Deploying AnyConnect SSL VPN with ASA (and Firepower Threat Defense)

Ned Zaldivar, Security Architect
Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKSEC-2501
Who is your Speaker?

• ned@cisco.com
• ~18 years @ Cisco / ~26 in Industry
• Security Architect for Large Global Companies
• CISSP #74780 | SFCE | CICSP (Web / Email)

• Background in Education, Healthcare, Retail and Energy
  • Security / Networking / Systems / Helpdesk

• Other sessions on ciscolive.com
  • Practical PKI for Remote Access (with ISE) – BRKSEC-2053/3053
  • Deploying PKI for Today’s Networks (for 802.1x and VPN) – TECSEC-2053
  • It’s all about Securing the Endpoint – BRKSEC-2051
Agenda

- Introduction
- AnyConnect Fundamentals
- AnyConnect Network Integration
- Provisioning Client Certificates
- AAA Deep Dive Client Certificates
- AAA Deep Dive RADIUS & LDAP
- Posture Checking
- Securing the Client
- Customizing the User Experience
What We Won't Cover

- Clientless SSL VPN via Web Portal
- AnyConnect with IOS and IPSEC/IKEv2 : see BRKSEC-3054/BRKSEC-2338
- AnyConnect modules like Umbrella Roaming Security, AMP, Network Visibility, Web Security, Network Access Manager or see BRKSEC-2051
- Roadmaps
- Licensing

but may be covered in other Cisco Live sessions
More info in Mega Slide Deck and Previous Sessions

- Moving some configuration, advanced stuff/troubleshooting to mega-slides
- Also please look at BRKSEC-3053 for ISE/VPN and Certificate scenario focus
The Scenario: Labrats

- Pharmaceutical Research Conglomerate* run by Rats and Cats

- Using Corporate Devices
  - Windows, MACs, iPADs

- Embracing BYOD

- Key Requirements:
  - Security
  - Easy to Use
  - IPv6
Clientless SSL VPN or AnyConnect?

<table>
<thead>
<tr>
<th>Feature</th>
<th>Clientless SSL VPN</th>
<th>AnyConnect</th>
</tr>
</thead>
<tbody>
<tr>
<td>End User Experience</td>
<td>Web Browser to access some applications</td>
<td>Just like in the Office</td>
</tr>
<tr>
<td>Access Control</td>
<td>Granular at URL level</td>
<td>Network ACL: IP, TCP/UDP port, SGT FTD: URL, Applications</td>
</tr>
<tr>
<td>Installation of client SW</td>
<td>No, uses browser. *</td>
<td>Yes, Thick Client</td>
</tr>
<tr>
<td>Maintenance</td>
<td>New versions of browsers, java, applications...</td>
<td>Once setup works fine</td>
</tr>
</tbody>
</table>

* Features may depend on OS, browser version, Java, Active-X, endpoint security settings.
SSL VPN uses TLS, not SSL!

- SSL has since been replaced by TLS (Transport Layer Security)
- Current version is TLS 1.2

Limitations of TLS for SSLVPN
- TCP in TCP – slow
- TCP retransmissions

Cisco's implementation of DTLS (RFC 6347)
- DTLS is optional, fallback to TLS if required
- TLS tunnel is maintained in parallel to DTLS for keepalives (inc. PMTU discovery) and backup
- Any firewalls between AnyConnect and ASA need to allow both TCP 443 and UDP 443 for DTLS to work
The TLS Handshake

**Client**
- **ClientHello**
  - Client Version, ClientNonce
  - SessionID, Ciphersuites

- **ClientKeyExchange**, ChangeCipherSpec, ClientFinished
  - Encrypted pre_master_secret
  - PRF computation

**Server**
- **ServerHello**, ServerCertChain, ServerHelloDone
  - Server Version, ServerNonce
  - Selected Ciphersuite, CertificateChain
  - (Option: CertRequest)

- **ChangeCipherSpec**, ServerFinished
  - PRF computation

**Application Data**

**Encrypted**
AnyConnect also supports IPSec

- AnyConnect only supports IKEv2 (not IKEv1) for IPSec

- ASA IPSEC/IKEv2 for Remote Access is compatible with 3rd party clients (ASA 9.3.2 – Tested with Apple iOS, Strongswan, Android, Windows7+(no PSK))

- Why would you prefer SSL over IPSec/IKEv2?
  - It is more likely to work anywhere – through firewalls and proxies!

- Why would you want to use IPSec/IKEv2 instead of SSL?
  - Usually only reason is if mandated by compliance
# AnyConnect VPN Concentrator Platforms

<table>
<thead>
<tr>
<th>ASA</th>
<th>ASA5500*</th>
<th>ASA5500-x</th>
<th>FPR2100</th>
<th>FPR4100</th>
<th>FPR9300</th>
<th>ASAv (KVM, ESX, AWS, Azure)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTD (NGFW)</td>
<td>NA</td>
<td>ASA5500-x**</td>
<td>FPR2100</td>
<td>FPR4100</td>
<td>FRP9300</td>
<td>FTDv (KVM, ESX, AWS, Azure)</td>
</tr>
<tr>
<td>IOS</td>
<td>ASR</td>
<td>CSR</td>
<td>ISR</td>
<td></td>
<td></td>
<td>ISRv/CSRv</td>
</tr>
</tbody>
</table>

*ASA5500 is EoL/EoS – Last version is 9.1.7x which is also EoL/EoS

**ASA5585-x does not support Firepower Threat Defense
VPN Management Support:

• ASDM or CSM used to configure ASA

• Firepower Management Center (FMC) or Firepower Device Manager (FDM) used to configure FTD / NGFW
  • Not all ASA features configurable via FMC/FDM
  • Features relying on AnyConnect Client will work

Highlights a feature is not yet in FTD as per 6.2.2
VPN Concentrator Management Option: ASA

- ASDM for easy management and troubleshooting
  - 100% feature support – recommended management in most deployments
  - Primarily Used in this breakout!

- CLI – beware that not all config is visible in “show running”
  - will also require management of XML files

- Cisco Security Manager (CSM)
  - For configuration of multiple ASAs
  - It does support most features
AnyConnect Windows Version Reminder!

• Versions older than 3.1MR13 or 4.2MR1 will no longer run on Windows from 2/14/2017

• Due to Microsoft code signing enforcement
AnyConnect - Installation

• Installation Options
  - download from ASA or ISE (requires admin privileges for install only)
  - use Desktop Management System
  - Appstore, Google Play ... (mobile devices)

• Optional modules to install
  - DART
  - Posture (VPN Only)
  - ISE Posture (required when deploying with ISE)*
  - Start-Before-Login
  - AMP Enabler
  - Web security
  - Network Access Manager
  - Feedback Module
  - Network Visibility
  - Umbrella Roaming Security

Automatic Upgrades from cisco.com if using Umbrella Roaming with AnyConnect 4.3*
Anyconnect Secure Mobility Client

• Latest version is AnyConnect 4.5
• See table for OS Support
<table>
<thead>
<tr>
<th></th>
<th>Windows 7, 8.x, 10</th>
<th>Mac OSX</th>
<th>Linux</th>
<th>iOS</th>
<th>Android</th>
<th>Blackberry 10.3.2+</th>
<th>Win 8.1 Phone</th>
<th>ChromeOS 43+</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VPN</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Network Access Manager</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Posture</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Telemetry</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Network Visibility</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>DART</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Umbrella Roaming Security</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>AMP</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
AMP Enabler

• Optional AnyConnect module that installs AMP for Endpoints on client
• AMP installation software location specified in AMP Enabler Service Profile
• Note: AMP still has a separate UI, but in most deployments this is hidden to the end-users
Network Visibility Module:

• New module that reports traffic from client
  - Open framework

• Reports enhanced Netflow metadata (5-tuple tcp/udp, bytes sent/received) and in addition info on
  - process name
  - hash
  - parent process
  - and much, much more….
Umbrella Roaming Security

Encrypted
Authenticated
DNS/IP Security Filtered

First Match Rule Table by Identity

<table>
<thead>
<tr>
<th>Rule</th>
<th>AD User Policy: Bandwidth Hogs + Security + Log All Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>65 identities</td>
</tr>
<tr>
<td>2</td>
<td>Default Settings</td>
</tr>
<tr>
<td>3</td>
<td>Abuse Containment</td>
</tr>
<tr>
<td>4</td>
<td>Guest Policy (non AD users &amp; BYOD): High Web Filtering + S1600</td>
</tr>
<tr>
<td>5</td>
<td>Executive Policy: No Web Filtering + Security + Log Security</td>
</tr>
<tr>
<td>6</td>
<td>Marketing Policy: Access to Facebook</td>
</tr>
<tr>
<td>7</td>
<td>At Home Laptop Policy: No Web Filtering + Loggi...</td>
</tr>
<tr>
<td>8</td>
<td>Default Policy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category Setting</th>
<th>Security Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Web Filtering</td>
<td>All Security Protect...</td>
</tr>
<tr>
<td>No Web Filtering</td>
<td>All Security Protect...</td>
</tr>
<tr>
<td>All</td>
<td>All Security Protect...</td>
</tr>
</tbody>
</table>

Roaming Security:
- You are protected by Umbrella. DNS queries are encrypted.

- Roaming Security: Disabled while you are on a trusted network.

