



# Possibilities

#CiscoLive

# AnyConnect Optimization

Improving your Remote Access Solution

Matthew Yengle, Technical Consulting Engineer

DGTL-TSCSEC-508



June 2-3, 2020 | [ciscolive.com/us](https://ciscolive.com/us)

#CiscoLive



# About Me

Matthew Yengle, CCIE Security #63968

Technical Consulting Engineer

Global CX Centers, VPN



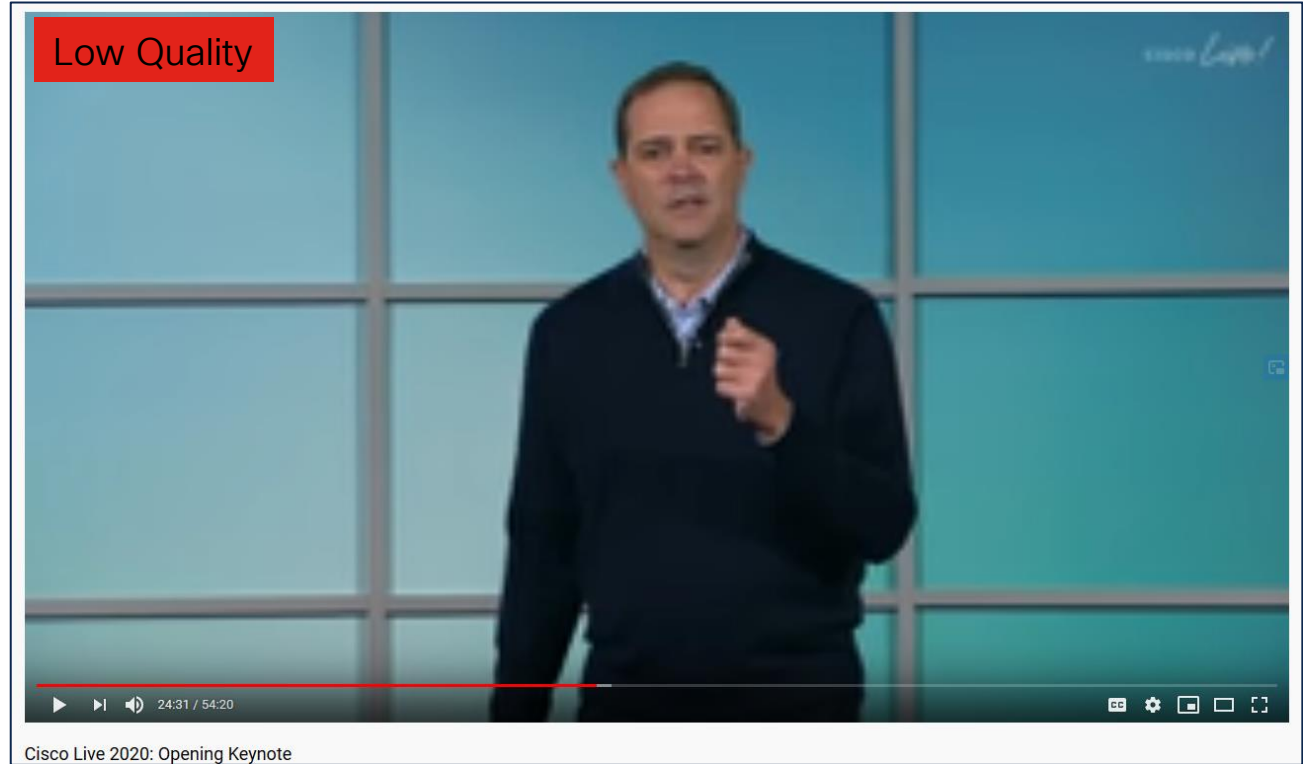
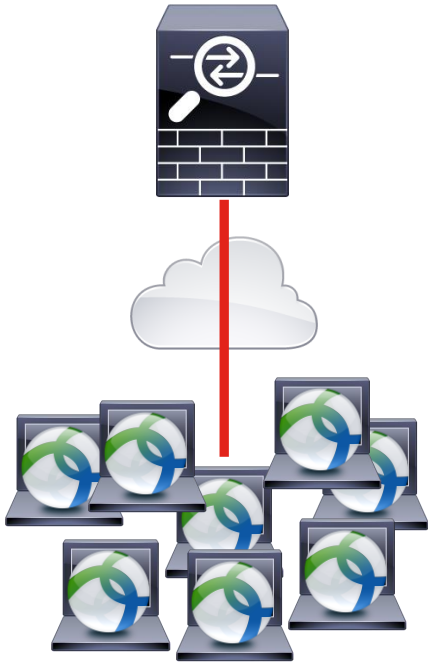
# Agenda

- Introduction
- Finding the bottlenecks
- Distributing the load
- Maximizing the performance
- Fine Tuning
- Conclusion

