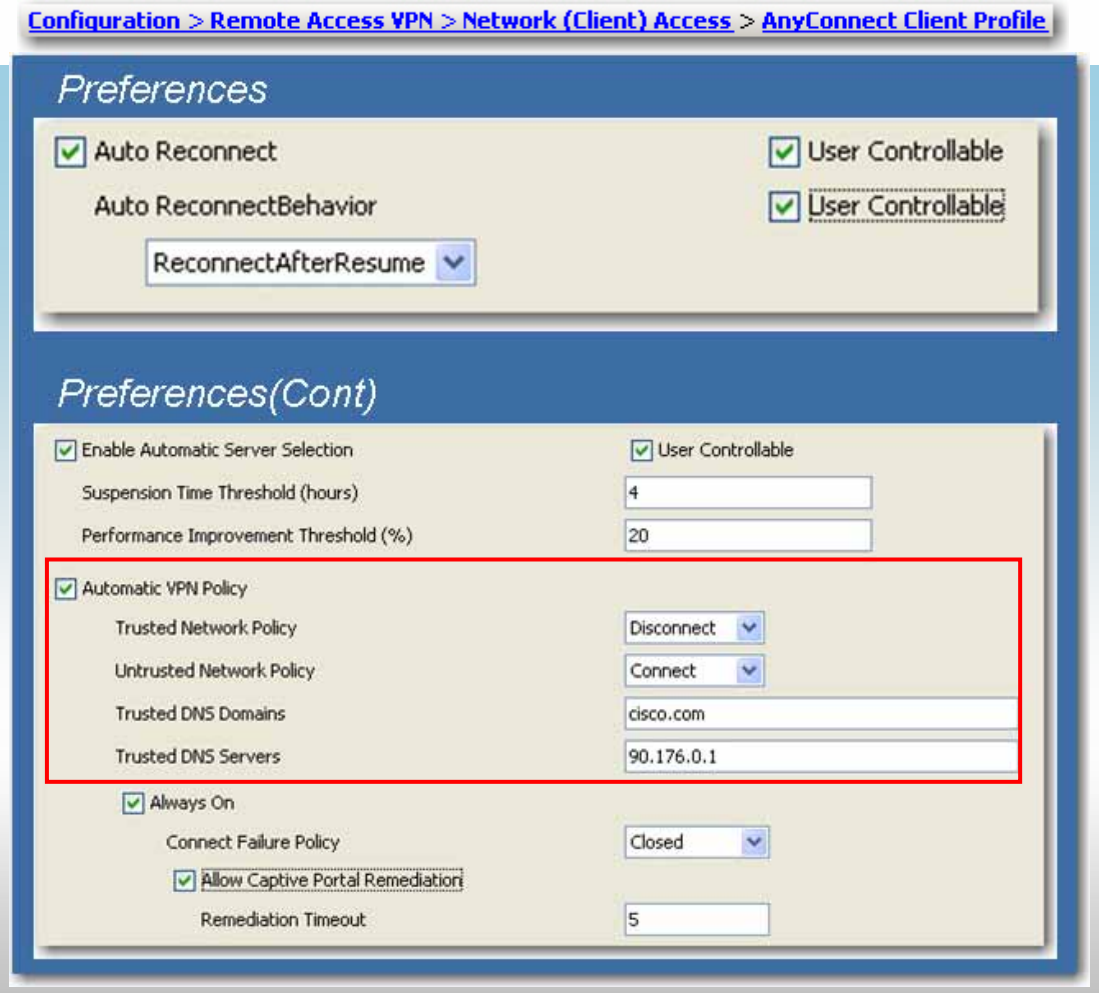
Corporate Headquarters



Home Office

Trusted Network Detection

ASDM Profile Configuration

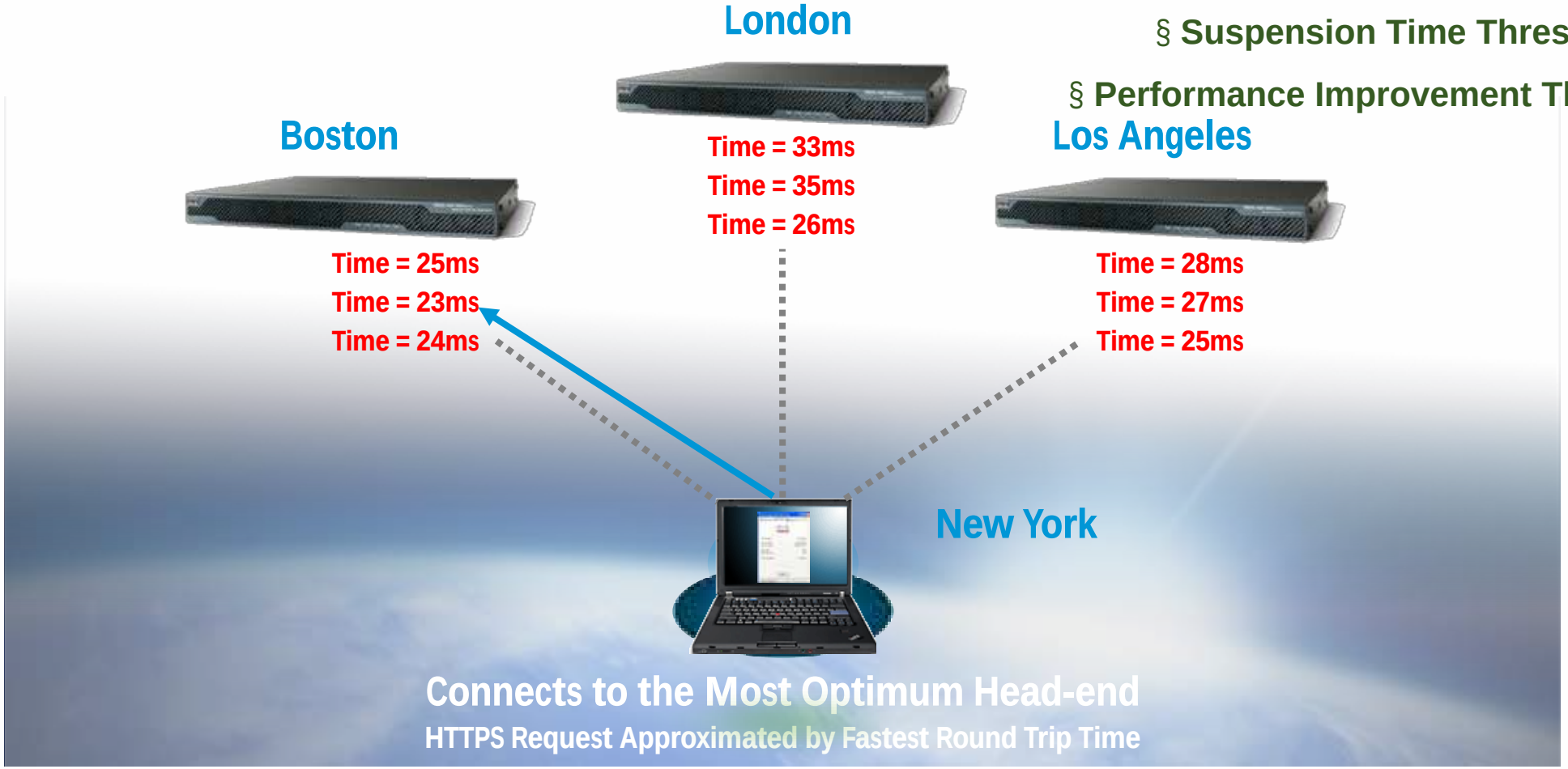


Optimal Gateway Selection

Knowledge Is Power.
Learn. Share. Collaborate.

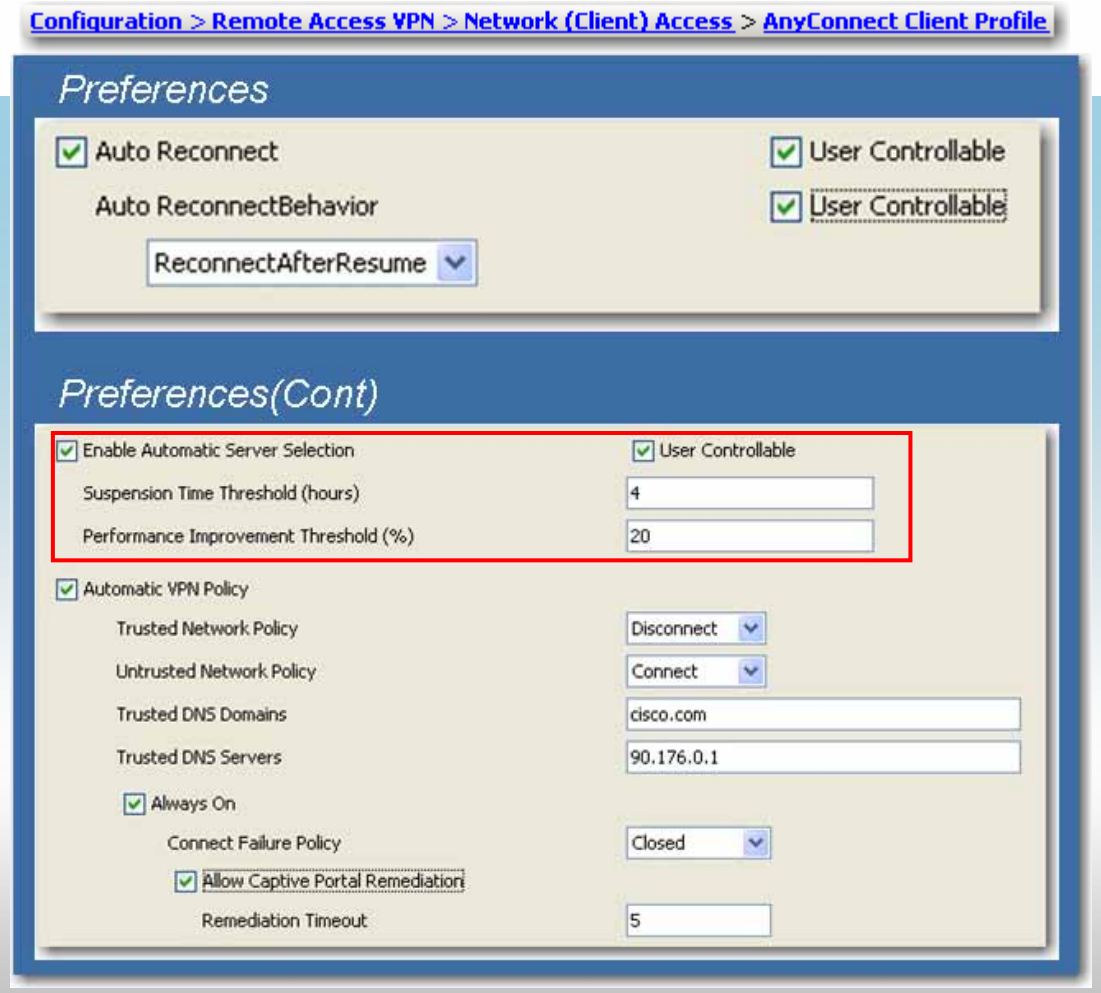
Feature Parameters:

- **Suspension Time Threshold (hours)**
- **Performance Improvement Threshold (%)**