Cisco Umbrella

208.67.222.222
208.67.220.220

On Trusted Network
Client goes dormant
Network is Protected

Root/SP DNS
Local Corp DNS
At least one pkg file needed

- At least one pkg file must be uploaded to ASA, even if AnyConnect pre-deployed on clients (MSI, Appstore…)
- pkg file contains binaries… and more
- To check out, rename pkg file to zip and decompress

Anyconnectxxx.pkg
AnyConnect Upgrades

• AnyConnect can be upgraded from ASA, ISE or Cloud (with Umbrella Roaming Security module)

• ASA 9.0/AnyConnect 3.1 introduced **deferred updates**, giving the end-user the option to upgrade now or later

• Configured with **custom attributes**

• Configured per Group Policy

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeferredUpdate</td>
<td>DeferredUpdateAllowed</td>
<td>true</td>
</tr>
<tr>
<td>DeferredUpdate</td>
<td>DeferredUpdateMinimumVersion</td>
<td>4.4</td>
</tr>
<tr>
<td>DeferredUpdate</td>
<td>DeferredUpdateDismissTimeout</td>
<td>120</td>
</tr>
<tr>
<td>DeferredUpdate</td>
<td>DeferredUpdateDismissResponse</td>
<td>update</td>
</tr>
</tbody>
</table>
On the Client: AnyConnect Configuration Files

- AnyConnect Configuration Files are stored on the client in the following directories:

<table>
<thead>
<tr>
<th>OS</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 10,8,7,Vista</td>
<td>C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client</td>
</tr>
<tr>
<td>Windows XP</td>
<td>C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client</td>
</tr>
<tr>
<td>MAC OS X and Linux</td>
<td>/opt/cisco/anyconnect/</td>
</tr>
<tr>
<td>Windows 10,8,7,Vista</td>
<td>C:\Users\username\AppData\Local\Cisco\Cisco AnyConnect VPN Client\preferences.xml</td>
</tr>
<tr>
<td>Windows XP</td>
<td>C:\Documents and Settings\username\Local Settings\ApplicationData\Cisco\Cisco AnyConnect VPN Client\preferences.xml</td>
</tr>
<tr>
<td>MAC OS X and Linux</td>
<td>/Users/username/..anyconnect</td>
</tr>
</tbody>
</table>
On the Client: AnyConnect Configuration Files

- Apply to all Users logged onto the machine
AnyConnect Local Policy File


- XML file defining important aspects of AnyConnect behavior
  - allowing user to accept untrusted ASA certificates
  - allowing client software updates from ASA (and from which ASAs)

```xml
<FipsMode>true</FipsMode>
<BypassDownloader>true</BypassDownloader>
<RestrictWebLaunch>true</RestrictWebLaunch>
<StrictCertificateTrust>true</StrictCertificateTrust>
<EnableCRLCheck>false</EnableCRLCheck>
<RestrictPreferenceCaching>false</RestrictPreferenceCaching>
<ExcludePemFileCertStore>false</ExcludePemFileCertStore>
```

Standalone Profile Editor
Local Policy File Example:

- If the server certificate is not trusted, do you want the user to be able to accept the certificate?

  ```xml
  <StrictCertificateTrust>
  false
  </StrictCertificateTrust>
  ```

- .... or do you want AnyConnect to refuse to connect?

  ```xml
  <StrictCertificateTrust>
  true
  </StrictCertificateTrust>
  ```
DART Tool (Windows and MAC)

- DART Tool can be installed with the client
- Similar to “show tech” on client
- Gathering of OS Data and log files in large zip file
AnyConnect Troubleshooting Toolbox (iOS, Android)

Possible to view Profiles and Certificates

One click email of logs
AnyConnect Troubleshooting Toolbox (Windows)

MMC console with snap-ins:
- Event Viewer
- Certificate (Current User)
- Certificate (Local Computer)
AnyConnect Troubleshooting Toolbox (MAC)

Utilities/Console
Utilities/Keychain Access
AnyConnect Fundamentals: ASA Server Certificate

- ASA certificate should be trusted by clients
  - Public (well-known) Certificate Authority (e.g. Verisign, Thawte)
  - Enterprise Certificate Authority, e.g. Microsoft Active Directory
  - Self-Signed (need to import certificate to all clients)
  - AnyConnect 4.1: check of CRL is configurable (Local Policy File)

- FQDN in Subject
Ensure Clients Trust the ASA Certificate

• AnyConnect uses OS to validate certificate
  - Microsoft Windows: MS CAPI
  - MAC OS: Keychain
  - Linux: Varies with distribution

• Tip: Examine warnings with browser
  - Untrusted CA chain
  - Mismatch domain name
  - Validity time (GOT NTP?)
AnyConnect 4.5 Certificate Pinning

- If configured, AnyConnect will only connect to ASAs with specific certificates/issuers
- Any certificate in the certificate chain can be pinned
- Possible to pin per entry in server-list or globally

AnyConnect Client will only connect to ASAs with certs from CA with this cert (pinning to SHA512)
Key Usage and Extended Key Usage Checking

- Extended Key Usage (EKU) and Key Usage (KU) determine how certificate can be used (client authentication, server authentication, email encryption etc)
- AnyConnect does **not require** EKU or KU to be in ASA server certificate
- From AnyConnect 3.1: **if** EKU or KU are present, they **must** be correct
  - EKU must contain “Server Authentication”
  - KU must contain “Digital Signature” and “Key Encipherment”
AnyConnect Fundamentals : IPv4 and IPv6

- AnyConnect supports **IPv6** tunneled inside **IPv4** or **IPv6**
  - management/control servers (CA, AD, RADIUS) IPv4 only
Which IP protocol should be used to Connect to ASA

- A dual-stacked host has the choice of connecting via IPv4 or IPv6
- Default: try to connect to ASA via its IPv4 address first, if that fails try IPv6
- Roaming between IPv6 and IPv4 supported
Configuring (inside) IPv6 Address Pools and DNS

IP address assignment via DHCP and AAA works only for IPv4.

IPv6 address assignment through address pool.

DNS Servers may be IPv4 or IPv6.
Agenda

- Introduction
- AnyConnect Fundamentals
- AnyConnect Network Integration
- Provisioning Client Certificates
- AAA Deep Dive Client Certificates
- AAA Deep Dive RADIUS & LDAP
- Posture Checking
- Securing the Client
- Customizing the User Experience
Don’t NAT/PAT VPN traffic

• If you need to NAT your outgoing IPv4 internet traffic, add exception for VPN

<table>
<thead>
<tr>
<th>Match Criteria: Original Packet</th>
<th>Action: Translated Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Intf</td>
<td>Dest Intf</td>
</tr>
<tr>
<td>inside</td>
<td>outside</td>
</tr>
<tr>
<td>2 Any</td>
<td>outside</td>
</tr>
</tbody>
</table>
High Availability Design: Active/Standby Failover

• Easy: Leveraging ASA failover
• Appears as one ASA sharing IP, MAC addresses
• Configuration changes replicated (incl. certs)
  - AnyConnect Images **not** replicated
  - AnyConnect Profiles **not** replicated
• VPN sessions replicated: seamless failover
• Requires L2 adjacencies between ASAs
  - AWS/Azure native HA not supported….but
    HA Agent -
    Native Load Balancer -
    https://www.youtube.com/watch?v=KAK_wCbMyAg
VPN Load Balancing

• Multiple ASAs in a VPN Cluster
  - **Not the same as ASA Clustering** technology (which does not support remote access VPN)

• Each ASA has separate config and IPs

• ASA “master” also owns the shared virtual IP

• AnyConnect Client connects to master and is redirected to “least loaded” ASA

• No configuration or state-synch

• Rarely used today!
  - Complexity and lack of seamless failover
  - …but, allows for different hardware/software across ASAs (easy upgrading/expansion)
AnyConnect with Multiple Contexts

• ASA 9.5(1) and 9.6(2)
• One physical ASA with multiple contexts
• …with unique configurations
  - Certificates,
  - AnyConnect images
  - Policies
• …with separate management views
• …with separate ip address spaces
When Pigs Fly: AnyConnect with Multiple Contexts
When Pigs Fly: AnyConnect with Multiple Contexts
When Pigs Fly: AnyConnect with Multiple Contexts
Context Resource Classes

- Possible to specify AnyConnect resource utilization (sessions) for contexts via resource class
  - AnyConnect
    - Guaranteed to a context
    - Cannot be oversubscribed
  - AnyConnect Burst
    - Allow extra sessions to context if available
ASA 9.6(2): Private and Shared Storage

- Private Storage: Only specific context (and systems context has) read-write access.
- Shared Storage: Only system context has write access, other context have read access.
- Choose private or shared for your AnyConnect Images/Profiles depending on security policy.
AnyConnect in Global Networks – Let user decide!

• Let user choose gateway
  - From dropdown
  - Each gateway may have predefined backups using Server list in Client Profile
AnyConnect in Global Networks: Automatic Selection

- Optimal Gateway Selection (OGS)
  - Automatically selects gateway based on Round-Trip-Time (RTT) using HTTP(S) requests
  - Calculation takes place after coming back from VPN suspension
  - Caches the result per client location (defined with domain name/DNS server)
  - Not supported with Always-On
  - If password based authentication is used, another login may be necessary
AnyConnect in Global Networks: Automatic Selection

• Optimal Gateway Selection (OGS)
  - Automatically selects gateway based on Round-Trip-Time (RTT) using HTTP(S) requests
  - Calculation takes place after coming back from VPN suspension
  - Caches the result per client location (defined with domain name/DNS server)
  - **Not supported with Always-On**
  - If password based authentication is used, another login may be necessary

Some server resources may be more important
  - E.g Exchange server at home office
Many Enterprise WANs are slower than the Internet
Optimal Gateway Selection may be sub-optimal!
Configuring Optimal Gateway Selection

OGS calculation will take place if VPN suspended for longer than X hours

New Gateway selected if RTT performance increased by X%
AnyConnect : Straight or on the Rocks? (with ISE)

Cisco Identity Services Engine (ISE)
See breakouts:
BRKSEC-2695
BRKSEC-3053 (for Certificate and VPN specific scenarios)
AnyConnect to ASA without ISE integration

• ASA has interfaces to potentially multiple AAA servers including the Directory, e.g.
  - RADIUS to OTP servers
  - LDAP to Enterprise Directory

• ASA manages posture enforcement

• ASA authorizes user based on
  - AAA information: authentication method
  - AAA information: AD group membership
  - Posture: e.g. Antivirus up-to-date
  - Authorization typically implies applying a pre-defined ACL to user session
AnyConnect to ASA with ISE Integration

- **Most control logic moved to ISE**
- Allowing for a **more consistent** policy
  - Remote Access VPN
  - Wired Campus
  - Wireless Campus
- …determining access to internal resources based on
  - AAA information: authentication method
  - AAA information: AD group membership (superior integration)
  - Posture: e.g. Antivirus, Patch Management
  - Authorization can use Security Group TAGs (SGTs)
AnyConnect to ASA with ISE Integration

• Most control logic moved to ISE
• Allowing for a more consistent policy
  - Remote Access VPN
  - Wired Campus
  - Wireless Campus
• …determining access to internal resources based on
  - AAA information: authentication method
  - AAA information: AD group membership
    (superior integration)
  - Posture: e.g. Antivirus, Patch Management
  - Authorization can use Security Group TAGs
    (SGTs)
AnyConnect to ASA with ISE Integration

• **Most control logic moved to ISE**

• Allowing for a **more consistent** policy
  - Remote Access VPN
  - Wired Campus
  - Wireless Campus

• …determining access to internal resources based on
  - AAA information: authentication method
  - AAA information: AD group membership (superior integration)
  - Posture: e.g. Antivirus, Patch Management
  - Authorization can use Security Group TAGs (SGTs)
AnyConnect to ASA with ISE Integration

- **Most control logic moved to ISE**
- Allowing for a **more consistent** policy
  - Remote Access VPN
  - Wired Campus
  - Wireless Campus
- …determining access to internal resources based on
  - AAA information: authentication method
  - AAA information: AD group membership (superior integration)
  - Posture: e.g. Antivirus, Patch Management
  - Authorization can use Security Group TAGs (SGTs)
AnyConnect to ASA with ISE Integration

- Most control logic moved to ISE
- Allowing for a more consistent policy
  - Remote Access VPN
  - Wired Campus
  - Wireless Campus
- …determining access to internal resources based on
  - AAA information: authentication method
  - AAA information: AD group membership (superior integration)
  - Posture: e.g. Antivirus, Patch Management
  - Authorization can use Security Group TAGs (SGTs)
AnyConnect VPN and ISE: Workload Distribution

ASA Administrators
We no longer need to care about AD, LDAP or LDAP maps, posture, DAP...