# Scenario



# Scenario

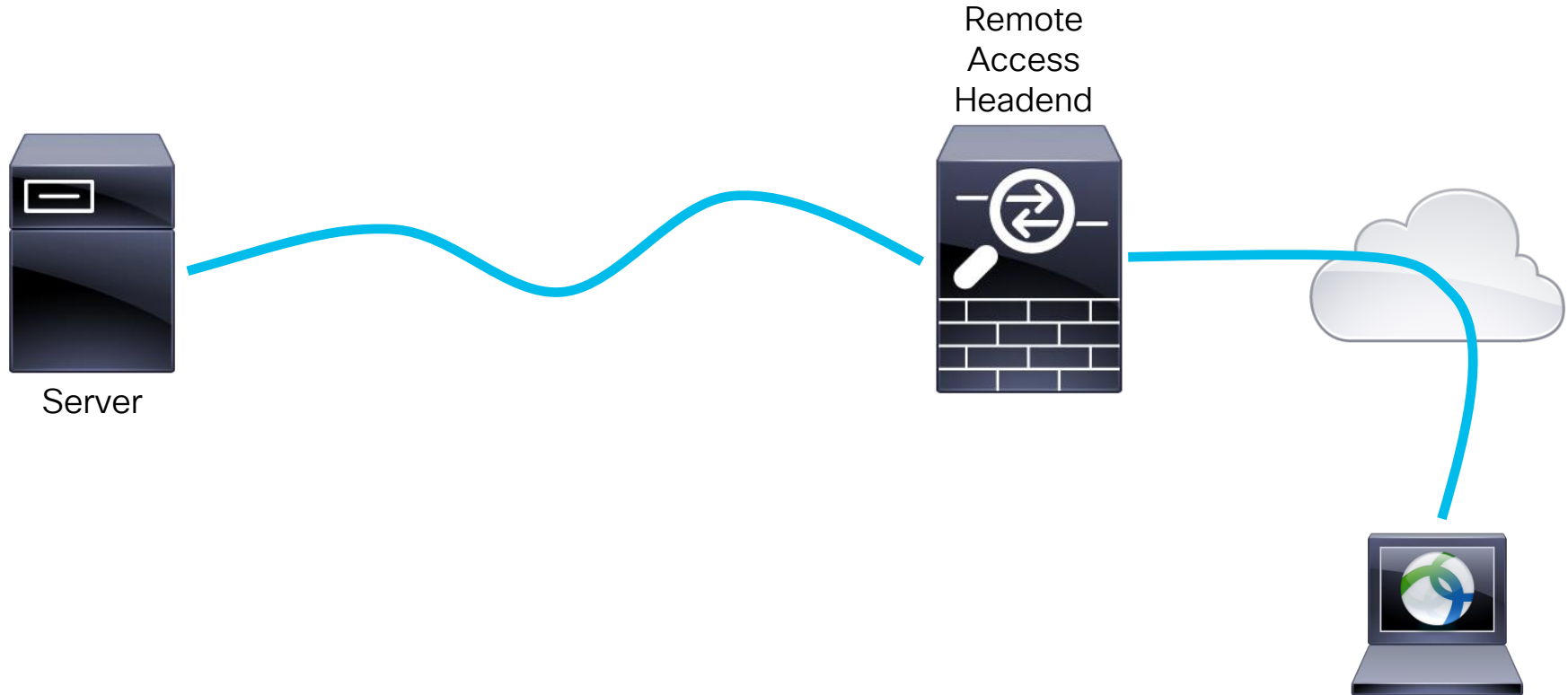




The background is a dark blue field filled with numerous small, semi-transparent squares and dots in various colors including light blue, green, yellow, orange, and red. These elements are scattered across the frame, with a higher concentration of orange and red dots forming a diagonal streak from the upper right towards the lower right.