Optimal Gateway Selection

ASDM Profile Configuration



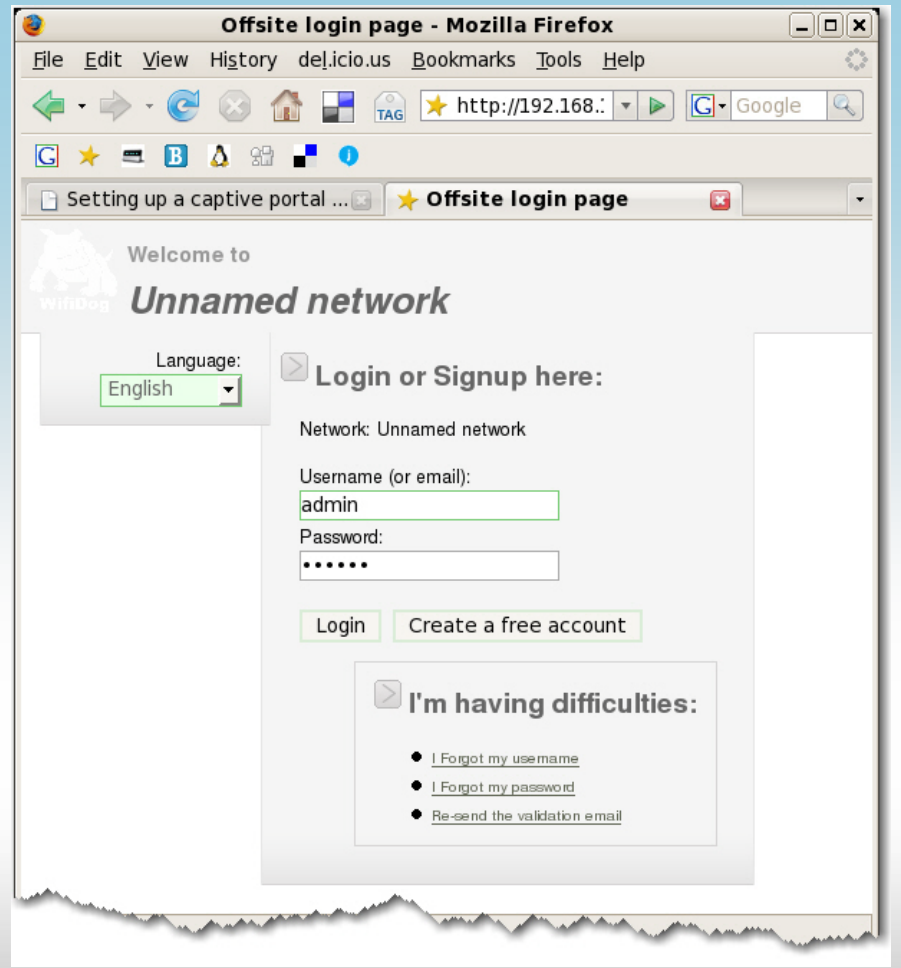
Captive Portal Detection

Knowledge Is Power.
Learn. Share. Collaborate.

§ Always-On enforces VPN connectivity.

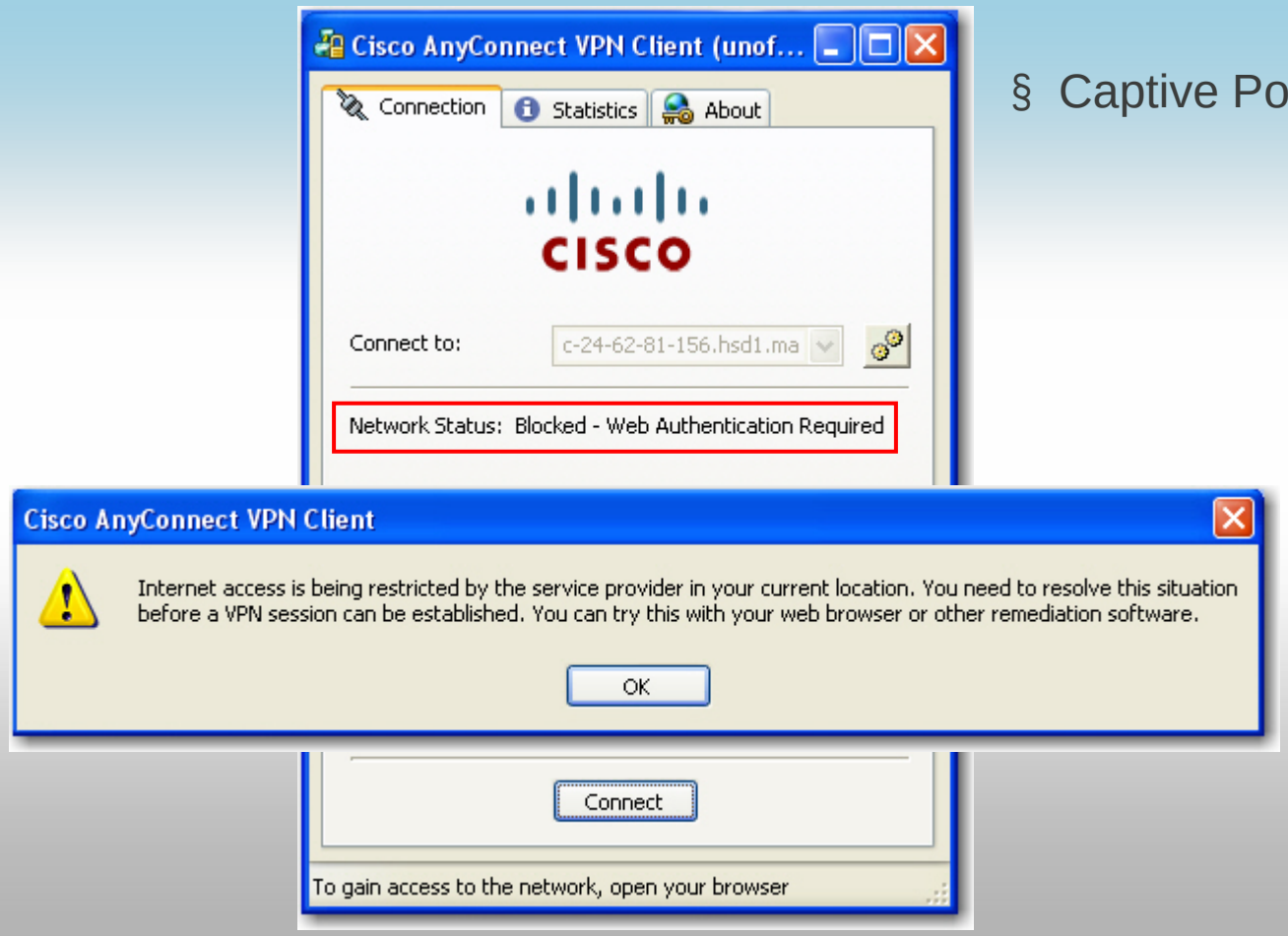
§ If AnyConnect fails to connect, its endpoint can fail closed, preventing network connectivity to and from the endpoint.

§ Always-On allows AnyConnect users to remediate their Captive Port prior to required VPN establishment.