ISE Administrators
Send your colleagues to ISE breakouts!
Traditional Segmentation

• Based on VLAN
• Tied to IP addressing

Rules change with Network changes!
Expensive to maintain!
Segmentation based on Security Groups TAGs

- All clients associated with Security Group TAG
- Based on
  - Identity,
  - Device type
  - Posture requirements
  - Access method (vpn… campus)
  - Location…

Rule table independent of addressing!
Simple to maintain!
Increased granularity taking into account device type etc.

<table>
<thead>
<tr>
<th>Source</th>
<th>User</th>
<th>Dest</th>
<th>Application</th>
<th>?</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPAD</td>
<td>HR</td>
<td>Citrix</td>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td>Iphone</td>
<td></td>
<td>Gateway</td>
<td>SIP</td>
<td></td>
</tr>
<tr>
<td>Sensor</td>
<td></td>
<td>ICSserver</td>
<td>SCADA</td>
<td></td>
</tr>
</tbody>
</table>
ISE information sharing with pxGrid

- ISE has full knowledge of who/what connects to network (via VPN, Wired, Wireless)
- Shared with security components
  - E.g Firewall, IPS, Analytics, Single-Sign-On… etc.
- Now they know who the user is behind a certain IP address
- And they can tell infrastructure to quarantine device (Rapid Threat Containment)
Agenda
AAA in ASA: Some Important Concepts

Proving Who you are
- Static Passwords (local to ASA, Active Directory, LDAP)
- OTP (One-Time-Passwords), typically RADIUS
- Certificates

Determining What you are and What You can do
- ACL
- Split Tunnelling
- Proxy settings
- Timeouts
- etc..

AnyConnect behaviour...
- Which ASA and Connection Profile to connect to
- "Always On"
- which certificate to use, etc...
Labrats Requirements

- **Strong Authentication**
  - Corporate devices (laptops, iPads) use certs
  - BYOD use OTP sent as text to mobile

- **Granular Authorization**
  - Depending on Active Directory group and device (corporate vs. BYOD)
  - Access Rights differ with regards to
    - ACL (Filter)
    - IP address pool
    - Split Tunneling
    - Client Profile
    - Restrict to VLAN...
Avoid too many Group Policies

- You don’t have to create group policies to control where client is allowed to go!
  - Pre-defined ACL (Filter-ID can be applied to session)
  - Downloadable ACL applied to session
  - Security Group TAG from ISE assigned to session

- Only add Group Policies when needed!
  - … split tunnelling policy
  - … certificate enrolment (covered later)
  - ….don’t be too creative here!
Access Lists to Authorize User access

- "Loose Hanging" Access Lists defined on ASA
  - applied from different places in GUI, not from main Firewall Ruleset
  - applied from RADIUS (Filter-ID)
On Statefulness of the stand-alone ACLs

- RA VPN ACLs applied by Group Policy, DAP, Filter-ID or dACLs do not support stateful creation of openings for return traffic to clients on inside
Security Groups in main Statefull Firewall Rule Table

Unselect, to let VPN traffic go through Global/interface ACLs

Mix and Match ACEs with and without SGTs

Security Group
Firepower: Access Policy based on SGTs

- Cisco NGFW can use SGTs in the policy (Source Only)
- Flexconfig needed to get this to work in 6.2. (see hidden slide)
Workaround for SGTs to work:

- FMC by default enables native SGT tagging on interfaces
- If TAG is assigned to VPN user, packets will be tagged natively on inside
- …which breaks things unless inside infrastructure does not support SGT
- Workaround: Disable SGT tagging on inside with Flexconfig

interface GigabitEthernet0/1
nameif inside
cs manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 10.0.1.2 255.255.255.0

Remove offending commands with Flexconfig
SGTs in logging

- No SGT in Active Sessions (but Group Policy and Connection Profile)
Possible Integration with Multi VRFs

• Users mapped to VLAN (sub-interface) on the ASA per the group-policy.

Restrict access to VLAN:

\[ \text{VlanCatsCorp} \]

• Routes tied to interfaces

route VlanCatsCorp 10.0.0.0 255.0.0.0 10.0.151.1 2
route VlanRatsCorp 10.0.0.0 255.0.0.0 10.0.152.1 3

• Overlapping IP addresses concerns:
  • AAA server
  • ASA interfaces
  • IP Pools
Possible Integration with Multi VRFs

• Users mapped to VLAN (sub-interface) on the ASA per the group-policy.

Restrict access to VLAN:

151 (assigned to interface: VlanCatsCorp)

• Routes tied to interfaces

route VlanCatsCorp 10.0.0.0 255.0.0.0 10.0.151.1 2
route VlanRatsCorp 10.0.0.0 255.0.0.0 10.0.152.1 3

• Overlapping IP addresses concerns:
  • AAA server
  • ASA interfaces
  • IP Pools
Authentication and Authorization by RADIUS

- RADIUS attribute IETF 25 (Class) is used to assign the group policy
- RADIUS Filter-ID can define a pre-defined ACL on ASA
- RADIUS SGT can be sent from ISE
Connection Profile: How to Authenticate

AAA Server Group: RADIUS

Default Group-Policy used unless overwritten by Authorization Server

AAA, Certificate or Both?

AAA server group
ASA configuration of ISE AAA Server Group

- **Interim Accounting**
- **Authorization-Only if using Certificates**
- **Dynamic Authorization (CoA, Change of Authorization)**
RADIUS Server Definition

Double check port numbers on RADIUS server

Shared Secret must match with RADIUS server
Connection Profile: Where Send Accounting

- Possible to define AAA Server Group for RADIUS Accounting
Adding RADIUS Attribute for Connection Profile to ISE

Attribute for Connection Profile is Cisco-VPN3000:146
Has to be added to ISE 1.1.1 dictionary before use
RADIUS Deep-Dive: AnyConnect Identity Extensions

- AnyConnect Identity Extensions (ACIDEX) forwarded via ASA to ISE
- Contains info on OS, Version, MAC Addresses, AnyConnect version....
- Can be used for ISE profiling and policy decisions

ACCESS REQUEST
- user-name=scratchy@labrats.se
- device-os=win
- device-mac=000C2908CA2F
- device-platform=6.1 SP1
- device-anyconnect = 4.0.0051
- device-uid=1398FB9......
AnyConnect Identity Extensions from Mobile Devices

- AnyConnect Mobile (iOS, Android) do not send MAC address
  - not available through OS API
- Currently ISE uses MAC address as key for Profiling, MDM lookup
- Future versions of ISE may leverage device UID for these lookups

```plaintext
AVP: l=15 t=Calling-Station-Id(31): 83.226.83.240
AVP: l=34 t=Vendor-Specific(26) v=ciscoSystems(9)
 ▪ VSA: l=28 t=Cisco-AVPair(1): mdm-tlv=device-mac=unknown
AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)
 ▪ VSA: l=29 t=Cisco-AVPair(1): mdm-tlv=device-type=iPad4,2
AVP: l=41 t=Vendor-Specific(26) v=ciscoSystems(9)
 ▪ VSA: l=35 t=Cisco-AVPair(1): mdm-tlv=device-platform=apple-ios
AVP: l=43 t=Vendor-Specific(26) v=ciscoSystems(9)
 ▪ VSA: l=37 t=Cisco-AVPair(1): mdm-tlv=device-platform-version=8.1
AVP: l=67 t=Vendor-Specific(26) v=ciscoSystems(9)
 ▪ VSA: l=61 t=Cisco-AVPair(1): mdm-tlv=device-uid=5d50064d7df5a0f1e885487c5eba3b15aa2cc591
AVP: l=80 t=Vendor-Specific(26) v=ciscoSystems(9)
 ▪ VSA: l=74 t=Cisco-AVPair(1): mdm-tlv=ac-user-agent=AnyConnect_AppleSSLVPN_Darwin_ARM (iPad) 3.0.12169
```
Verifying Mobile Devices with MDMs

- ISE can verify posture of mobile devices via external API
- MDM API uses MAC address for lookup, so this does not currently work over VPN

It is a rat, but device is not jailbroken and PIN code is 6 digits… I will let him in
RADIUS: Keeping track of IP addresses

• Client physical ip address in RADIUS Calling-Station-ID
• Client virtual ip address in RADIUS Accounting Framed-IP-Address
  - turn on RADIUS accounting for visibility

Update Session Directory for this IP

ACCESS REQUEST
- user-name=scratchy@labrats.se
- Calling-Station-ID=85.12.17.22

ACCOUNTING START
- user-name=scratchy@labrats.se
- Framed-IP-Address=10.99.19.1
How Restrict VPN Access from Specific Subnets?