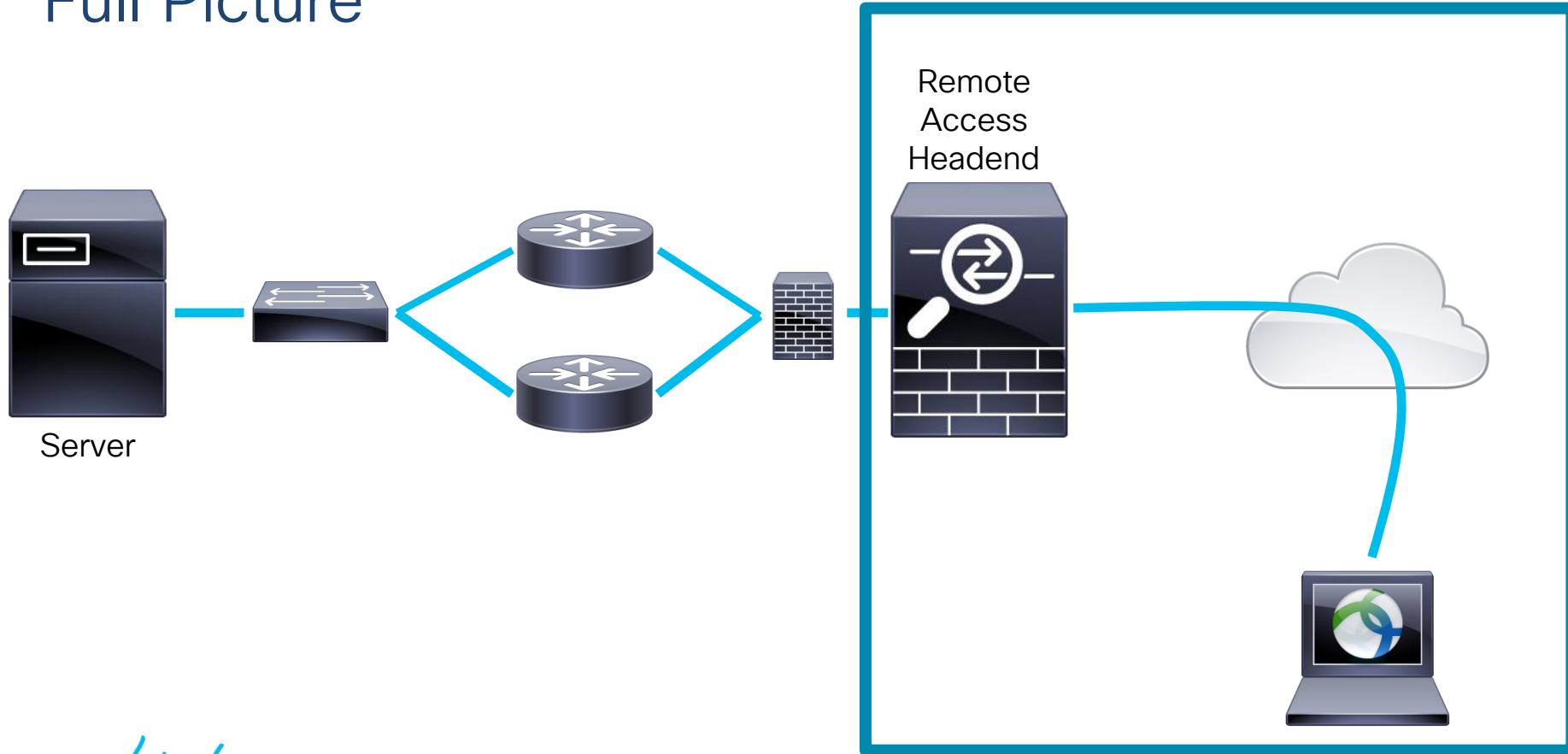
# Finding the Bottlenecks

# Know Your Network





# Full Picture



# Factors Outside of our Network

ASA 5585-X  
SSP-60

Crypto  
Throughput  
5 Gbps



ISP  
Rate Limited  
to 1 Gbps



# Scaling Numbers

```
ASAv# show crypto accelerator statistics
```

```
Crypto Accelerator Status
```

```
-----
```

```
[Capability]
```

```
Supports hardware crypto: False
```

```
Supports modular hardware crypto: False
```

```
Supported TLS Offload Mode: SOFTWARE
```

```
Max accelerators: 1
```

```
Max crypto throughput: 225 Mbps
```

```
Max crypto connections: 750
```

Data Plane

Control Plane

# Platform data sheets

- **Cisco ASA 5500 Series Data Sheet**  
<https://www.cisco.com/c/en/us/products/collateral/security/asa-firepower-services/datasheet-c78-742475.html>
- **Cisco ASA 5585-X Stateful Firewall Data Sheet**  
<https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-730903.html>
- **Cisco ASA with FirePOWER Services Data Sheet**  
<https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html>
- **Cisco Adaptive Security Virtual Appliance (ASAv) Data Sheet**  
<https://www.cisco.com/c/en/us/products/collateral/security/adaptive-security-virtual-appliance-asav/datasheet-c78-733399.html>
- **Cisco Firepower 1000 Series Data Sheet**  
<https://www.cisco.com/c/en/us/products/collateral/security/firepower-1000-series/datasheet-c78-742469.html>
- **Cisco Firepower 2100 Series Data Sheet**  
<https://www.cisco.com/c/en/us/products/collateral/security/firepower-2100-series/datasheet-c78-742473.html>
- **Cisco Firepower 4100 Series Data Sheet**  
<https://www.cisco.com/c/en/us/products/collateral/security/firepower-4100-series/datas>
- **Cisco Firepower 9300 Series Data Sheet**  
<https://www.cisco.com/c/en/us/products/collateral/security/firepower-9000-series/datasheet-c78-742471.html>



For Your  
Reference

# ASA Datapath

```
ASAv# show cpu usage
CPU utilization for 5 seconds = 81%; 1 minute: 79%; 5 minutes: 79%
```

```
Virtual platform CPU resources
-----
```

```
Number of vCPUs           :      4
```

```
ASAv# show process cpu-usage sorted non-zero
```

PC	Thread	5Sec	1Min	5Min	Process
-	-	41.7%	40.5%	40.3%	DATAPATH-0-1602
-	-	37.6%	37.0%	36.6%	DATAPATH-1-1603

Packet processing for VPN and basic Firewall features.

# ASA Control Point

CPU utilization appears low

```
ASAv# show cpu usage
CPU utilization for 5 seconds = 3%; 1 minute: 2%; 5 minutes: 2%
```

```
ASAv# show cpu detail
```

Break down of per-core data path versus control point cpu usage:

Core	5 sec	1 min	5 min
Core 0	26.9 (2.5 + 24.4)	22.5 (2.2 + 20.3)	21.7 (2.2 + 19.5)
Core 1	0.6 (0.6 + 0.0)	0.5 (0.5 + 0.0)	0.5 (0.5 + 0.0)
Core 2	27.1 (1.9 + 25.2)	26.6 (1.4 + 25.2)	19.0 (1.4 + 17.6)
Core 3	1.2 (1.2 + 0.0)	0.8 (0.8 + 0.0)	0.8 (0.8 + 0.0)