Captive Portal Detection

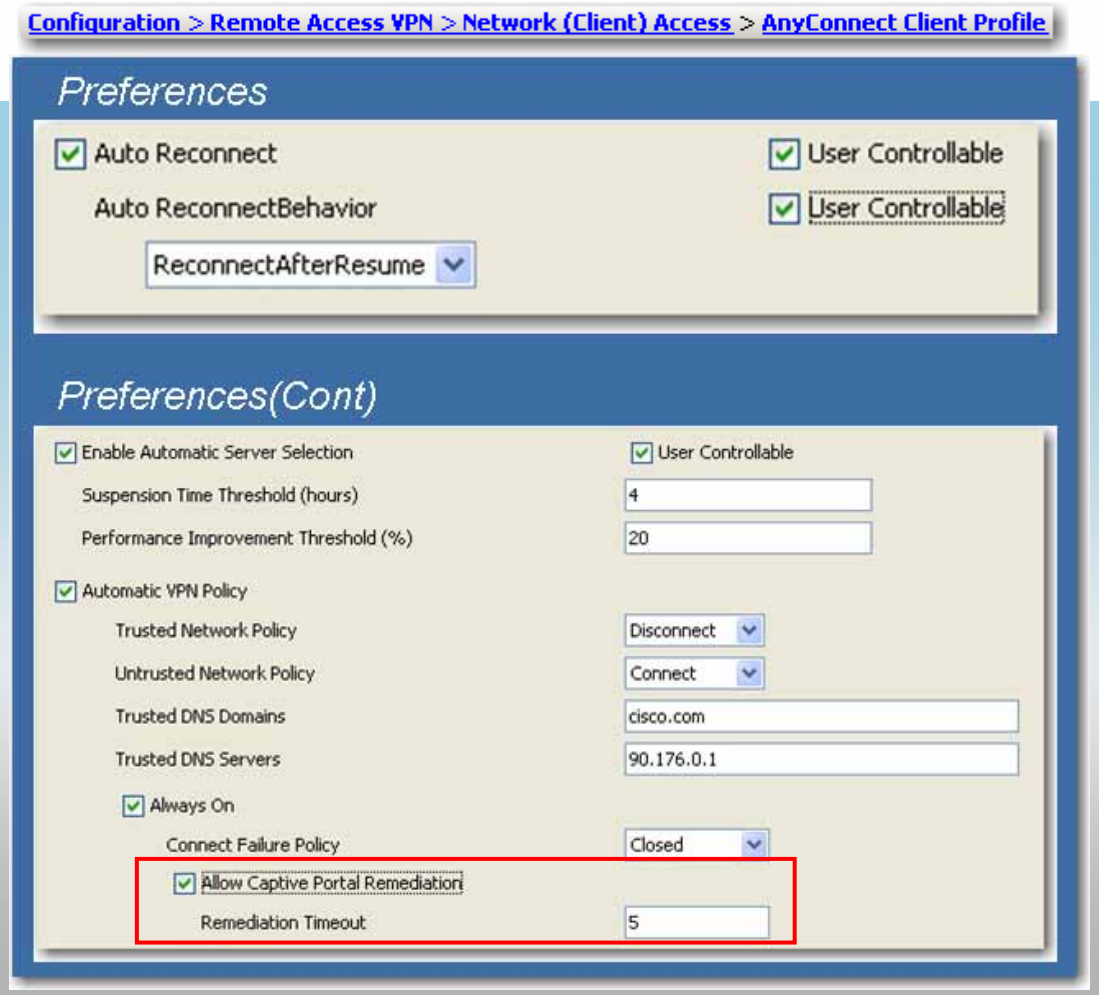
User Experience



- Captive Portal Remediation Required

Captive Portal

ASDM Profile Configuration



AnyConnect Session Persistence

Network Follows Users – It Just Works

Persistent Connectivity

Auto-detect and connect

Transparent handoff

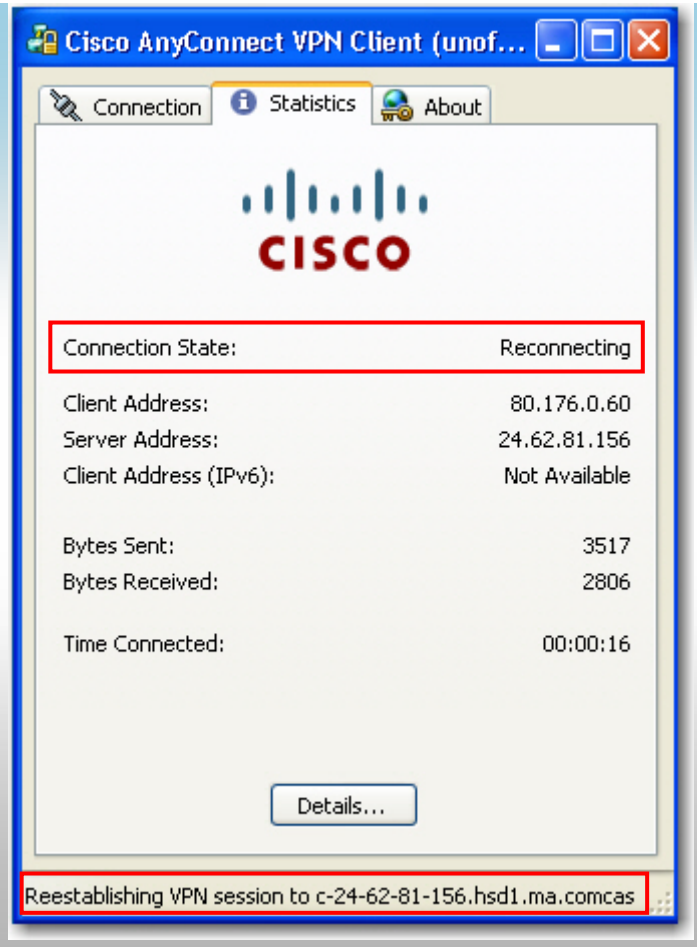
Session persistence

- **VPN session remains connected**
  - While user migrates between networks (3G, WiFi, LAN, etc)
  - During loss of network connectivity
  - During system hibernation / standby
- Administratively controlled policy
- Compatible with all auth methods

User does not re-authenticate after hibernation/standby

Session Persistence

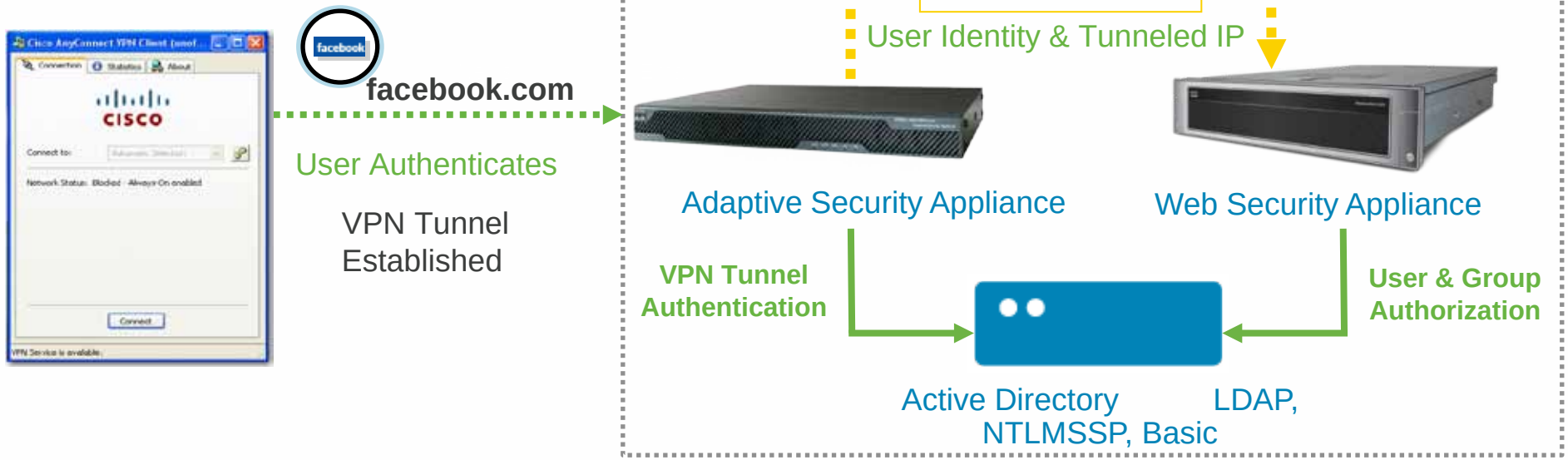
User Experience: User Indicator



- Connection State: Reconnecting

Cisco AnyConnect Secure Mobility

ASA-WSA Communication



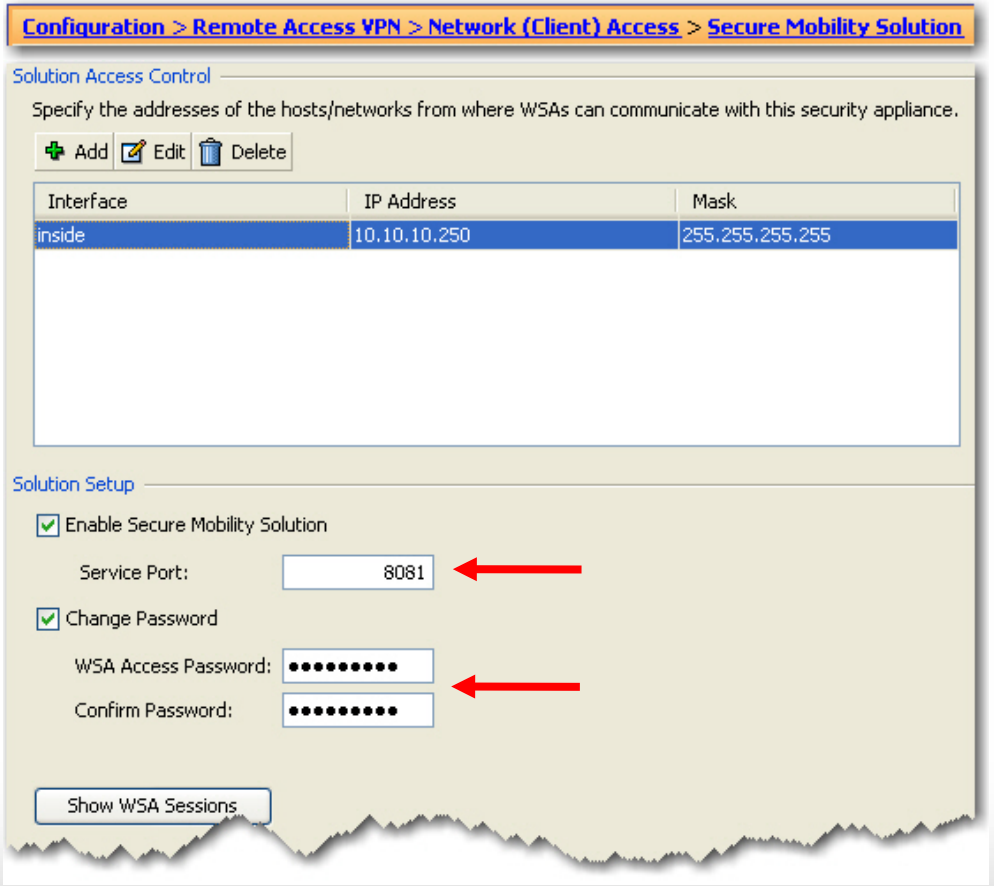
ASA → WSA

1. AnyConnect Authenticates and Establishes a VPN Tunnel to the ASA
2. ASA Extracts Username from Certificate or AAA Server
3. ASA Forwards Username and Tunneled IP Address to the WSA
4. WSA Verifies Username and Group Membership against Active Directory
5. WSA Applies Policies based on Username or Group Membership

ASA > WSA Configuration

ASA to WSA Communication

- ASA & WSA Communication Network
- Enable Secure Mobility Solution
- Services Port
- WSA Access Password

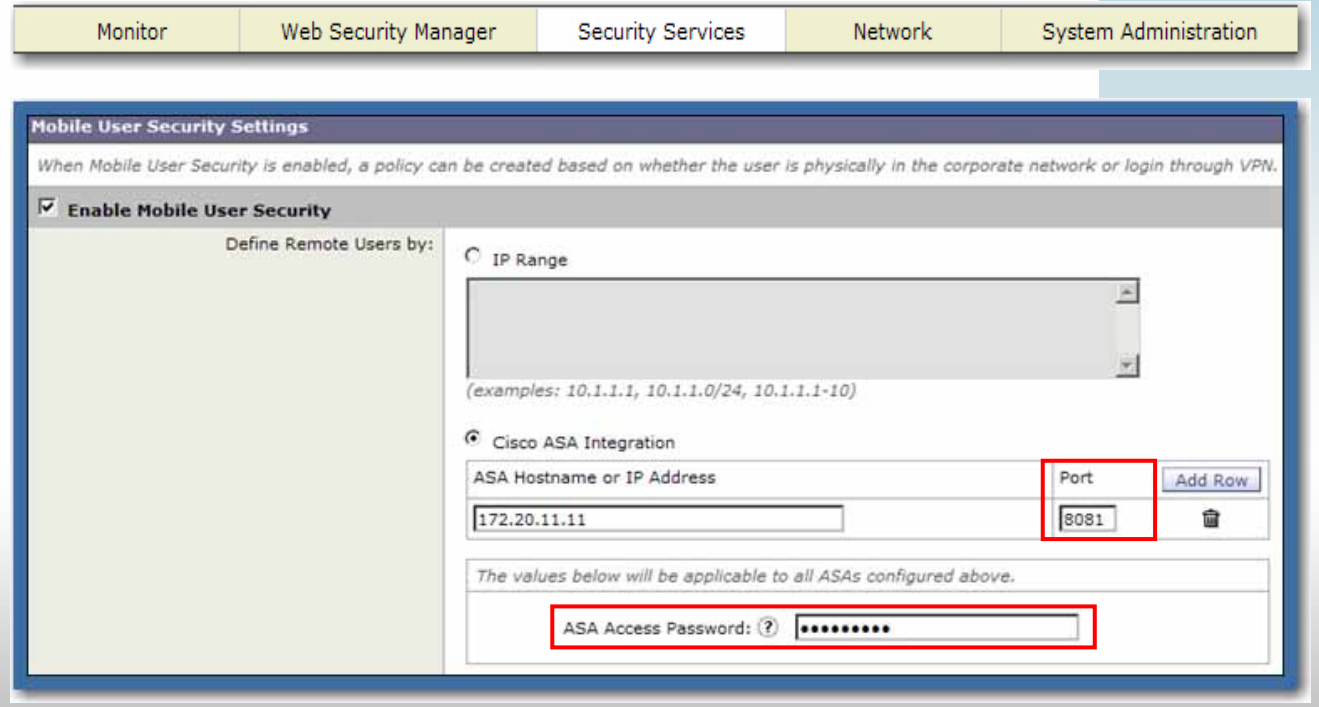


WSA > ASA Configuration

ASA to WSA Communication

Knowledge Is Power.
Learn. Share. Collaborate.