• How can we limit access to clients coming from specific subnets?
  • E.g allow remote access only from Partner net, public ip 64.103.49.0/24
  • ASA Firewall ACLs does not work for traffic terminating at the ASA
Authentication by RADIUS  Authorization by LDAP

• User authenticated by RADIUS (typically strong authentication, OTP)
• Username used for LDAP lookup
• LDAP attributes are mapped to a Group Policy
Connection Profile : How to Authorize

- Possible to define different AAA server group for authorization (if not specified, the same group is used for authentication and authorization).
AAA Server Groups

- Using the same authentication protocol and characteristics

Same Protocol but different Groups if different characteristics

Several Servers in a Group for redundancy
LDAP Server Definition (Active Directory)

- LDAP over SSL
- Domain is labrats.se
- Attribute for user lookup
- Map LDAP attributes to ASA attributes (to be covered)
- ASA Credentials

- Server Group: AD_SamAccount
- Interface Name: Infrastructure
- Server Name or IP Address: ratbert.labrats.se
- Timeout: 10 seconds

LDAP Parameters for authentication/authorization

- Enable LDAP over SSL
- Server Port: 636
- Server Type: Microsoft

- Base DN: dc=labrats,dc=se
- Scope: All levels beneath the Base DN

- Naming Attribute(s): sAMAccountName
- Login DN: roddy@labrats.se
- Login Password: *********

- LDAP Attribute Map: ADmemberOf
A Good LDAP Browser is Useful

- To learn LDAP structure, and for troubleshooting: http://www.softerra.com

```plaintext
memberOf
CN=ITsupport,CN=Users,DC=labrats,DC=se
memberOf
CN=Cats,CN=Users,DC=labrats,DC=se
sAMAccountName=scratchy
```
Using Active Directory “memberOf”

- A user in Active Directory can be a member of many groups
  - But can only belong one Group Policy in ASA
- A group may be a member of another group in AD
  - ASA will not do recursive lookup
Mapping “memberOf” to Group Policy

- **Beware:** First match will apply (many memberOf one Group Policy)
- **Beware:** No support for lookup of nested groups (“group in group”)

- Solution 1: Using Cisco ISE allows for better flexibility in assigning Group Policy
- Solution 2: DAP (covered later) allows for more flexibility in handling "many memberOf"

**LDAP map**

- \text{CN=Rats,CN=Users,DC=labrats,DC=se} : RatsBYOD
- \text{CN=Cats,CN=Users,DC=labrats,DC=se} : CatsBYOD
User Selection of Connection Profile

Alias for drop-down at login page

URL to land on this connection profile
User Selection of Connection Profile (2)

Drop-Down list allows user to select login method (Connection Profile)
AnyConnect Client Profiles

• XML file created by ASDM, downloaded to client from ASA or pre-deployed to client via desktop management system.

```xml
<AutomaticVPNPolicy>true
<TrustedDNSSDomains>labrats.se</TrustedDNSSDomains>
<TrustedDNSServers>10.1.41.10</TrustedDNSServers>
<TrustedNetworkPolicy>Disconnect</TrustedNetworkPolicy>
<UntrustedNetworkPolicy>Connect</UntrustedNetworkPolicy>
<AlwaysOn>true
```

Client Profile
In the AnyConnect Client Profile: Server List

- Specify servers in the server list (also for fallback)
- Do not specify Host Address
  - May cause cert warnings
- Don’t have the user choose connection profile
  - Save mouse clicks
Troubleshooting AAA server
Troubleshooting a VPN Session

• Checking that the right Group Policy has been assigned
Troubleshooting VPN on FTD with FMC

Current Users
- Search Constraints (Edit Search Save Search)

Table View of Current Users
- Username
- VPN Group Policy
- VPN Connection Profile
- VPN Client Public IP
- VPN Client Application

Group Policy
- Login Time
- Current IP
- Username
- VPN Group Policy
- VPN Connection Profile
- VPN Client Public IP
- VPN Client Application

Connection Profile
- Active Sessions
- User
- Authentication Type
- Current IP
- Username
- Discovery Application
- VPN Group Policy
- VPN Connection Profile

Active Users
- Login Time
- Last Seen
- User
- Authentication Type
- Current IP
- Username
- Discovery Application
- VPN Group Policy
- VPN Connection Profile

FMC 6.2.2
Troubleshooting RADIUS : debug radius (1)

roddy(config)# sh debug
debbug radius session
debbug radius decode
roddy(config)# radius mkreq: 0xa1......
got user 'scratchy' got password
add_req 0xade2da48 session 0xa1 id 80
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=192.168.254.4

RADIUS packet decode (authentication request)
--------------------------------------
Raw packet data (length = 172).....
01 50 00 ac 10 09 0e 2f 3c c5 1a 4b 28 41 e6 27 | .P...../<..K(A.'
d4 7d 72 c3 01 0a 73 63 72 61 74 63 68 79 02 12 | .}r...scratchy..
67 58 f2 72 53 db 00 ee 29 1a 49 b4 f1 c7 1a c7 | gX.rS...).l.....
05 06 00 04 b0 00 1e 0f 31 39 32 2e 31 36 38 2e | ........192.168.
31 31 30 2e 31 1f 0f 31 39 32 2e 31 36 38 2e 32 | 110.1..192.168.2
35 34 2e 34 3d 06 00 00 00 05 42 0f 31 39 32 2e | 54.4=.....B.192.
31 36 38 2e 32 35 34 2e 34 04 06 0a 01 29 6e 1a | 168.254.4....n.
22 00 00 00 09 01 1c 69 70 3a 73 6f 75 72 63 65 | "......ip:source
34 1a 0f 00 00 0c 04 92 09 53 4d 53 2d 4f 54 50 | 4.......SMS-OTP
1a 0c 00 00 0c 04 96 06 00 00 00 02 | ..........
Troubleshooting RADIUS: debug radius (2)

Parsed packet data.....

........

Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 15 (0x0F)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 9 (0x09)
Radius: Value (String) = 53 4d 53 2d 4f 50 | SMS-OTP

Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
send pkt 10.1.41.51/1645
Troubleshooting RADIUS: debug radius (3)

RADIUS packet decode (response)

Raw packet data (length = 142).....
02 51 00 8e 13 94 12 5d 9c 56 84 ab bc 99 85 0d | .Q.....].V......
6a 71 7b 18 01 0a 73 63 72 61 74 63 68 79 18 28 | jq{...scratchy.
52 65 61 75 74 68 53 65 73 69 6f 6e 3a 30 3a 61 | ReauthSession:0a
30 31 32 39 33 33 33 30 30 30 30 30 30 30 30 30 | 0129330000351E50
44 42 33 31 35 42 19 0e 52 65 73 65 61 72 63 68 | DB315B..Research
42 59 4f 44 44 43 41 43 53 3a 30 61 30 31 32 0e | BYOD.4CACS:0a012
39 33 33 30 30 30 30 30 33 35 31 45 35 30 44 42 | 9330000351E50DB3
31 35 42 3a 69 73 65 31 32 31 34 31 35 38 39 31 | 15B:ise1/1415891
37 31 2f 32 32 34 33 33 31 3d 06 00 00 00 01 | 71/22431......

Parsed packet data.....

.........

**Radius: Type = 25 (0x19) Class**
Radius: Length = 14 (0x0E)
Radius: Value (String) =
43 61 74 73 42 59 4f 44 | CatsBYOD

........

**Radius: Type = 29 (0x1D) Termination-Action**
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination

RADIUS server may assign Group Policy with the Class attribute
## Troubleshooting RADIUS

### RADIUS Authentication Details

<table>
<thead>
<tr>
<th>Authentication Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logged At:</td>
</tr>
<tr>
<td>RADIUS Status:</td>
</tr>
<tr>
<td>NAS Failure:</td>
</tr>
<tr>
<td>Username:</td>
</tr>
<tr>
<td>MAC/IP Address:</td>
</tr>
<tr>
<td>Network Device:</td>
</tr>
<tr>
<td>Allowed Protocol:</td>
</tr>
<tr>
<td>Identity Store:</td>
</tr>
<tr>
<td>Authorization Profiles:</td>
</tr>
<tr>
<td>SGA Security Group:</td>
</tr>
<tr>
<td>Authentication Protocol:</td>
</tr>
</tbody>
</table>

### Authentication Result

- User-Name=scratchy
- State=ReauthSession:0a0129330000366450E94A95
- Class=CatsBYOD
- Class=CAC:0a0129330000366450E94A95:i.e1/141589171/24482
- Termination-Action=RADIUS-Request
Troubleshooting LDAP

• debug ldap

roddy(config)# debug ldap 100
download ldap enabled at level 100
roddy(config)#
[42] Session Start
[42] New request Session, context 0xaddbaacc, reqType = Other
[42] Fiber started
[42] Creating LDAP context with uri=ldaps://10.1.41.10:636
[42] Connect to LDAP server: ldaps://10.1.41.10:636, status = Successful
[42] supportedLDAPVersion: value = 3
[42] supportedLDAPVersion: value = 2
[42] Binding as roddy@labrats.se
[42] Performing Simple authentication for roddy@labrats.se to 10.1.41.10

[42] LDAP Search: Base DN = [dc=labrats,dc=se] Filter = [sAMAccountName=scratchy] Scope = [SUBTREE]
[42] User DN = [CN=Scratchy Cat,CN=Users,DC=labrats,DC=se]
Troubleshooting LDAP (2)

- debug LDAP (2)

[42] Talking to Active Directory server 10.1.41.10
[42] Reading password policy for scratchy, dn:CN=Scratchy Cat,CN=Users,DC=labrats,DC=se
[42] Read bad password count 0
[42] LDAP Search: Base DN = [dc=labrats,dc=se] Filter = [sAMAccountName=scratchy]
Scope = [SUBTREE]
[42] Retrieved User Attributes:

………….
[42] displayName: value = Scratchy Cat
[42] uSNCreated: value = 386330
[42] memberOf: value = CN=Cats,CN=Users,DC=labrats,DC=se
[42] mapped to Group-Policy: value = CatsBYOD
[42] mapped to LDAP-Class: value = CatsBYOD
[42] uSNChanged: value = 387490
[42] department: value = Cats
[42] name: value = Scratchy Cat

………..
Agenda
Authentication with Client Certificates

ClientHello

ClientKeyExchange, ChangeCipherSpec, Client Certificate
Encrypted Random byte string
ClientFinished

Application Data

ServerHello, ServerCertChain, ServerHelloDone
Client Certificate Request

Application Data

ChangeCipherSpec, ServerFinished
Why Authentication with Client Certificates?

• Considered stronger authentication than passwords

• No need to manage passwords (password complexity, resetting passwords, expiring passwords...)