How the CP usage is calculated  
 $24.4 + 25.2 = 49.6\%$



# More on ASA Troubleshooting

Troubleshooting ASA Firewalls

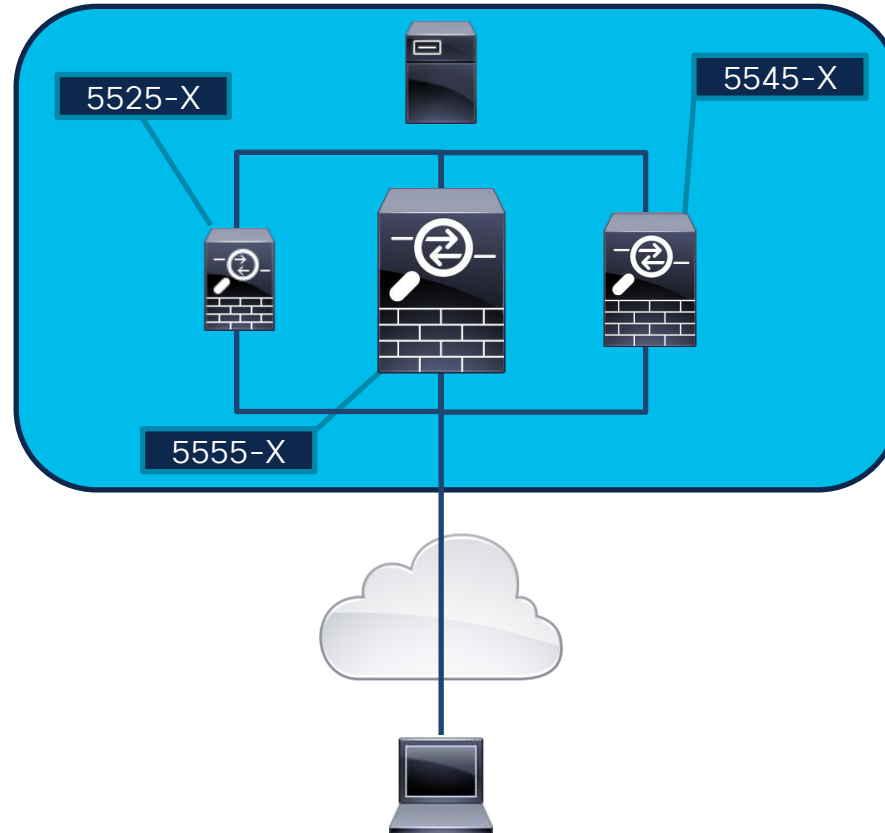
DGTL-BRKSEC-3020



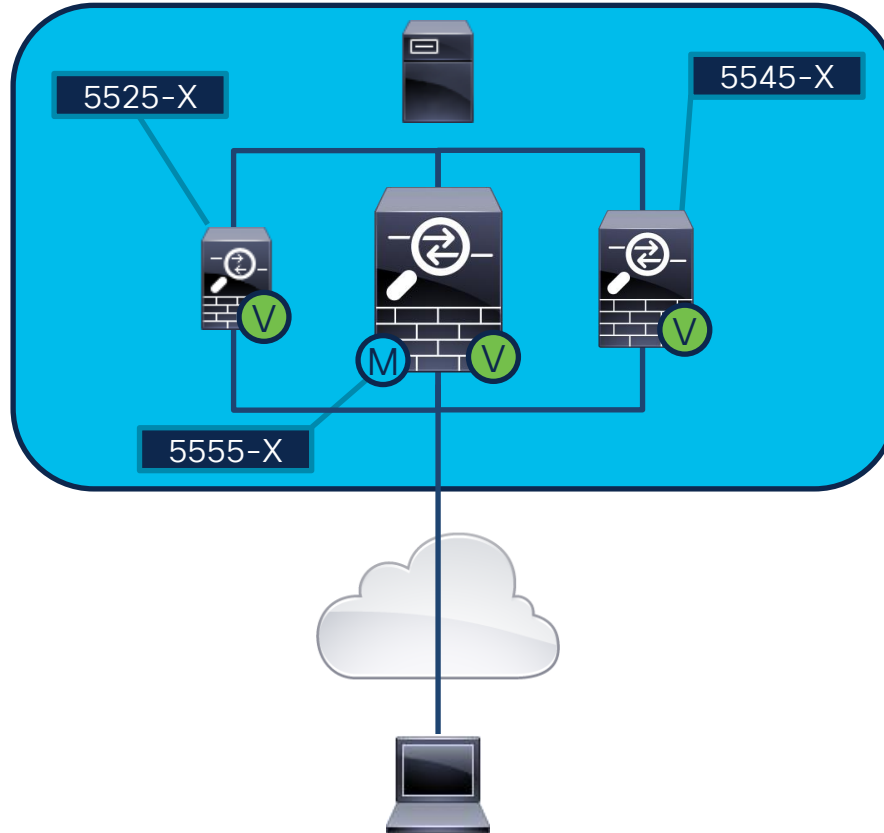
For Your  
Reference

# Distributing the Load

# VPN Load Balancing

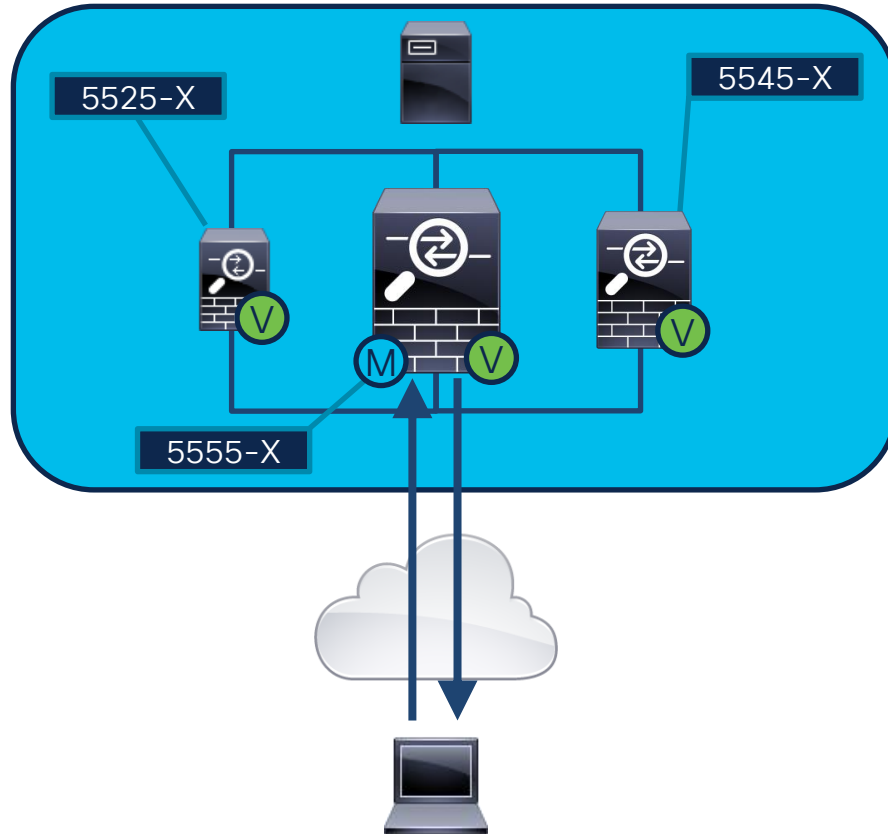




# About VPN Load Balancing



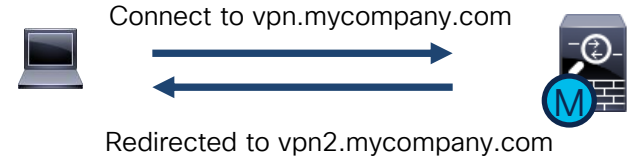
- $N + 1$  Public IP Addresses (FQDNs) and certificates
- ASAs must be on same LAN
- Mix of ASA hardware (that supports AC)
- Same version recommended (but not required)
- Supports up to 10 ASAs