- Enable Secure Mobility Solution
- Enable Cisco ASA Integration
- ASA Hostname or IP Address & Service Port & Access Password

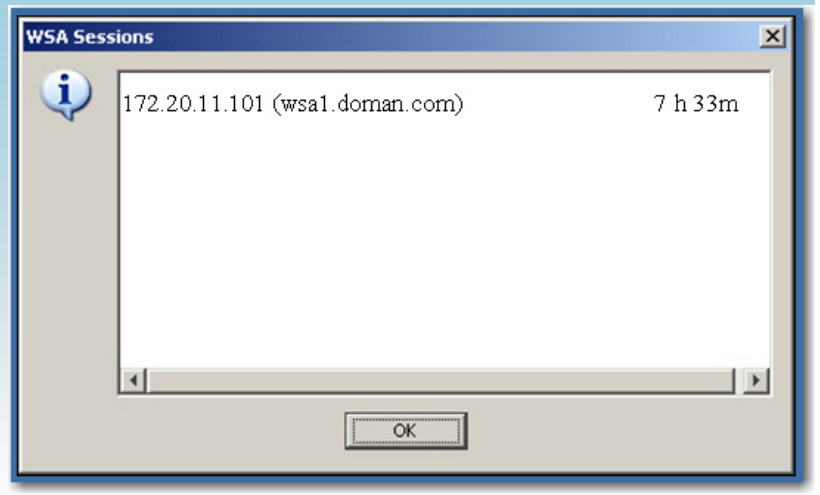


ASA > WSA Configuration

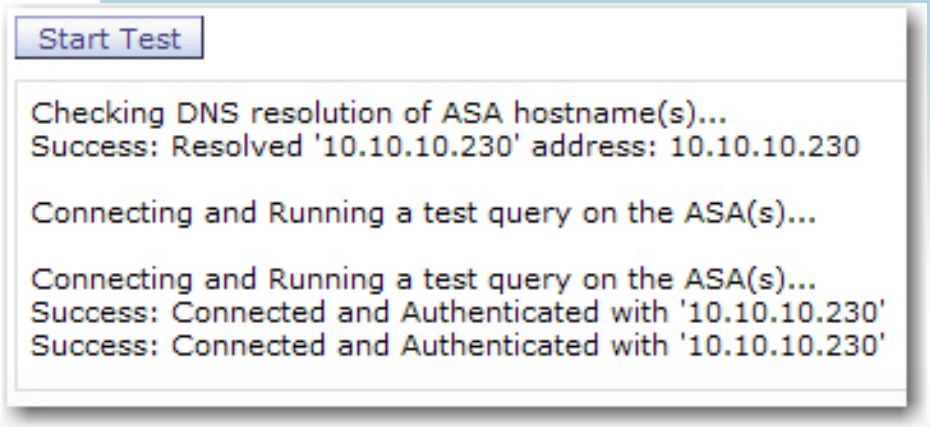
Communication Test

Knowledge Is Power.
Learn. Share. Collaborate.

§ Verify ASA > WSA Communication



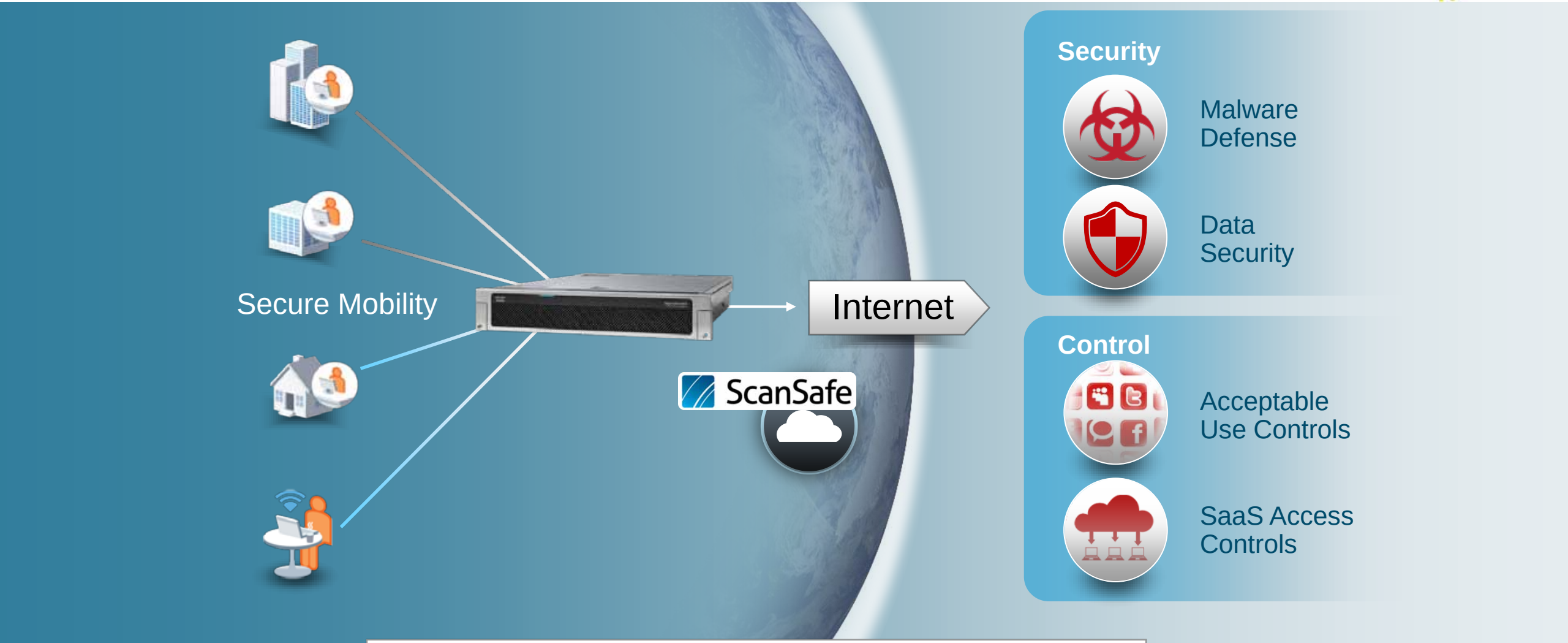
§ Verify WSA > ASA Communication



Policy Enforcement Control / Security

Cisco IronPort Web Security Appliance
Industry Leading Secure Web Gateway

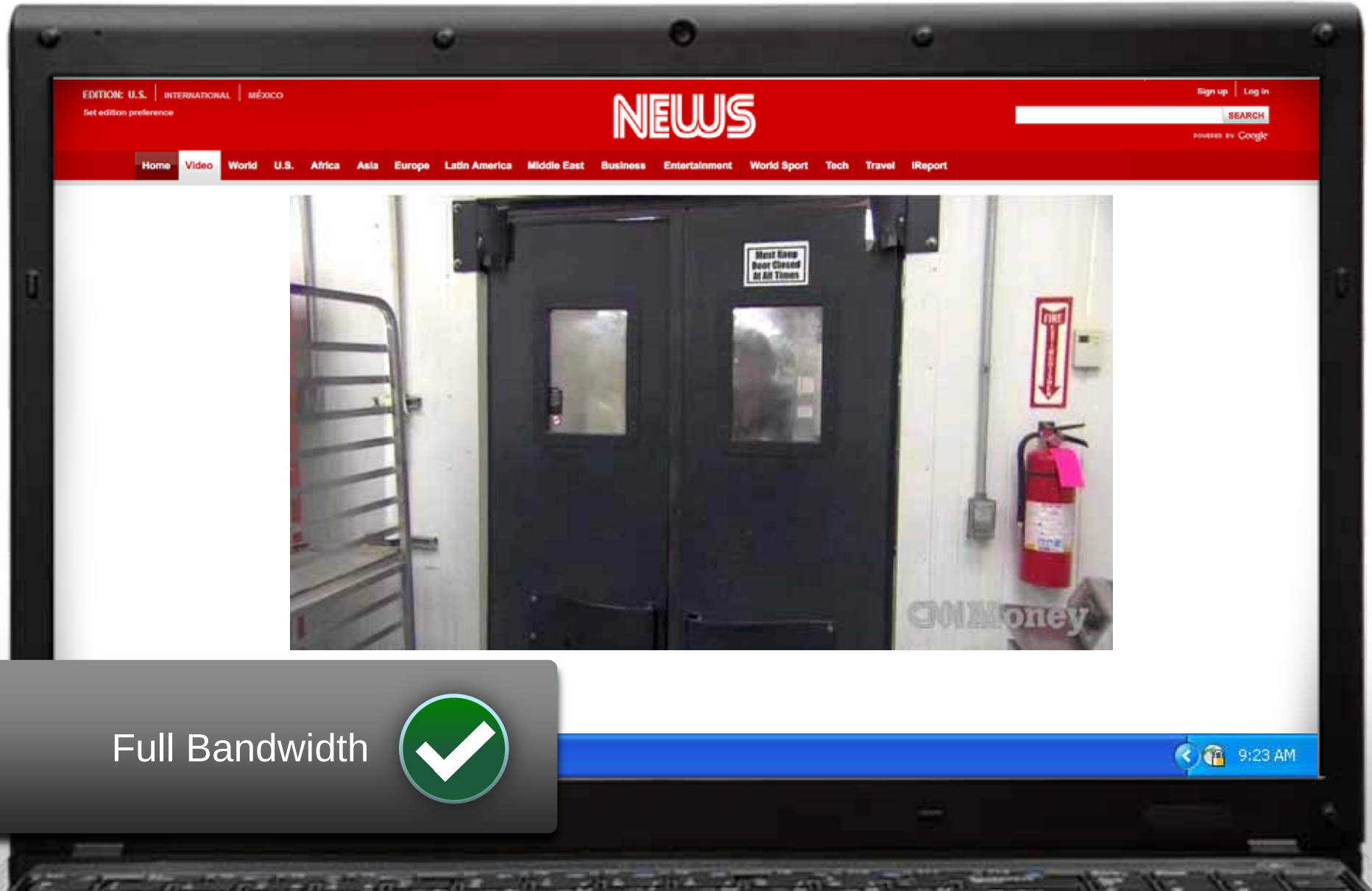
Knowledge Is Power.
Learn. Share. Collaborate.



Controls in Action

Bandwidth Control: Corporate Approved

Knowledge Is Power.
Learn. Share. Collaborate.