• Need to manage a PKI (Public Key Infrastructure) to enroll and revoke certificates

• Client Certificates may be tied to machine or user (including smart cards)

• We can make it difficult to move a certificate from one machine to another: Using client certificates allows us to distinguish corporate devices from other devices (employee iPADs etc)
ASA must trust the Issuer of Client Certificates

- Install Issuer CA Certificate
  - from file
  - paste PEM file
  - SCEP

- Issuer of client certificates may be different to the issuer of the ASA certificate

Install From File
Paste PEM
Install from SCEP
Be Careful with Whom You Trust

- You may have more than one Trustpoint, but maybe you only trust one for client authentication

- Example:
  - Clients get certs from internal CA
  - ASA gets cert from public PKI

Warning
Careful if CA chain with root cert is imported when installing ASA public cert…
Checking for lost/stolen certificates

- CRL (Certificate Revocation List) downloads a list of revoked certificates (can be cached)
- OCSP (Online Certificate Status Protocol) checks status of individual certificates

Do we trust certificate if we cannot retrieve CRL?
Authentication with Client Certificates
Authorization with RADIUS (ISE)

- User authenticated with client certificate
- Username (some field) of certificate used for RADIUS lookup
- RADIUS server returns Group Policy and/or SGT
Authentication with Client Certificates

- Defined in Connection Profile
- Choosing "both" means that user first has to authenticate with certificate, then with username/password
  - Use case: Checking that user uses a corporate machine (with a soft certificate)
Client Certificate Authentication with ISE

- Authentication is between AnyConnect and ASA
- ISE never sees or validates cert
- ASA does an authorize-only lookup (RFC 5176) with no password
Client Certificate Authentication with ISE

- Authentication is between AnyConnect and ASA
- ISE never sees or validates cert
- ASA does an authorize-only lookup (RFC 5176) with no password
Client Certificate Authentication with ISE

- Authentication is between AnyConnect and ASA
- ISE never sees or validates cert
- ASA does an authorize-only lookup (RFC 5176) with no password
Connection Profile Name sent to ISE

- ASA sends info about Connection Profile and Client Type to RADIUS server
- Can be used by RADIUS Server Policy
Connection Profile Name sent to ISE

- ASA sends info about Connection Profile and Client Type to RADIUS server
- Can be used by RADIUS Server Policy
Connection Profile Name sent to ISE

- ASA sends info about Connection Profile and Client Type to RADIUS server
- Can be used by RADIUS Server Policy

ACCESS REQUEST
- user-name=scratchy@labrats.se
- service-type= authorize-only
- "connection-profile" = certs
Connection Profile Name sent to ISE

- ASA sends info about Connection Profile and Client Type to RADIUS server
- Can be used by RADIUS Server Policy
Authentication with Client Certificates Authorization with LDAP

- User authenticated with client certificate
- Username (some field) of certificate used for LDAP lookup
- LDAP attributes are mapped to a Group Policy
Authorization with Client Certificates

- Work out which fields in cert to use and how to map to LDAP

Client Certificate: SAN (Principal Name)
scratchy@labrats.se

LDAP: userPrincipalName
scratchy@labrats.se
Authorization with Client Certificates

Client Certificate

LDAP Database

Connection Profile:
User mapping from Cert=UPN (Users’ Principal Name)

AAA Server:
Naming Attribute=userPrincipalName
A smart card is just another client certificate

- Same principles and configuration as for soft client certificates
Double Certificate Authentication

• ASA 9.7.1 with AnyConnect 4.4 now support “double” cert authentication!
  • First authenticate with computer certificate
  • Second authenticate with user certificate/smart card
  • Proves it is a “corporate machine” and adds strong user authentication
Client Profile Options to select the right certificate

Certificate Store: User, Machine or All

Certificate Store Override: Check if non administrator needs access to machine certificate

Uncheck for Automatic certificate Selection
Certificate Matching (for automatic cert selection)

If client (or smartcard) contains many certificates, we can specify which one should be selected (used with automatic certificate selection).
Agenda

- Introduction
- AnyConnect Fundamentals
- AnyConnect Network Integration
- Provisioning Client Certificates
- AAA Deep Dive: Client Certificates
- AAA Deep Dive: RADIUS & LDAP
- Posture Checking
- Securing the Client
- Customizing the User Experience
Certificate Enrollment : Active Directory

• Microsoft Active Directory supports automatic certificate enrolment for user and machine certificates

• User and machine are members of Active Directory Domain: Their certificates can be pushed by GPOs (Group Policy Objects)

Certificate Enrolment: Active Directory (2)

- Microsoft CA also supports web enrolment
- Can be used by non-domain members, e.g. MACs
Simple Certificate Enrolment Protocol (SCEP)

- Protocol for enrolling certificates over HTTP (basically encapsulating PKCS#10, PKCS#7 over HTTP)
- Originally developed by Verisign for Cisco
- **Widely** supported by network devices (including ASA and AnyConnect), clients and most Certificate Authorities (including Microsoft CA and Cisco ISE)
AnyConnect SCEP Proxy

- ASA can be an SCEP proxy, enabling AnyConnect on the outside to enroll to a CA on the inside of ASA without poking holes in Firewall

- Not to be confused with Legacy SCEP, where AnyConnect speaks directly to the CA over the VPN tunnel.

- SCEP proxy requires AnyConnect 3.0 or later:
BYOD Use case: Secure Enrollment of Certificates to Mobile Devices

• Mobile users (Windows, MAC, Phone, Android) logon from anywhere (over internet) to enroll

• Secure authentication via OTP sent by SMS to mobile

• Certificate automatically enrolled with correct subject name

• Note : to mitigate risk of stolen phones, use certs + AAA for authentication
  - is phone PIN code protection of certificate enough?
1. User Connects to ASA
2. User Gets SMS with OTP
3. User logs on with OTP
4. AnyConnect Gets Certificate from ASA (proxy to CA)
Cert can also be used for 802.1X*
4. AnyConnect Gets Certificate from ASA (proxy to CA)
Cert can also be used for 802.1X*
4. AnyConnect Gets Certificate from ASA (proxy to CA)
Cert can also be used for 802.1X*
4. AnyConnect Gets Certificate from ASA (proxy to CA)

Cert can also be used for 802.1X*
4. AnyConnect Gets Certificate from ASA (proxy to CA)
Cert can also be used for 802.1X*
4. AnyConnect Gets Certificate from ASA (proxy to CA)

Cert can also be used for 802.1X*
4. AnyConnect Gets Certificate from ASA (proxy to CA)
Cert can also be used for 802.1X*
What to Configure on ASA for SCEP

- Configuration example on

Client Profile For Certificate Enrollment

Subject-name can use %USER% %MACHINEID%

EA can be used instead of SAN

Default of 512 will not work with Windows CA default
Group Policy for Certificate Enrollment

Group Policy "SCEPProxyEnroll"

URL for Microsoft CA
http://ad.labrats.se/certsrv/mscep/mscap.dll

URL for ISE CA
http://ise.labrat.se:9090/auth/caservice/pkiclient.exe

Client Profile "scepproxy"
Connection Profile for Certificate Enrollment

Connection Profile "SCEPProxyEnroll"

Authentication set to "Both" for SCEP Proxy

Enable SCEP on Connection Profile
Configuration on Windows 2008 R2 Server (1)

By default Microsoft requires user to enter challenge password to get certificate. Careful when changing this!! MUST limit access to SCEP CA/RA.

SCEP RA (Registration Authority)
Configuration on Windows 2008 R2 Server (2)

- Good Microsoft document on

Microsoft registry setting to change default Certificate Template used by SCEP

Hint: the default template does not work for SSL VPN
Troubleshooting Tips

• Pay attention to the certificate templates used by Microsoft CA
  - certificate usage
  - security permissions
  - minimum key length

• Logs from Microsoft Server may be helpful
  - Event Viewer : Server Roles
  - IIS access logs

```
<table>
<thead>
<tr>
<th>Level</th>
<th>Date and Time</th>
<th>Source</th>
<th>Event ID</th>
<th>Task Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>12/21/2012 3:28:03 PM</td>
<td>NetworkDeviceEnrollmentService</td>
<td>31</td>
<td>None</td>
</tr>
<tr>
<td>Warning</td>
<td>12/21/2012 3:28:03 PM</td>
<td>CertificationAuthority</td>
<td>53</td>
<td>None</td>
</tr>
</tbody>
</table>
```

The Network Device Enrollment Service cannot submit the certificate request (The public key does not meet the minimum size required by the specified certificate template.). 0x80004005
Agenda
AnyConnect Posture with ISE: Do the Clients meet Requirements?

- Possible to check that client meets Posture Requirements: OS, Anti-Virus, Personal Firewall, Registry Keys
- … or compliance to patch management status
- Leverages AnyConnect ISE Posture Module
- Posture control and decision defined in ISE
AnyConnect ISE Posture Module

- Windows and MAC
- Checks and Remediates Posture
  - Works on campus (wired, wireless 802.1X)
  - Works with AnyConnect VPN
- Posture checking with Patch Management (SCCM)
- Software and XML config file provisioned from
  - ASA
  - ISE or
  - via Desktop Management System

• Requires Compliance Module provisioned from
  - ISE or
  - via Desktop Management System
AnyConnect ISE Posture Flow
AnyConnect ISE Posture Flow

ACCESS REQUEST
- url-redirect-ACL=Quarantine
- url-redirect=https://ise...
- SGT = Quarantine

ACCESS ACCEPT

Logon

ISE
AnyConnect ISE Posture Flow

Logon

Discovers ISE

ACCESS REQUEST

ACCESS ACCEPT
- url-redirect
- ACL=Quarantine
- SGT = Quarantine
AnyConnect ISE Posture Flow

Logon

ACCESS REQUEST
- url-redirect-ACL=Quarantine
- url-redirect=https://ise...
- SGT = Quarantine

Discovers ISE

Posture Req
AnyConnect ISE Posture Flow

- Logon
- Discovers ISE

ACCESS REQUEST
- url-redirect-ACL=Quarantine
- url-redirect=https://ise...
- SGT = Quarantine

ACCESS ACCEPT

Posture Req
AnyConnect ISE Posture Flow

Logon

ACCESS REQUEST
- url-redirect-ACL=Quarantine
- url-redirect=https://ise...
- SGT = Quarantine

ACCESS ACCEPT

Discovers ISE

Posture Report (Compliant)

Posture Req

ISE

ASA
AnyConnect ISE Posture Flow

Logon

ACCESS REQUEST
- url-redirect-ACL=Quarantine
- url-redirect=https://ise...
- SGT = Quarantine

Discovers ISE

Posture Report (Compliant)

ACCESS ACCEPT

ISE

ASA

Posture Req

Logon

System Scan:
Compliant.
Network access allowed.

Connecting to asa5515x.labrats.se.