# How it works

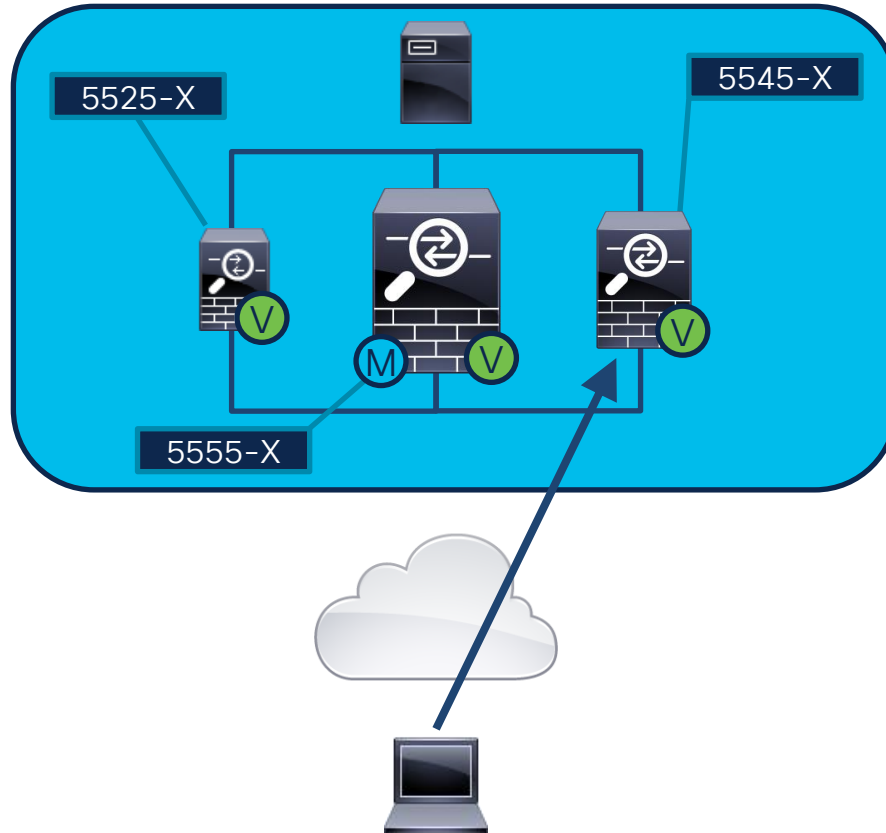



-  VPN Load Balance Master
-  VPN ASA

## Step 1 – Master ASA



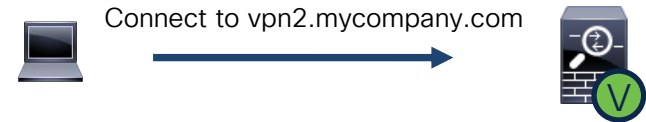
# How it works



 VPN Load Balance Master

 VPN ASA

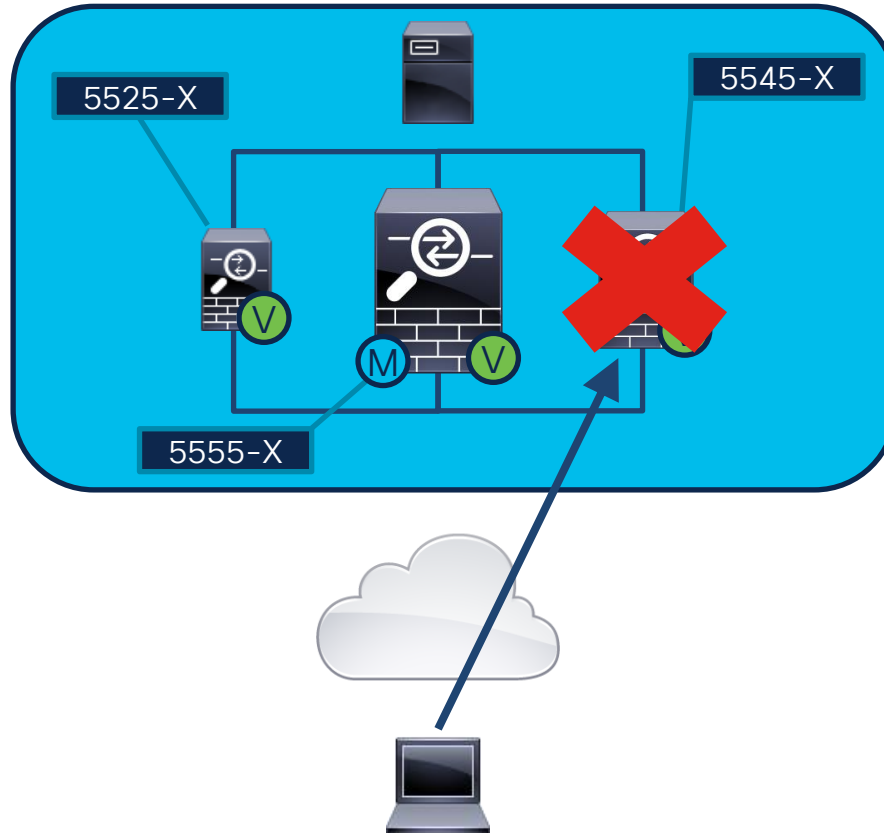
## Step 2 – VPN ASA



Each new connection to the Master ASA FQDN will be redirected to a participating ASA VPN.