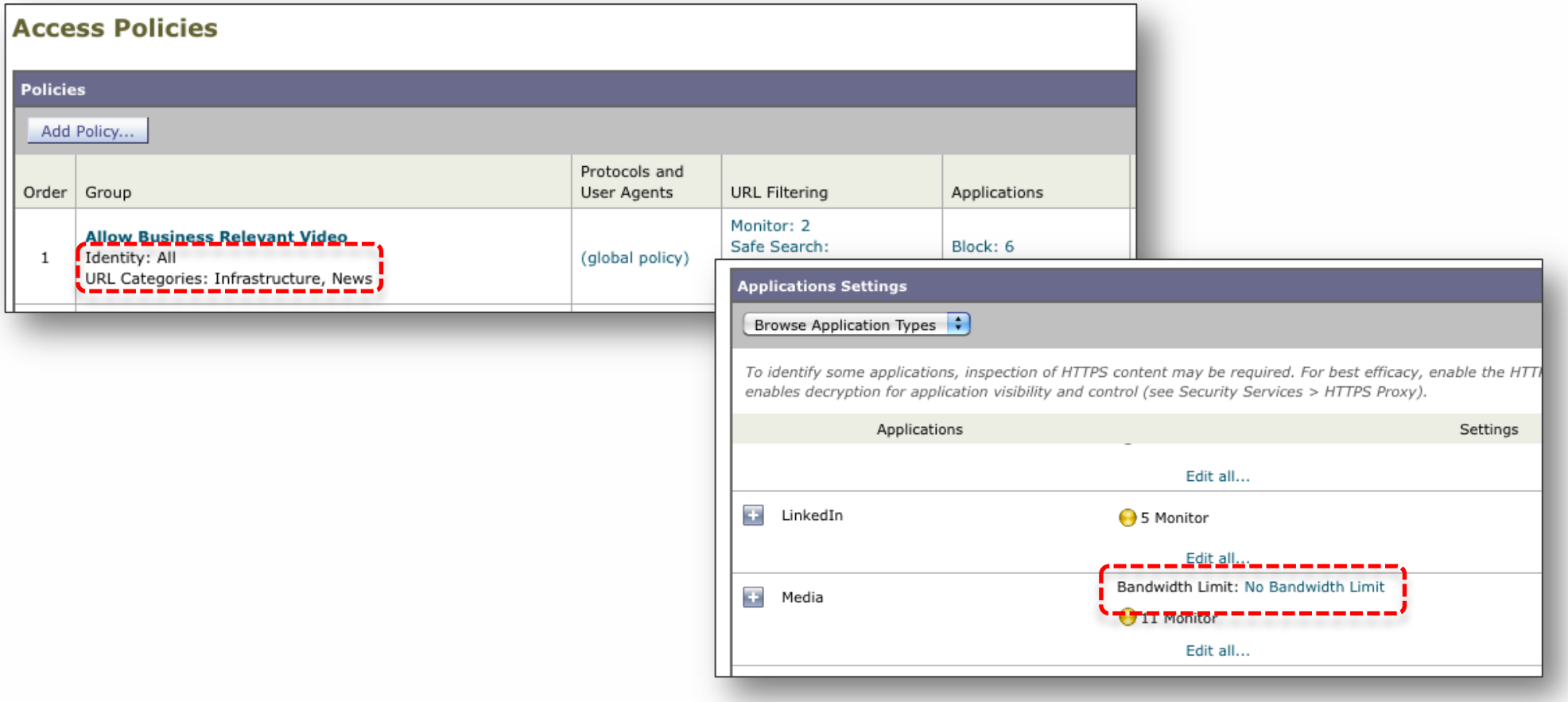


Full Bandwidth

Web Security Appliance Configuration

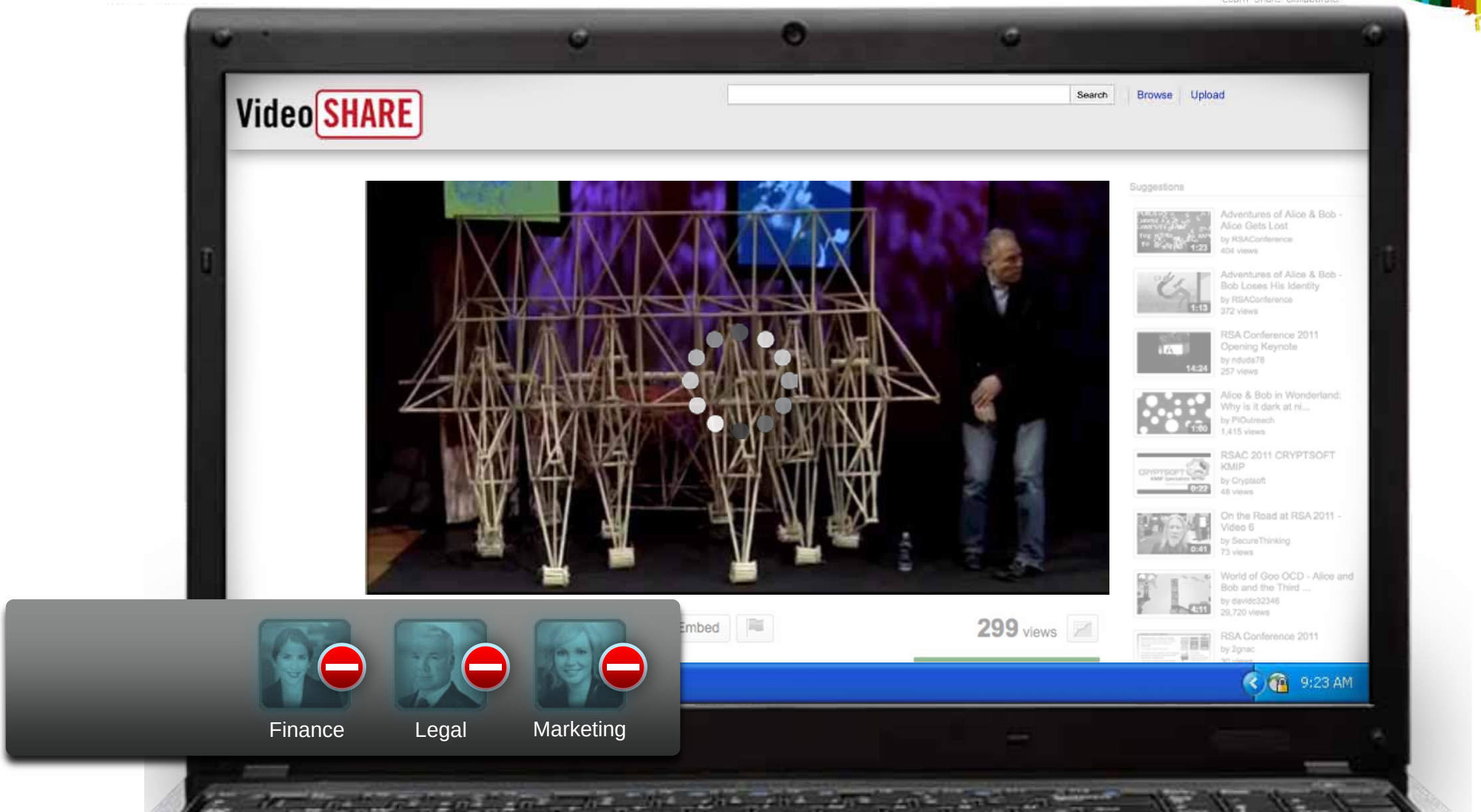
Allow Business Relevant Video

Knowledge Is Power.
Learn. Share. Collaborate.



Bandwidth Control: Restricted

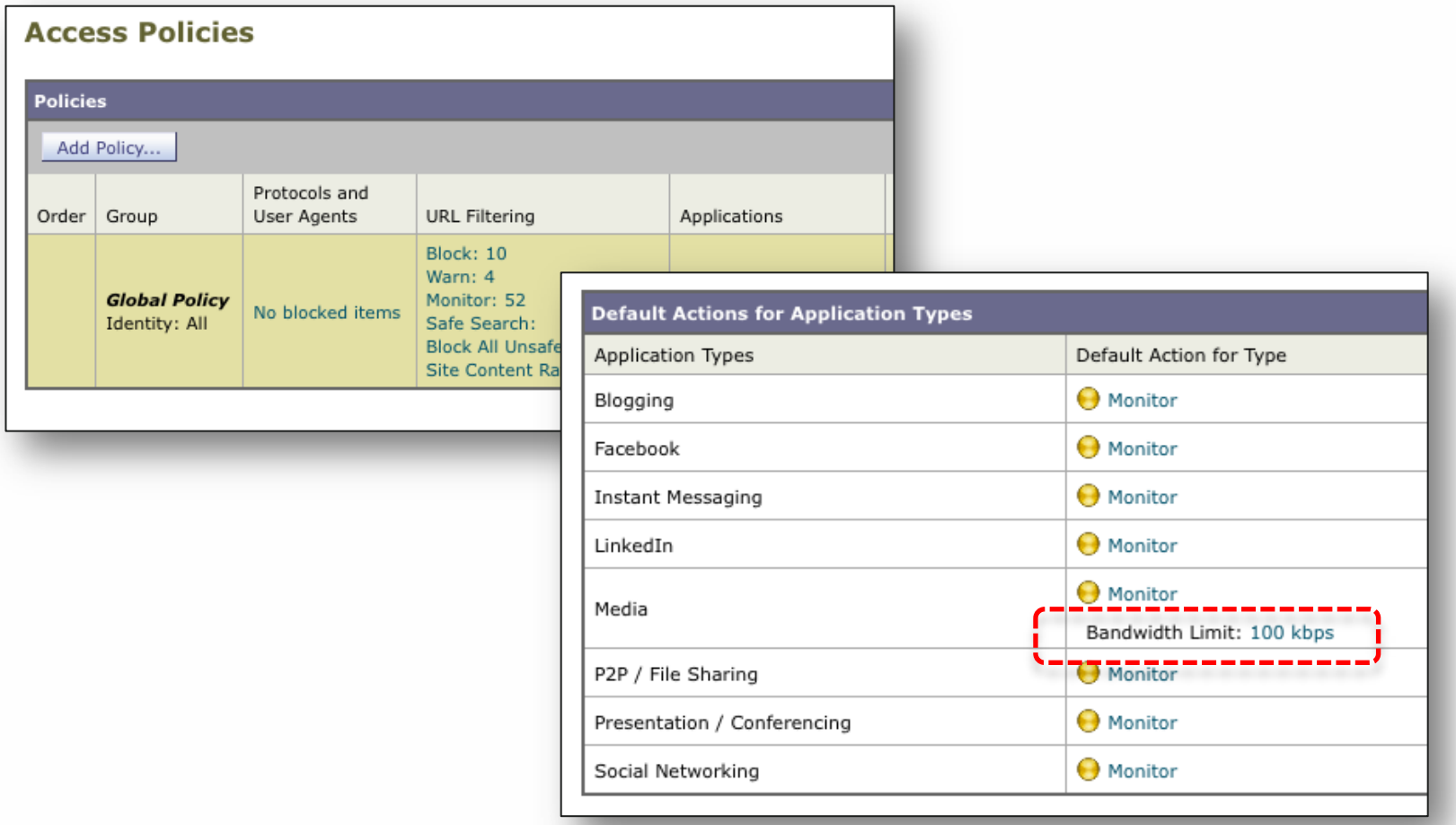
Knowledge Is Power.
Learn. Share. Collaborate.