Disconnected.
AnyConnect ISE Posture Flow

Logon

ACCESS REQUEST
- url-redirect-ACL=Quarantine
- url-redirect=https://ise...
- SGT = Quarantine

ACCESS ACCEPT

Discovers ISE

Posture Report (Compliant)

CoA REQUEST
- SGT = CleanCat
- DACL
AnyConnect ISE Posture Flow

Logon

ACCESS REQUEST
- url-redirect-ACL=Quarantine
- url-redirect=https://ise...
- SGT = Quarantine

ACCESS ACCEPT

Discovers ISE

Posture Report (Compliant)

Posture Req

CoA REQUEST
- SGT = CleanCat
- DACL

CoA ACK
What to Configure on ASA for ISE Posture

- Configure a standalone ACL
  - permit means redirect traffic to ISE (default)
  - deny means do not redirect: this is traffic to ISE itself, traffic to remediation servers...
  - name of ACL must match RADIUS attribute "url-redirect-acl" signaled by ISE
# Desktop Posture Assessment

## Agent Listing

<table>
<thead>
<tr>
<th>Client Provisioned by ISE</th>
<th>Windows AnyConnect / ISE Posture</th>
<th>MAC OSX AnyConnect / ISE Posture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Posture Assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Updates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Packs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hotfixes</td>
<td></td>
<td>Not Applicable</td>
</tr>
<tr>
<td>OS / Browser Versions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patch Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-Malware- Installation / Signatures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application / Processes</td>
<td></td>
<td>Not Available</td>
</tr>
<tr>
<td>Anti-Phishing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registry Keys</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Posture Remediation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passive Re-Assessment (PRA)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AnyConnect Posture without ISE: Do the Clients meet Requirements?

- AnyConnect Posture Module (Hostscan)
- Possible to check that client meets Posture Requirements: OS, Anti-Virus, Personal Firewall, Registry Keys, Process, File
- Used in combination with Dynamic Access Policies (DAP) to grant access to clients depending on their posture status

Microsoft Firewall ON, but No Antivirus... and he is a RAT!!!!!
Posture/Host Scan – Software Packages Options

- Host Scan is packaged standalone or with AnyConnect.
- Some features deprecated
Specifying Host Scan Image

Download Software

Downloads Home > Products > Security > VPN and Endpoint Security Clients > Cisco Hostscan

Cisco Hostscan

Search...
Expand All | Collapse All

Release 3.1.02026

Latest Releases
3.1.02026
3.0.11033

All Releases

File Information
Host Scan Engine Update 3.1.02026
hostscan_3.1.02026-k9.pkg

Standalone Host Scan location on CCO
The Host Scan Process

Host Scan loads

Prelogin Checks based on OS, ip, cert, file, registry

Both in Parallel

Advanced Endpoint Assessment: Remediation/Fix FW, AV, AS

Endpoint Assessment Get info on FW, AV, AS, Registry, Processes, Files...

"MAC"

"Corp Windows"

Other

DAP

Policy

BRKSEC-2501 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 171
Configuring Host Scan

Possible to create checks for Process, File and Registry keys that can be enforced by DAP.

Endpoint Assessment must be checked to retrieve info on AV, AS, Firewall settings that can be enforced by DAP.
Prelogin Policy

- Typical use case is to differentiate corporate devices
  - Check client ip address, OS, that file exists, registry keys/values and certificate
    - client ip is the ip of network adapter (before any NAT…)
    - note: certificate check only checks if certificate exist, it does not cryptographically verify that the private key is there
  - Possible to deny login immediately, or pass Policy Name to DAP for enforcement
Dynamic Access Policies (DAP)

- DAP allows **granular access control** to resources based on authentication method, AAA parameters and Posture

- Very flexible, allowing policies set by **Data Owners** access to Data:
  - "to access **my data** you must be member of AD groups Cats and ProjectX, you must be logged in with strong authentication and you must have Antivirus on a corporate machine"

Microsoft Firewall ON, Antivirus ON, `memberOf Cats AND projectX`

Internet

ASA

PERMIT

DENY
How DAP relates to AAA

Posture: .....  

Default Group Policy  
Group Policy CatsBYOD  
Group Policy RatsBYOD  

Connection Profile SMS  

Dynamic Access Policies override certain attributes from Group Policy depending on AAA, Posture, Connection Profile...

memberOf ProjectX  
memberOf Cats  

LDAP map  

AAA Server Group SMS (RADIUS)  
AAA Server Group AD (LDAP)
Configuring DAP

If member of Cats and ProjectX logged on with certificate...

and Policy is Corporate Windows Registry Key is… Antivirus Updated...

Authorization IPv4/IPv6 ACL don’t mix permit and deny in ACL
Default DAP (DfltAccessPolicy)

<table>
<thead>
<tr>
<th>Condition</th>
<th>ACL</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITSupport w clean PC</td>
<td>RDP to everything</td>
<td>Terminate</td>
</tr>
<tr>
<td>Cats+ProjectX w clean PC</td>
<td>ProjectX</td>
<td></td>
</tr>
<tr>
<td>Rats</td>
<td>Rats WebSite</td>
<td></td>
</tr>
<tr>
<td>DfltAccessPolicy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If no DAP matches then DfltAccessPolicy Applies

Table:

<table>
<thead>
<tr>
<th>ACL Priority</th>
<th>Name</th>
<th>Network ACL List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>90</td>
<td>ITsupport Access</td>
<td>RDP-to-Everything</td>
<td>IT support Access with RDP</td>
</tr>
<tr>
<td>80</td>
<td>Access-ProjectX</td>
<td>ACLprojectX</td>
<td>Members of Cats AND Projects X logged on with cl...</td>
</tr>
<tr>
<td>70</td>
<td>Access to Rat Webserver</td>
<td>Permit-RatWebserver</td>
<td>Allow access to Rat Webserver to members of Rats...</td>
</tr>
<tr>
<td></td>
<td>DfltAccessPolicy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DAP Grows On You! (DAP accumulates)

Matching
Several conditions
Accumulates
Access Rights

<table>
<thead>
<tr>
<th>Condition</th>
<th>ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITSupport w clean PC</td>
<td>RDP to everything</td>
</tr>
<tr>
<td>Cats+Project X w clean PC</td>
<td>ProjectX</td>
</tr>
<tr>
<td>Rats</td>
<td>Rats WebSite</td>
</tr>
<tr>
<td>ACL Priority</td>
<td>Network ACL List</td>
</tr>
<tr>
<td>90</td>
<td>ITSupport Access</td>
</tr>
<tr>
<td>80</td>
<td>Access-ProjectX</td>
</tr>
<tr>
<td>70</td>
<td>Access to Rat Webserver</td>
</tr>
<tr>
<td></td>
<td>DftAccessPolicy</td>
</tr>
</tbody>
</table>
The Power of DAP

- Very flexible mapping to multiple "memberOf"
  - Example: 4 groups in Directory A B C D
  - A user may be a member of 0 to 4 groups: 16 combinations \(2^n\)

- Quiz: How many DAP policies do you need to cover the 16 combinations?

<table>
<thead>
<tr>
<th>Condition (memberOf)</th>
<th>ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>ACL-A</td>
</tr>
<tr>
<td>B</td>
<td>ACL-B</td>
</tr>
<tr>
<td>C</td>
<td>ACL-C</td>
</tr>
<tr>
<td>D</td>
<td>ACL-D</td>
</tr>
<tr>
<td>Endpoint Visibility</td>
<td>ASA Hostscan</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Policy Framework</td>
<td>DAP</td>
</tr>
<tr>
<td>Updates</td>
<td>Every 3 months</td>
</tr>
<tr>
<td><strong>IP, Hostname, Mac address</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>Certificate Fields</td>
<td>Yes</td>
</tr>
<tr>
<td>BIOS Serial Number</td>
<td>Yes</td>
</tr>
<tr>
<td>Personal Firewall</td>
<td>Yes</td>
</tr>
<tr>
<td>File CRC32 Check</td>
<td>Yes</td>
</tr>
<tr>
<td>Disk Encryption</td>
<td>Roadmap</td>
</tr>
<tr>
<td>SHA256 File Check</td>
<td>Roadmap</td>
</tr>
<tr>
<td>USB Check</td>
<td>Roadmap</td>
</tr>
<tr>
<td>Application</td>
<td>Roadmap</td>
</tr>
<tr>
<td>Stealth Agent</td>
<td>Roadmap</td>
</tr>
<tr>
<td>OS Support</td>
<td>Windows, Mac, Linux</td>
</tr>
</tbody>
</table>
DAP with Quarantine

• Possible to create a DAP (with ACL) that gives a user limited access to the network to remediate posture, after which he can "reconnect".

• Used together with "Advanced Endpoint Assessment"

• Remember that DAP accumulates ACL privileges (if other DAPs are matched user may still get full access to the network).
DAP for Mobile Devices (iOS, Android)
DAP with LUA

LUA (www.lua.org) – scripting language that allows for advanced checks, e.g.
- check for any AV
- check for any AV, AS, Firewall
- regexp matching of hotfixes, DN etc
LUA examples

assert(function()
    function check(antix)
        if (type(antix) == "table") then
            for k,v in pairs(antix) do
                if (EVAL(v.exists, "EQ", "true", "string")) then
                    return true
                end
            end
            return false
        end
    end
    return (check(endpoint.av) or check(endpoint.fw) or check(endpoint.as))
end()
LUA checks that User Connects with the "right" device

- Problem: A user with admin privileges may move a cert (and the private keys) from an "approved" device to a non-approved.