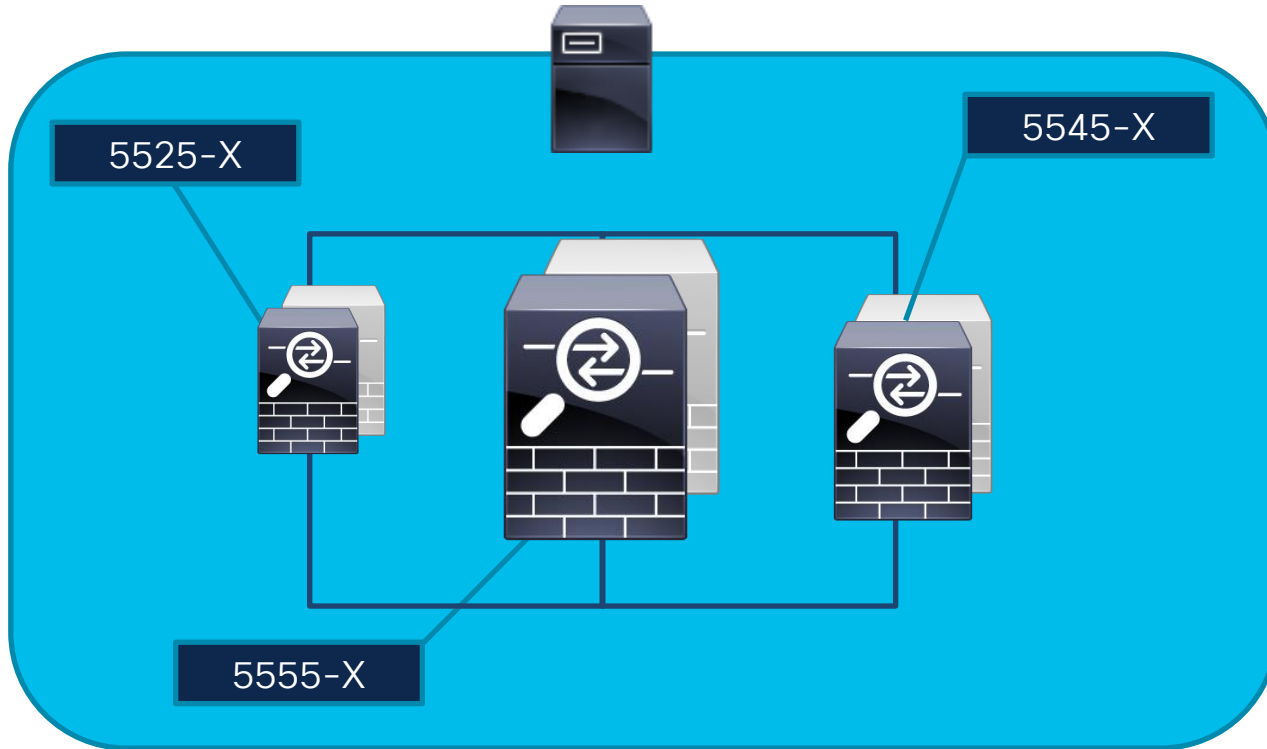


# Failure Recovery



- ASAs do not share stateful connections for the AnyConnect sessions.
- In case any ASA fails, those AnyConnect users will be disconnected.
- The end user will perform the same, familiar steps to re-connect.
- If the Master ASA fails, another ASA will automatically take on the Master role.

# Additional Redundancy



- Active/Standby Stateful Failover is supported.
- If Active ASA fails, Standby resumes AnyConnect sessions.



Active



Standby

# More on VPN Load Balancing

Configuration and additional information

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa914/configuration/vpn/asa-914-vpn-config/vpn-ha.html>