Web Security Appliance Configuration

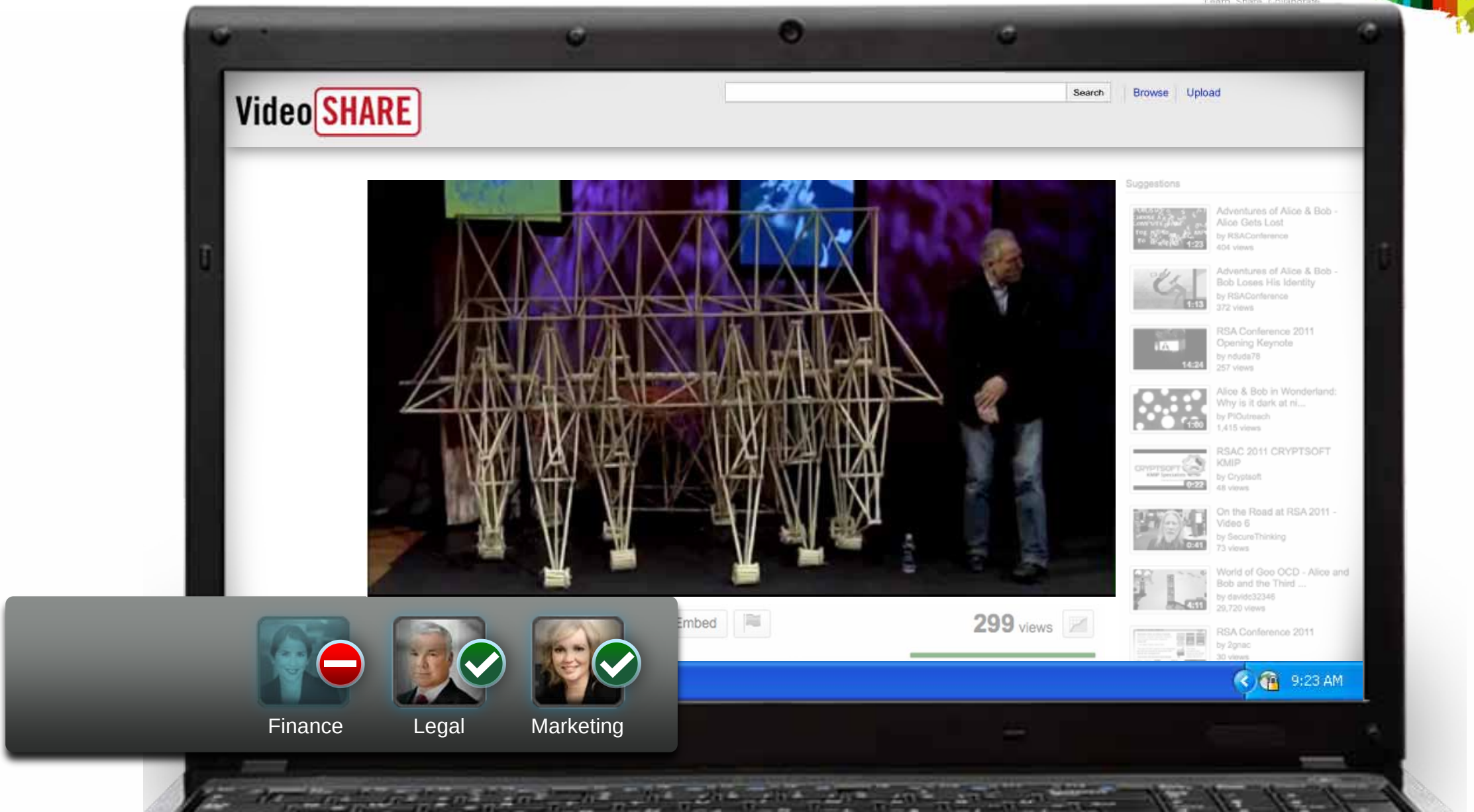
Restrict Media

Knowledge Is Power.
Learn. Share. Collaborate.



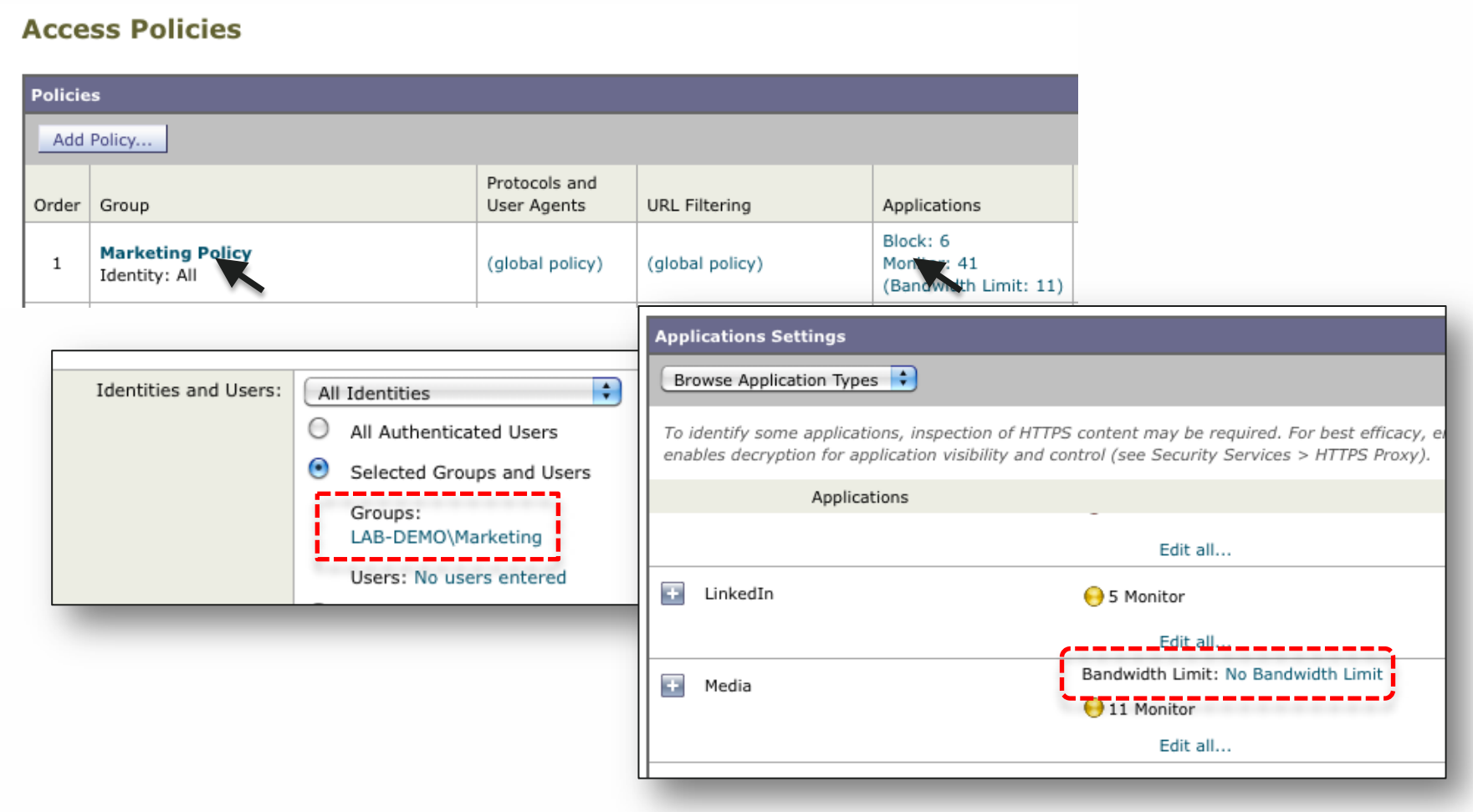
Bandwidth Control: Customized

Knowledge Is Power.



Web Security Appliance Configuration

Override Restrictions



Facebook Controls

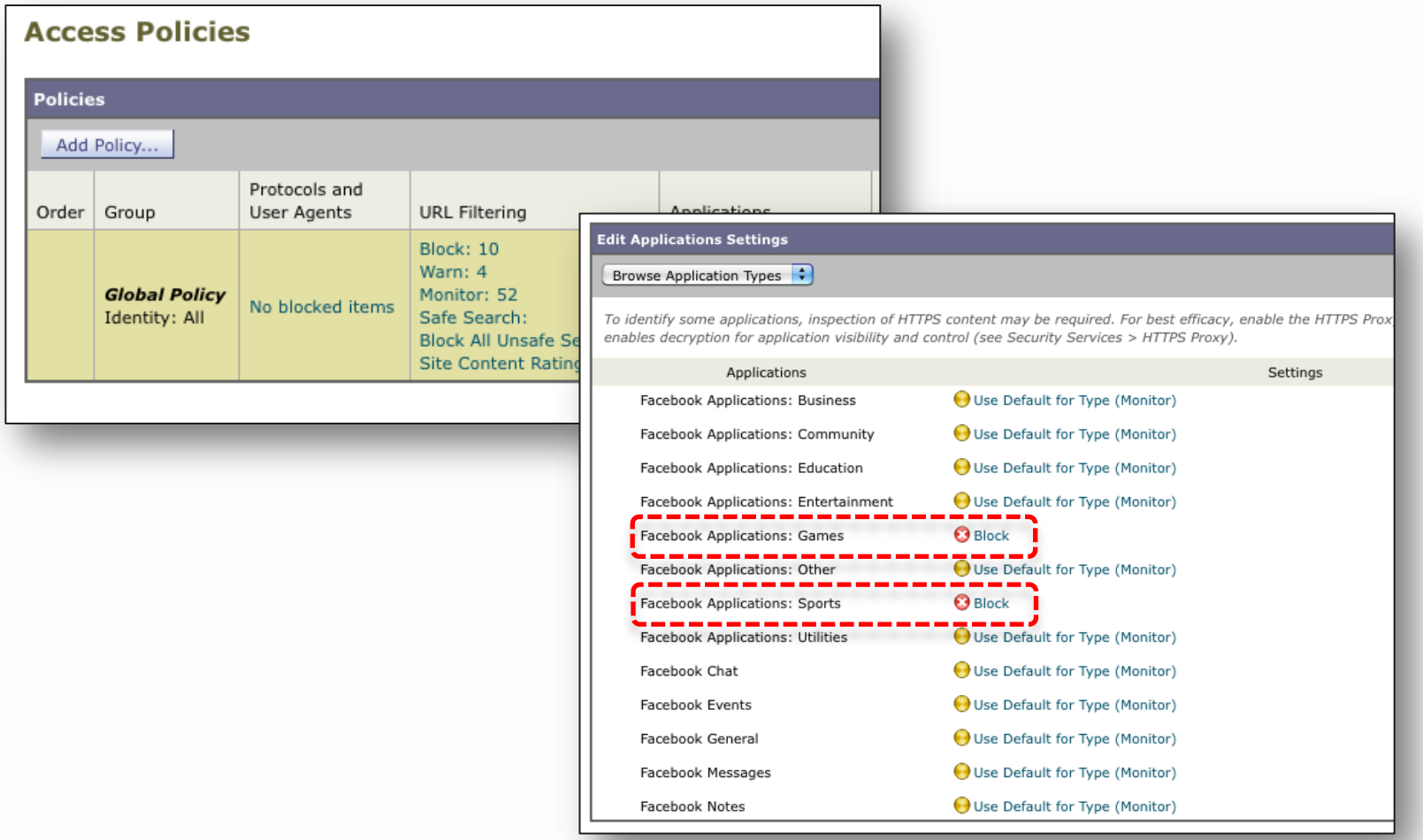
Knowledge Is Power.
Learn. Share. Collaborate.

Facebook Controls

Knowledge Is Power.
Learn. Share. Collaborate.