- LUA can detect this by comparing device ID signaled by AnyConnect with:
  - name in certificate (if certificate contains device ID)
  - an attribute from LDAP lookup (requires device IDs to be stored in LDAP server)

\[
\text{EVAL}(\text{endpoint.anyconnect.deviceuniqueid}, \text{"EQ"}, \text{aaa.ldap.mobileid}, \text{"caseless"})
\]
Troubleshooting DAP: debug dap trace

DAP_TRACE: DAP_open: B09086B0
DAP_TRACE: DAP_add_CSD: csd_token = [2441266B55C307BA5BEB70E5]

DAP_TRACE: Username: scratchy@labrats.se, aaa.ldap.logonCount = 15
DAP_TRACE: Username: scratchy@labrats.se, aaa.ldap.sAMAccountName = scratchy

DAP_TRACE:
dap_install_endpoint_data_to_lua:endpoint.as["MicrosoftAS"].(description="Windows Defender"
DAP_TRACE: name = endpoint.as["MicrosoftAS"].(description, value = "Windows Defender"
DAP_TRACE: dap_install_endpoint_data_to_lua:endpoint.as["MicrosoftAS"].(version="6.1.7600.16385"
DAP_TRACE: name = endpoint.as["MicrosoftAS"].(version, value = "6.1.7600.16385"

DAP_TRACE: name = endpoint.os.hotfix["KB2654428"], value = "true"
DAP_TRACE: dap_install_endpoint_data_to_lua:endpoint.os.hotfix["KB2656373"]="true"
DAP_TRACE: name = endpoint.os.hotfix["KB2656373"], value = "true"
Troubleshooting DAP: Monitoring

### Session Details

<table>
<thead>
<tr>
<th>Username</th>
<th>Group Policy Connection Profile</th>
<th>Assigned IP Address Public IP Address</th>
<th>Protocol Encryption</th>
<th>Login Time Duration</th>
<th>Bytes Tx</th>
<th>Bytes Rx</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:scratchy@labrats.se">scratchy@labrats.se</a></td>
<td>CatsCorp</td>
<td>10.99.110.1 2001:470:dfed:110::1 192.168.254.4</td>
<td>AnyConnect-Parent SSL-Tunnel DTLS-... 16:13:02 UTC Sun... 11684</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Details

The following ACL is being applied to this session:
```
access-list DAP-ip-user-50418800; 1 elements; name hash: 0xe4c6096c
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any
```

The following IPv6 ACL is being applied to this session:
```
access-list DAP-ip-user-50418800; 1 elements; name hash: 0xe4c6096c (dynamic)
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any object-group rdp (hitcnt=0) 0x27408a58
access-list DAP-ip-user-50418800 line 1 extended permit tcp any any eq 3389 (hitcnt=0) 0xdc9892a8
```
Troubleshooting DAP : Syslog

• Debug DAP trace not always practical in production
  - too much info
  - no filtering on username

• Syslog Message with good DAP info : **username** and **selected DAP records**

%ASA-6-734001: DAP: User scratchy@labrats.se, Addr 192.168.254.4, Connection AnyConnect: The following DAP records were selected for this connection: **ITsupport Access**
Troubleshooting Hostscan Component

• Enable Debugging level at ASDM, then rerun test on problematic client

  ![Configuration > Remote Access VPN > Secure Desktop Manager > Global Settings](image)

  Global Settings
  
  Logging level controls CSD logging on all VPN user endpoints that run CSD. By default, the Logging Level is set to Errors. Each event level is cumulative. For example, the Warnings option enables logging for both errors and warnings.

  ![Logging Level](image)

  • Check Host Scan log files on problematic client
    - libcbsd.log
    - cscan.log, detailed posture attributes
  
  • These are located at
    - Windows %LOCALAPPDATA%\Cisco\Cisco HostScan\log
    - MAC/Linux : ~/.cisco/hostscan/log

  • Examine Windows Event logs
Agenda

Introduction

AnyConnect Fundamentals

AnyConnect Network Integration

Provisioning Client Certificates

AAA Deep Dive Client Certificates

AAA Deep Dive RADIUS & LDAP

Posture Checking

Securing the Client

Customizing the User Experience
(No) Split Tunnelling Policy

- Defined in Group Policy: whether to allow traffic outside of the tunnel
Note on Split Tunnelling Policy for mobile devices

- Even with no Split Tunneling (Tunnel All Networks), certain traffic from mobile devices (e.g. iTunes) goes outside the tunnel.
Note on Split Tunnelling Policy for mobile devices

• Even with no Split Tunneling (Tunnel All Networks), certain traffic from mobile devices (e.g. iTunes) goes outside the tunnel.
Split Tunneling Example (IPv4 and IPv6)

Extended ACL (extended ACLs are unified v4 v6)

Add IPv4 and IPv6 networks in the Source of ACE
Client Bypass Protocol

- Defines if AnyConnect allows traffic in the clear if it has not been assigned an IP address for the protocol
- Example, if no IPv6 address assigned by ASA, should AnyConnect allow IPv6 in the clear?
- Default is “disable” : drop
No Split Tunneling but Allow Local LAN Access

- Group Policy
- Exclude Network List
  - 0.0.0.0/32
  - ::/128

- Must also be allowed per client profile

- ASA

- Denied
AnyConnect Client Firewall

- Uses the native OS firewall, to configure rules on the endpoint device
- Windows and MAC only
- L3/L4 IPv4 and IPv6 rules
- ASA will pass the firewall rules to the client on connect
- Rules will be applied when:
  - The VPN tunnel is active
  - The VPN tunnel is using Always-On but is in fail-close state (e.g. allowing local printing)
Client Firewall: ASDM Configuration

- Public Interface
  Any physical interface that has direct connectivity to a network \textit{other than the VPN}

  Only applied with a \textit{split tunneling configuration}

  If public rules can not be applied -> full tunneling will be applied.

- Private
  The Virtual Adapter interface
  Rules are independent of the public interface
Per App VPN

- Available for iOS 7.0+, Samsung Knox, Generic Android 5.0+
- Allows for tunneling specified subset of apps through one AnyConnect tunnel
  - save resources: don’t Netflix over VPN tunnel
  - security: don’t allow non enterprise apps on enterprise network
  - avoiding tunneling trusted cloud applications (to minimize latency)
- Configured via DAP
- Works with or without an Enterprise MDM
Dynamic Split Tunneling Exceptions

- AnyConnect 4.5 Windows and MAC
- Exclude specified DNS names from AnyConnect tunnel
  - save resources: don’t Netflix over VPN tunnel
  - security: don’t allow non-enterprise apps on enterprise network
  - avoiding tunneling trusted cloud applications (to minimize latency)
- Configured via custom attributes
Configuring Dynamic Split Tunneling Exceptions

Configure Custom Attribute Type: dynamic-split-exclude domains

Configure Custom Attribute Name: of type:dynamic-split-exclude domains and include the excluded domains separated by commas

Configure Custom Attributes in Group Policy
Dynamic Split Tunneling Exceptions

AnyConnect changes routing table dynamically from DNS responses to specified domains.
Seamless Security with Always-On

- Encourage/force (some) users to always be connected over VPN when off-premises
  - works on Windows, MAC
- Objective #1: Seamless, simple user experience
  - Automatic Connection, "I am always at work"
- Objective #2: Increased Security if surfing out via Enterprise Proxy or NGFW

**Trusted Network Detection**
automatically establishes tunnel if not on enterprise network

**Always On**
Blocks traffic until tunnel is established,
AnyConnect Client Profile with Always-On

- Define conditions for Trusted Network Detection
  - DNS Servers and Domain
  - AC 4.2: https://reachability

- Define Always-On (must also define Server List)

- Connection Failure Policy: Open or Closed
  - Balance Security Requirements vs. Risk of No Network...
  - If Closed, specify if traffic will be allowed for X minutes if Captive Portal is detected
  - "Last VPN Local Resource Rules": Last Client Firewall Rules

- If a profile with Always-On is downloaded, the other profiles are deleted

Always On
Blocks traffic until tunnel is established, except if Captive Portal is detected
Disabling Always-On with DAP

- Always-On can be disabled by DAP
- AnyConnect will remember this setting when disconnected
Always-On and Strict Certificate Trust

• With Always-On, AnyConnect always applies strict certificate trust (regardless of the localpolicy file)

• With Always-On, AnyConnect blocks outgoing traffic to all destinations other than the ASAs in the server-list of the client profile (and DNS and DHCP)

• If the CRL of ASA certificate has expired, the client will not be able to retrieve a new CRL, and connection will fail in previous versions (pre 3.1) of AnyConnect
Multiple Client Profiles on ONE Client?

• ONE client typically only has ONE Client Profile..... but

• Old Client Profiles are not deleted, multiple profiles maybe accumulated
  - a consultant connecting to different ASAs
  - testing/piloting AnyConnect using different profile names

• Upon connection, the profile assigned by the chosen ASA head end is downloaded and applies for the VPN session

• If a profile with Always-On is downloaded, the other profiles are deleted
Multiple Client Profiles on ONE Client?

• **ONE** client typically only has **ONE** Client Profile..... but

• Old Client Profiles are not deleted, multiple profiles maybe accumulated
  - a consultant connecting to different ASAs
  - testing/piloting AnyConnect using different profile names

• Upon connection, the profile assigned by the chosen ASA head end is downloaded and applies for the VPN session

• If a profile with Always-On is downloaded, the other profiles are deleted
Always On does not work for Mobile Devices

- Forcing Always-On not possible due to lack of OS APIs
  - ... vendor considerations for battery life, security
- Trusted Network Detection (TND) for Android
- On Demand VPN for iOS

Cisco Security Connector (NOT VPN)

See Aaron Woland @ BRKSEC-3444
On Demand VPN for iOS - Configuration

- VPN automatically connected when traffic directed to predefined domain
- Requires client certificate
- Configured in Client Profile/Server List/Additional Mobile Only Settings

![AnyConnect Client Profile]

Always connect when going to .labrats.se
On Demand VPN for iOS – User Experience
On Demand VPN for iOS – User Experience

Welcome to the Cats Website

New Mousetrap Locations - ProjectX
Research Project GoldFish evasive techniques in Aquarium
Claws Sharpening
On Demand VPN for iOS – User Experience

Welcome to the Cats Website

New Mousetrap Locations - ProjectX
Research Project GoldFish evasive techniques in Aquarium
Claws Sharpening
On Demand VPN for iOS – User Experience

Welcome to the Cats Website

New Mousetrap Research Project: Counting virtual mice in aquatic Claws Sharpening
Options for redirecting Internet Traffic to Proxy

- WCCP in router/switch
- WCCP in ASA
  - caveats: proxy must be on same interface as clients
- Explicit Proxy Settings in Browsers
  - configured by ASA/AnyConnect, GPOs, DNS, DHCP etc.
  - caveats: some applications may not follow proxy setting
Agenda
Seamless Office Experience by Start-Before-Logon

- Allows (some) Windows users to connect VPN before logging into computer
- Why? Allow domain-logon, GPOs, logon-scripts, change passwords, etc...
- Can be used with or without Always-On
Configuring SBL in Client Profile

- May make it user controllable

Note: Client certificates in User Store typically not accessible before logon (no knowledge of who the user is).
Machine certificates will work
Client certificates on Smart Cards will work!
SBL User Experience

Mouse Click Needed!
SBL User Experience with Smart Cards (2)
SBL User Experience with Smartcards (3)

Smartcard can also be leveraged for Domain logon, creating an “SSO Experience”
Running Scripts after Connect and Disconnect

• Runs a predefined script when (some) users connect to (or disconnect from VPN)
• Any native script language understood by client (*.vbs, *.sh etc)
• Script can be downloaded from ASA, or distributed by some other means
• Why?
  - Allow mapping of drives, GPO-update when SBL is not possible (e.g. behind a captive portal).
  - Also works on non domain members, including MAC, Linux
Running Scripts after Connect and Disconnect