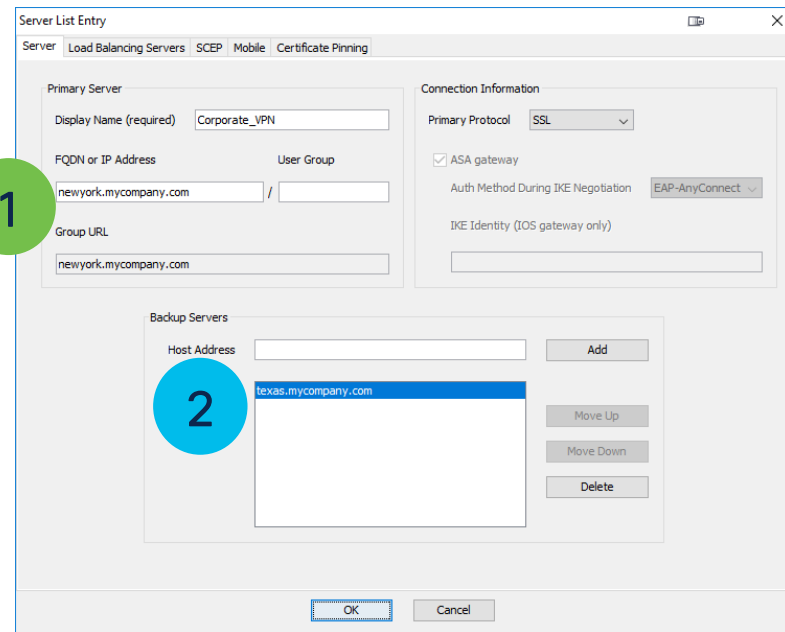
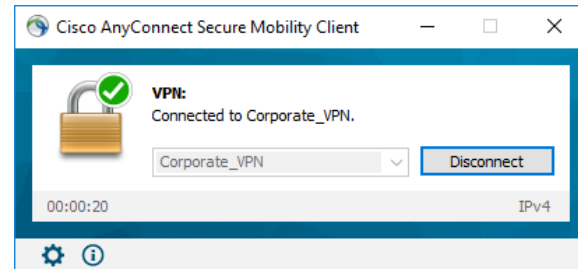
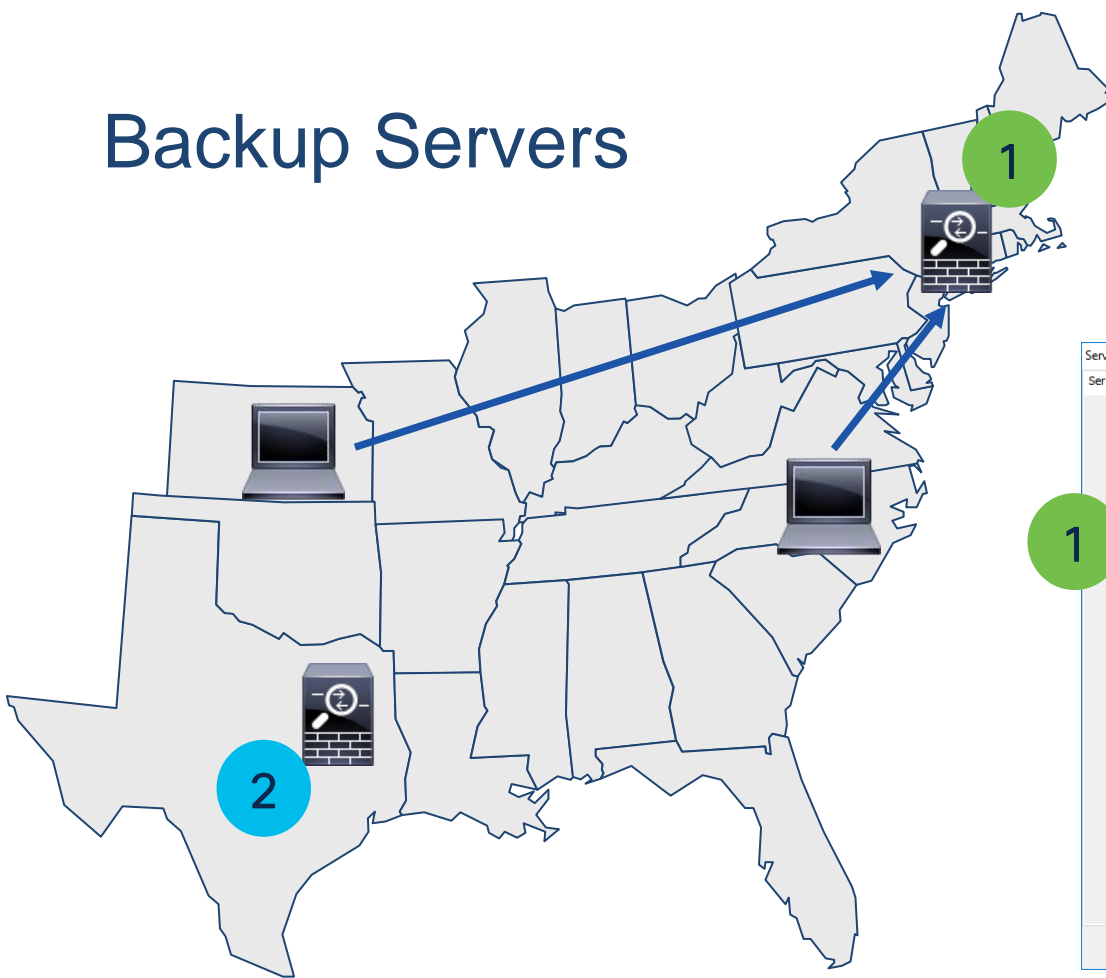
Deeper Look at Election Process

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118078-technote-vpn-00.html>