Web Security Appliance Configuration

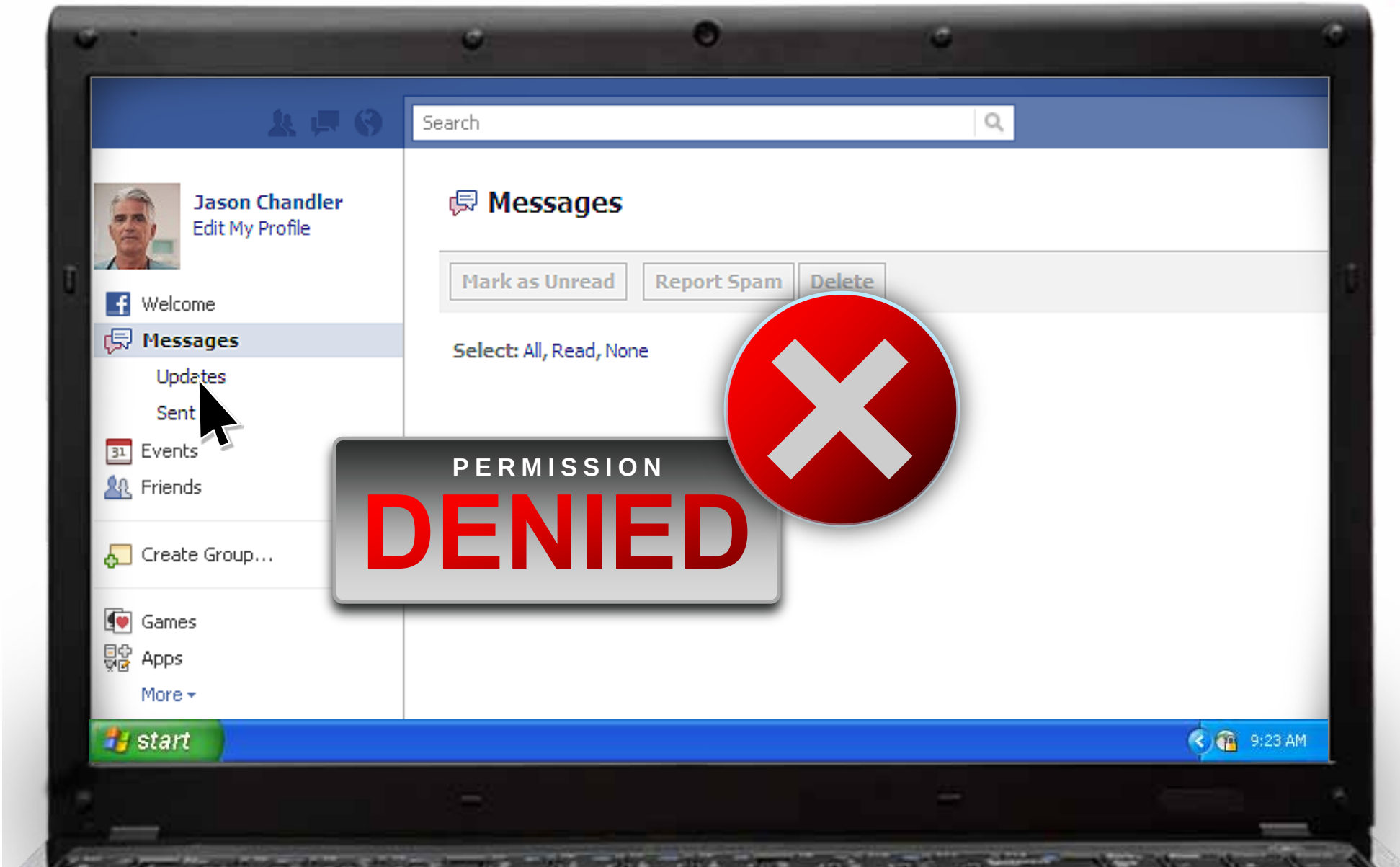
Facebook Control



Facebook Controls

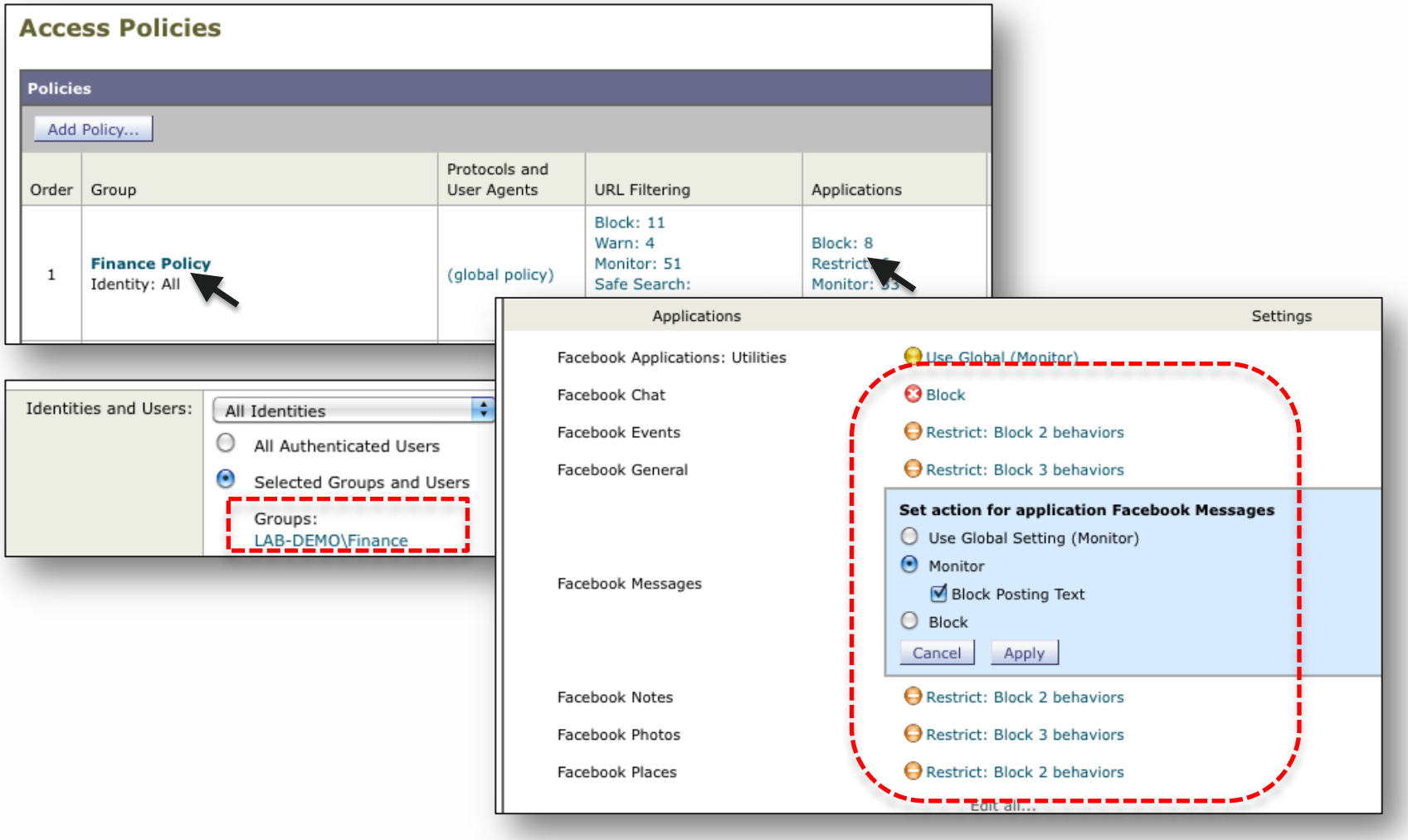
May 19, Toronto, Canada

Knowledge Is Power.
Learn. Share. Collaborate.