- Runs a predefined script when (some) users connect to (or disconnect from VPN)
- Any native script language understood by client (*.vbs, *.sh etc)
- Script can be downloaded from ASA, or distributed by some other means
- Why?
  - Allow mapping of drives, GPO-update when SBL is not possible (e.g. behind a captive portal).
  - Also works on non domain members, including MAC, Linux
Running Scripts after Connect and Disconnect

- Runs a predefined script when (some) users connect to (or disconnect from VPN)
- Any native script language understood by client (*vbs, *.sh etc)
- Script can be downloaded from ASA, or distributed by some other means
- Why?
  - Allow mapping of drives, GPO-update when SBL is not possible (e.g. behind a captive portal).
  - Also works on non domain members, including MAC, Linux
Running Scripts after Connect and Disconnect

- Runs a predefined script when (some) users connect to (or disconnect from VPN)
- Any native script language understood by client (*.vbs, *.sh etc)
- Script can be downloaded from ASA, or distributed by some other means
- Why?
  - Allow mapping of drives, GPO-update when SBL is not possible (e.g. behind a captive portal).
  - Also works on non domain members, including MAC, Linux
Configuring Scripting

- Enable Scripting in AnyConnect Client Profile
- Optionally: Import script to ASA for download to all clients
- Alternatively, use other means of putting the script in the script directory for desired clients
On the Client : The Scripts Folder

- AnyConnect executes the script in the folder that starts with "OnConnect"/"OnDisconnect" after VPN connection/disconnection
- Only one script is executed, but that script can launch other scripts
- Troubleshooting :
  - Check that script exists in folder and that AnyConnect Profile allows scripting.
  - Check that script executes ok when invoked from local machine (permissions etc).
## Summary: Firepower Threat Defense with FMC

<table>
<thead>
<tr>
<th>Feature</th>
<th>Works in 6.2(2)?</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA with RADIUS</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>AAA with LDAP authorization</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>AAA with client cert (RADIUS AuthZ)</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>SGTs in Access Policy</td>
<td>YES</td>
<td>Flexconfig needed</td>
</tr>
<tr>
<td>Posture (with ISE or Hostscan)</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Dynamic Access Policy (DAP)</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Always-On</td>
<td>YES</td>
<td>Client feature</td>
</tr>
<tr>
<td>Start-Before-login</td>
<td>YES</td>
<td>Client feature</td>
</tr>
<tr>
<td>Scripting</td>
<td>YES</td>
<td>Client feature</td>
</tr>
</tbody>
</table>
Unsupported VPN features as of FTD 6.2.2

- Hostscan
- Endpoint Posture Assessment
- Dynamic Access Policy
- VPN Load Balancing
- Local Authentication
- TACACS, Kerberos (KCD) Authentication
- RSA SDI
- Radius CoA
- Secondary/Double Authentication
- Single Sign-on using SAML 2.0
- LDAP Authorization (LDAP Attribute Map)
- Browser Proxy
- SCEP URL Forwarding
- Anyconnect Customization
- Anyconnect Localization
- Anyconnect Profile Editor
- NAT-Assigned IP to Public IP Connection
- Secure Mobility Solution (Integration with WSA)
- Anyconnect Custom Attributes: Features supported via Anyconnect Custom Attributes are thus not supported e.g.- per-App VPN for Mobile devices, Deferred update
Example Scripts on CCO

Cisco VPN Client Tools
Download Software

Release Sample Scripts

Find Release  Find
Expand all  Close all

All Releases
- AnyConnect
  - Translation Files
  - DART
  - Sample Transform
  - Profile Editor
  - Sample Scripts
- Hostscan
- 5.x
- 4.x

Related Information

Sort By: File Name

Download Nov
AnyConnectScriptSamples.zip
Release Date: 03/NOV/2009
AnyConnect Script Samples.
Size: 10.90 KB (11158 bytes)

Add to cart
Conclusion

- Secure Client with a Seamless User Experience
- Strong authentication and Granular Access Control with AAA and DAP
- Consider using ISE for Unified Policy (VPN, Wired, Wireless)
- Find Balance between Requirements and Complexity (testing, maintenance)
- Carefully examine required features before selecting FTD instead of ASA
- Good security and networking skills are essential, but also knowledge of adjacent technologies such as Active Directory, LDAP and PKI, ISE… as well as different client platforms
Important Information

• No animals were harmed during the making of this session
Important Information

• No animals were harmed during the making of this session
Continue Your IPv6 Education

• Demos in the Cisco campus: SRv6, 6CN (DevNet Zone)
• Walk-in Self-Paced Labs: LABCRS-1000, LTRRST-2016
• Lunch & Learn: Tuesday, Wednesday
• Meet the Engineer 1:1 meetings
• Related sessions: BRKRST-2667, BRKRST-2616, BRKSEC-2003, BRKSEC-3033, BRKSEC-3771, BRKRST-3304, BRKRST-2044, BRKRST-2312, BRKRST-3045, BRKSEC-3003, BRKRST-2022, BRKSPG-2300, BRKSEC-3200
• World of Solutions: ask about IPv6 support ;-)
Security Joins the Customer Connection Program

Customer User Group Program

- **Who can join:** Cisco customers, service providers, solution partners and training partners
- **Private online community** to connect with peers & Cisco’s Security product teams
- Monthly **technical & roadmap briefings** via WebEx
- Opportunities to **influence product direction**
- Local **in-person meet ups** started Fall 2016
- **New member thank you gift** & badge ribbon when you join in the Cisco Security booth
- **Other CCP tracks:** Collaboration & Enterprise Networks

---

**Join in World of Solutions**

Security zone → Customer Connection stand

- Learn about CCP and Join
- New member thank-you gift*
- Customer Connection Member badge ribbon

---

**Join Online**

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

Come to Security zone to get your new member gift* and ribbon

---

* While supplies last
Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKSEC-2501
• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Tech Circle
• Meet the Engineer 1:1 meetings
• Related sessions
Thank you
You're
Cisco Live!
Extra slides: How to get Started with FTD using FMC and AnyConnect
Creating pfx (PKCS#12) file with OpenSSL

openssl genrsa -out loke-ftd.key 2048

openssl req -new -key loke-ftd.key -out loke-ftd.csr

openssl pkcs12 -export -out loke-ftd.pfx -inkey loke-ftd.key -in loke-ftd.cer -certfile CA.cer
FMC Add Certificates to NGFW device
FMC Add Certificates

Add PKCS12 File

Install a new certificate on the device using a PKCS12 file. This new certificate must be associated with a certificate object to refer to it in other policies.

- **Device**: loke-ftd
- **Cert Enrollment**: loke-ftd-p12
- **PKCS12 File**: loke-ftd.pfx
- **Passphrase**: ********

Add | Cancel

Certificates

<table>
<thead>
<tr>
<th>Name</th>
<th>Enrollment Type</th>
<th>CA Certificate</th>
<th>Identity Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>loke-ftd</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>loke-ftd-p12</td>
<td>PKCS12 file</td>
<td>Available</td>
<td>Available</td>
</tr>
</tbody>
</table>
FMC Config Wizard

Remote Access VPN Policy Wizard

Targeted Devices and Protocols
This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

- Name: lake-RA-config
- Description:
- VPN Protocols: SSL, IPsec-DESv2
- Targeted Devices: Available Devices, Selected Devices

Before You Start
Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy:

- Authentication Server: Configure Radius or RADIUS Server Group to authenticate VPN clients.
- AnyConnect Client Package: Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.
- Device Interface: Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.
- Device Identity Certificate: Configure Cert Enrollment object and install it on the targeted devices to serve as VPN server identity certificate.
Remote Access VPN Policy Wizard

Connection Profile:
Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

- **Connection Profile Name**: Loke-RA-config
  - This name is configured as a connection alias, it can be used to connect to the VPN.

- **Authentication, Authorization & Accounting (AAA)**:
  - Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN.
  - **Authentication Method**: AAA Only
  - **Authentication Server**: ISE
  - **Authorization Server**: Use same authentication server
  - **Accounting Server**: ISE

- **Realm or RADIUS Server Group**
  - **ISP**
  - **RADIUS Server Group**

- **RADIUS Server**
  - **IP Address/Hostname**: 10.1.41.70
  - **Authentication Port**: 1812
  - **Accounting Port**: 1645

Add RADIUS Server Group

- **Name**: ISE
- **Description**: ISE Radius Server Group
- **Enable authorize only**
- **Enable interim account update**
- **Interval**: 24 hours
- **Group Accounting Mode**: Single
- **Login Interval**: 10 seconds
- **Realm**: ISE
- **RADIUS Servers (Maximum 16 servers)**

Save | Cancel
FMC Config Wizard (3)
FMC Config Wizard (4) Add AnyConnect image
FMC Config Wizard: Specify Interfaces

Remote Access VPN Policy Wizard

Network Interface for Incoming VPN Access
Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone: Z_outside

Enable DTLS on member interfaces

Device Certificates
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment: ike-fd-314
FMC Config Wizard : Summary

Remote Access VPN Policy Wizard

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings:

- **Name**: Labrats-RA-Config
- **Device Targets**: loke-ftd
- **Connection Profile**: Labrats-RA-Config
- **Connection Alias**: Labrats-RA-Config
- **AAA**:
  - **Authentication Method**: AAA Only
  - **Authentication Server**: 1SE
  - **Authorization Server**: 1SE
  - **Accounting Server**: 1SE
- **Address Assignment**:
  - **Address from AAA**: -
  - **DHCP Servers**: -
  - **Address Pools (IPv4)**: Loke-ftd-pool
  - **Address Pools (IPv6)**: Loke-ftd-pool-v6

Additional Configuration Requirements

- **Access Control Policy Update**: An Access Control rule must be defined to allow VPN traffic on all targeted devices.
- **NAT Exemption**: If NAT is enabled on the targeted devices, you must define a NAT rule to exempt VPN traffic.
- **DNS Configuration**: To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.
- **Network Interface Configuration**: Make sure to add interface from targeted devices to SecurityZone object 'Z_outside'.
- **Device Identity Certificate**: Make sure to install identity certificate on targeted devices using PKI Cert object 'Loke-ftd-p12'

Back | Finish
FMC Troubleshooting

VPN Troubleshooting
Table View of VPN Troubleshooting

Active Sessions
Table View of Active Sessions

Cisco Live!

BRKSEC-2501 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 252