Web Security Appliance Configuration

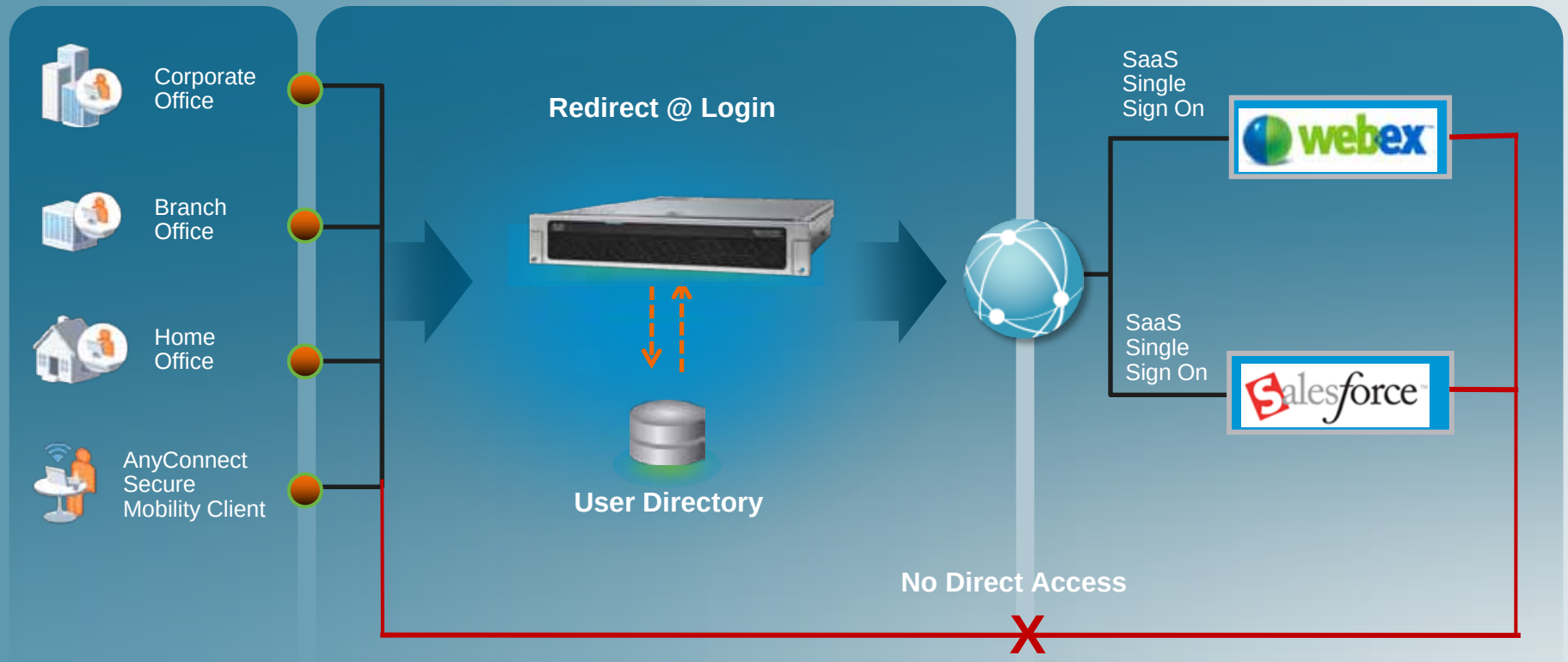
Override Restrictions



SaaS Access Control

Regaining Visibility and Control Through Identity

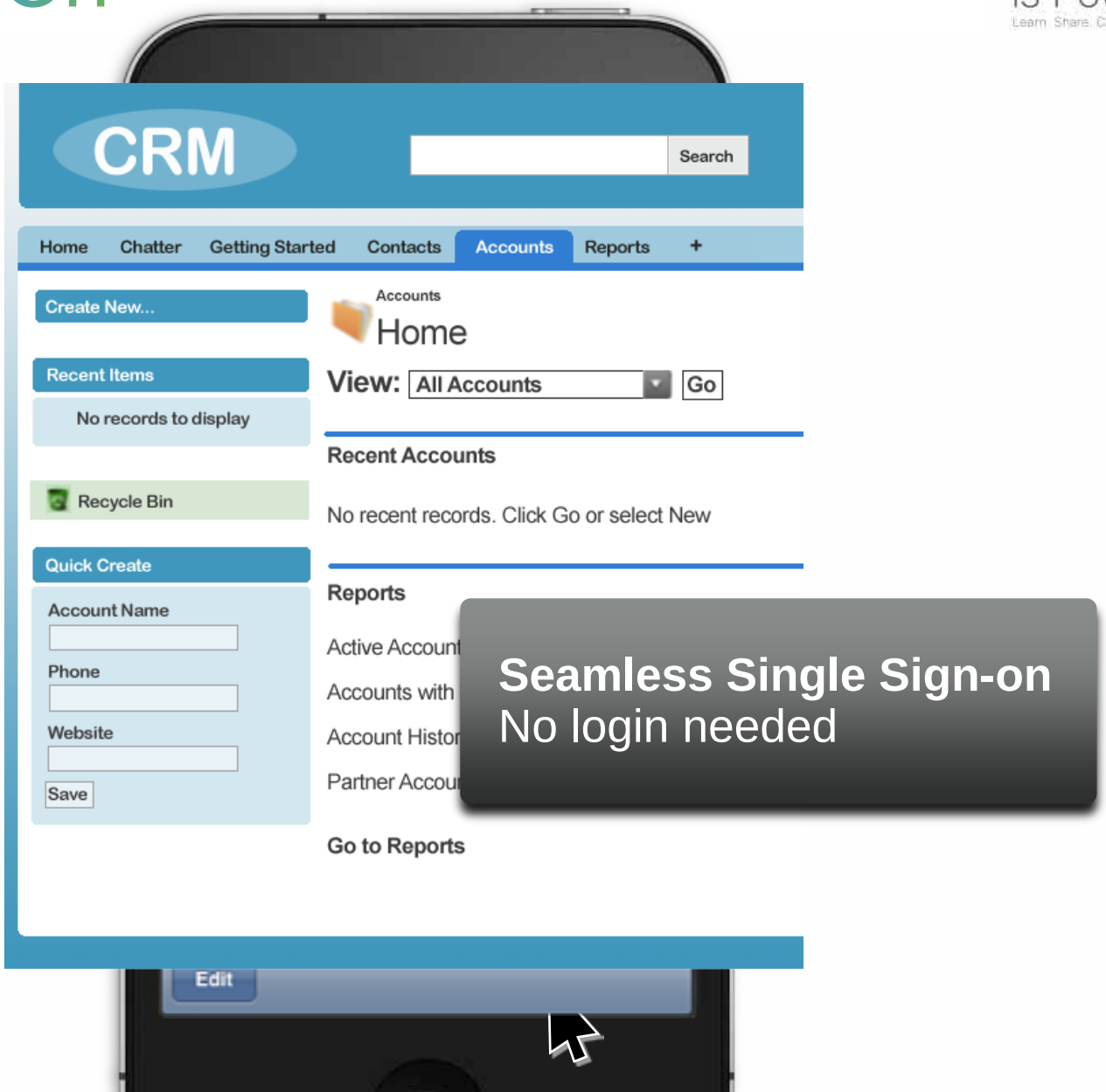
Knowledge Is Power.
Learn. Share. Collaborate.



Visibility | Centralized Enforcement | Single Source Revocation

SaaS Single Sign On

Knowledge Is Power.
Learn. Share. Collaborate.



SaaS Single Sign-On

User Accesses Web Site

Redirect to SAML SSO URL

Browser Requests SSO URL

Javascript POST ACS URL
+ SAML response

POSTS SAML response

Delivers Web User's Portal

Connection Proxied

Redirect to SAML SSO URL

POST proxied to website

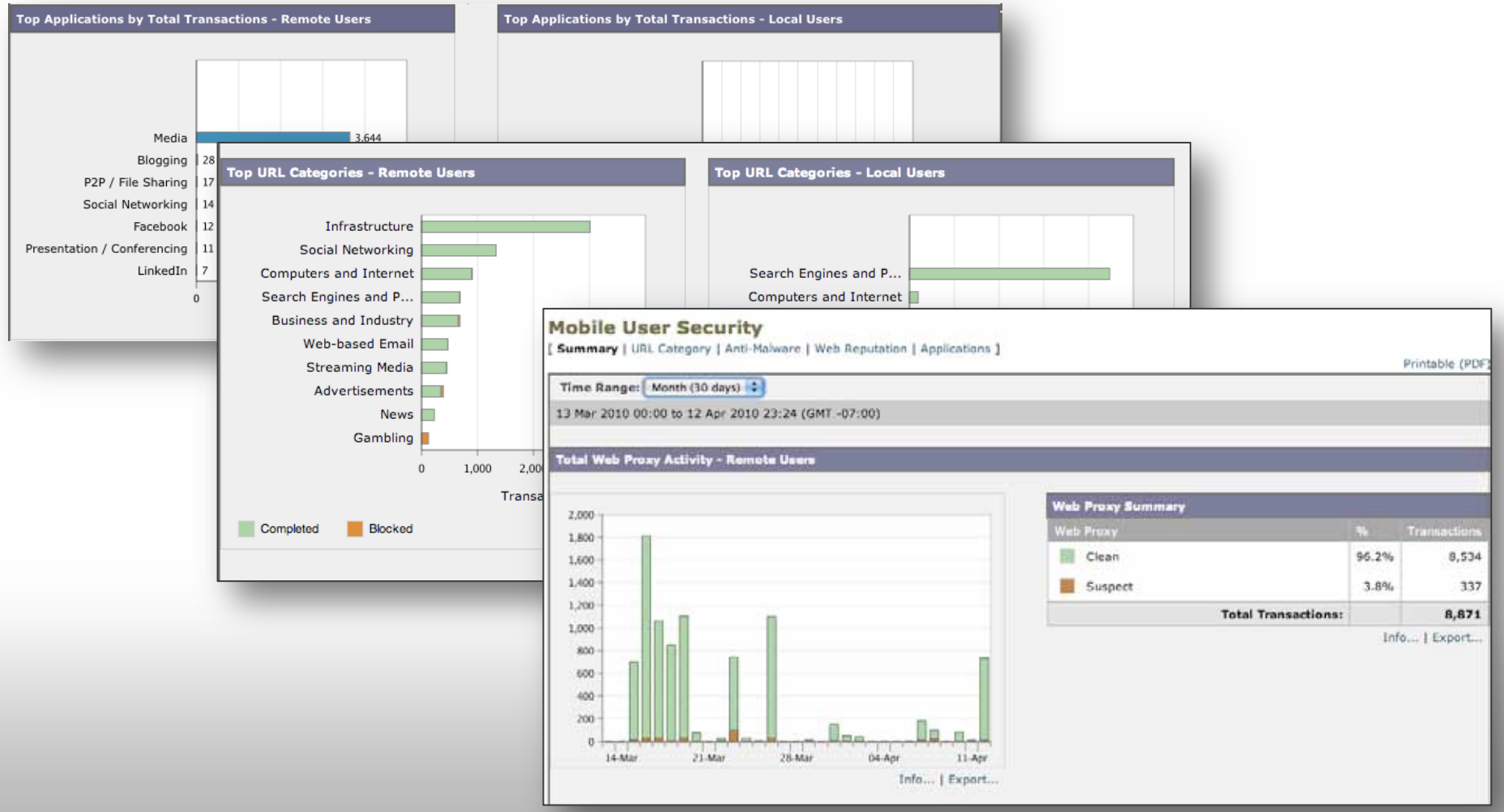
User Logged Into Service

Authenticate
(if unknown)

Secure Mobility Reporting

WSA Mobile User Reports

Knowledge Is Power.
Learn. Share. Collaborate.



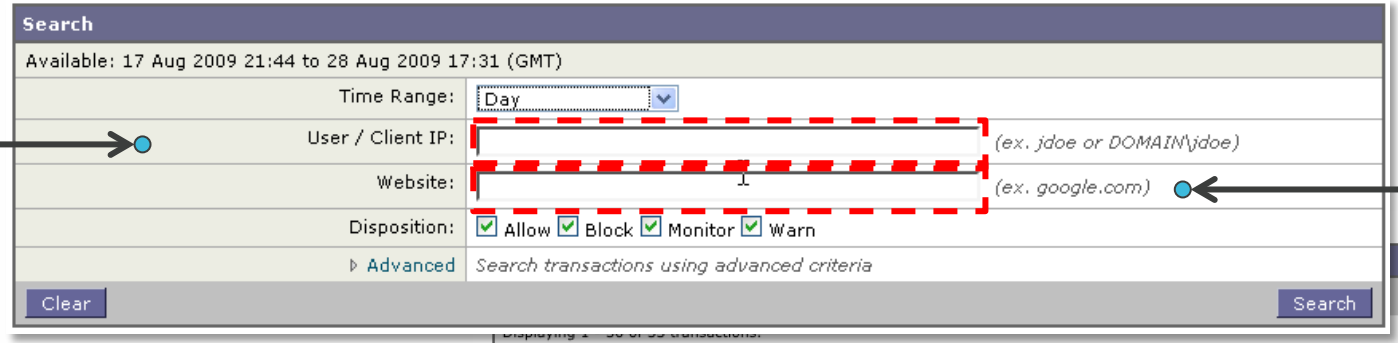
Secure Mobility Reporting

Simple investigative tool

Knowledge Is Power.
Learn. Share. Collaborate.

Track User activity /
Search by IP ranges

Track a web site



Printable Download

Items Displayed 50

« Previous | 1 | 2 | Next »

Time (GMT -05:00)	Transaction	Display Details...	Disposition	Bandwidth	User / Client IP
17 May 2010 11:05:13	http://www.ch-non-food.com/		Allow	21.5KB	173.37.9.25
17 May 2010 11:03:44	http://www.jobdig.com/		Allow	84.2KB	173.37.9.25
17 May 2010 11:02:21	http://m1.bzbattery.cn/up/up.htm		Block	2,151B	173.37.9.25
17 May 2010 11:01:43	http://www.oceanaresorts.com/default.asp		Allow	31.3KB	173.37.9.25
17 May 2010 11:00:53	http://www.booksamillion.com/		Allow	58.5KB	173.37.9.25
17 May 2010 11:00:01	http://www.reelviews.net/movies.php		Allow	72.6KB	173.37.9.25
17 May 2010 10:58:25	http://www.browserwelten.net/		Allow	158.1KB	173.37.9.25
17 May 2010 10:58:05	http://www.pathologyoutlines.com/		Allow	827B	173.37.9.25
17 May 2010 10:57:26	http://www.store.nodakoutdoors.com/		Allow	807.2KB	173.37.9.25
17 May 2010 10:57:00	http://www.cellularmagazine.it/include/common.js		Allow	80.7KB	173.37.9.25

- ü Know who is going to which web site
- ü Know who went to a specific web site
- ü And more…

Cisco AnyConnect Secure Mobility

Web Security with Next Generation Remote Access

Knowledge Is Power.
Learn. Share. Collaborate.

Choice

Diverse Endpoint Support for Greater Flexibility

Security

Rich, Granular Security Integrated into the network

Experience

Always-on Intelligent Connection for Seamless Experience and Performance

Questions

Final Thoughts

A pessimist sees the difficulty in every opportunity; an optimist sees the opportunity in every difficulty.

Winston Churchill

Thank you.