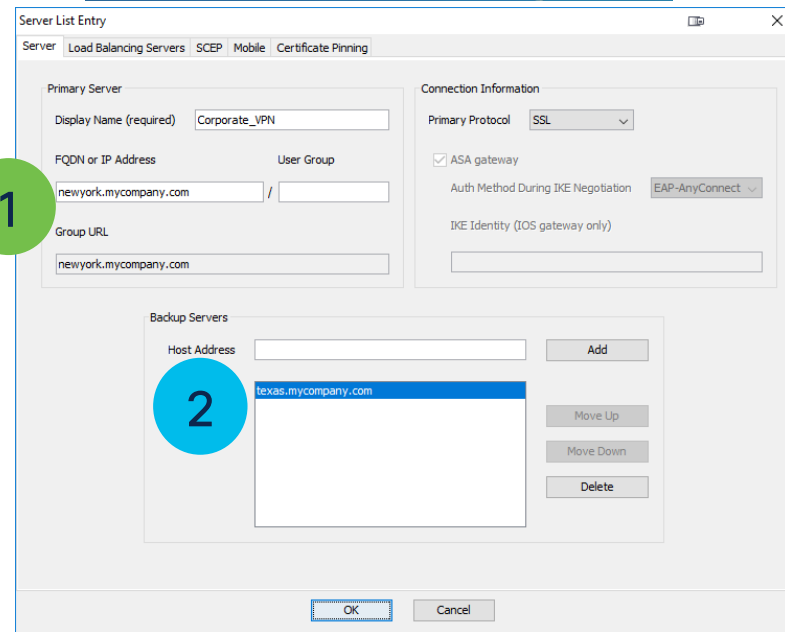
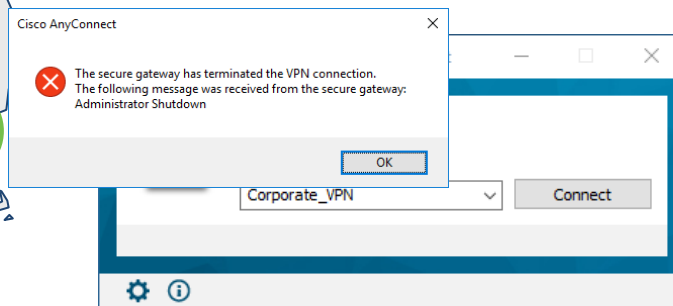
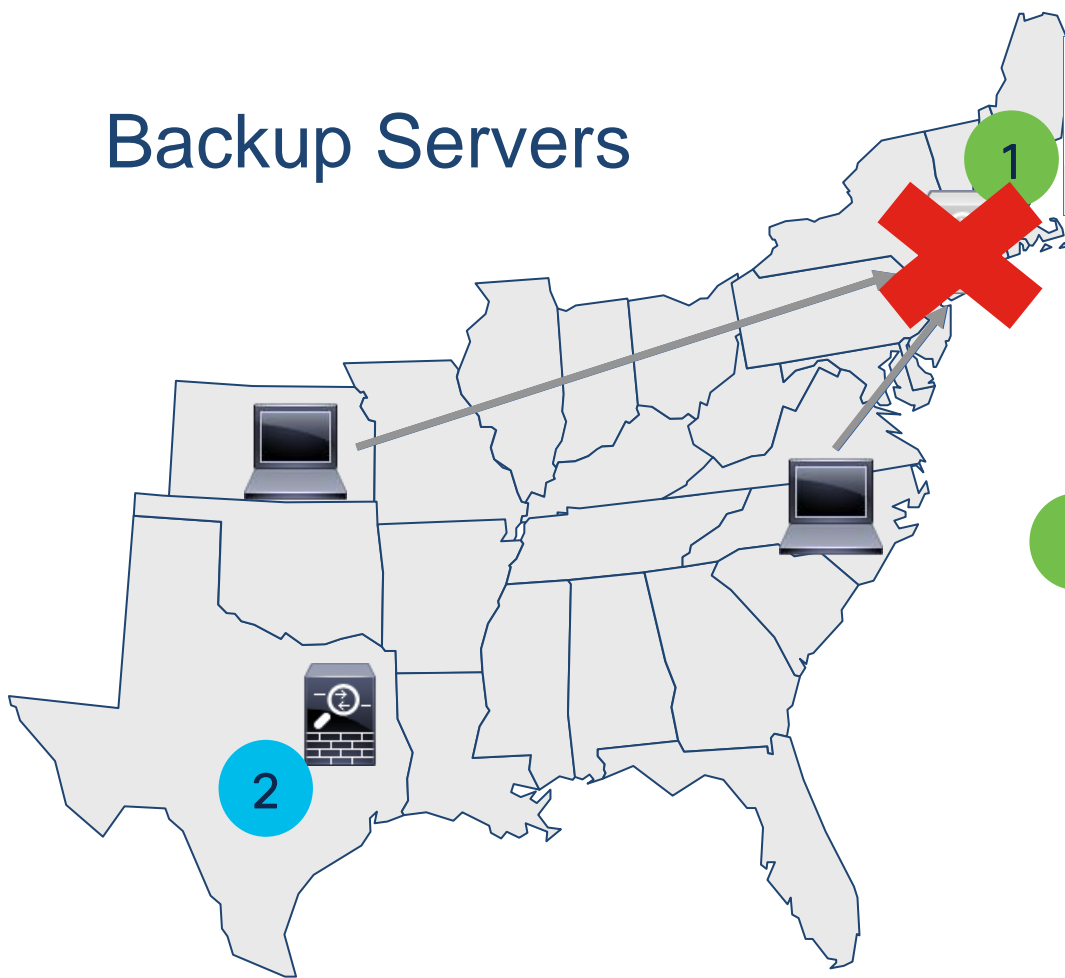


For Your  
Reference

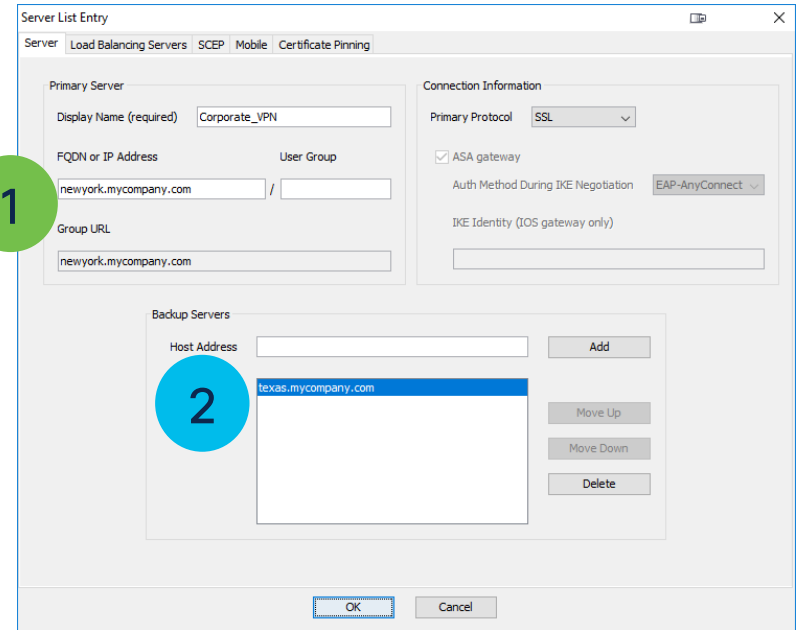
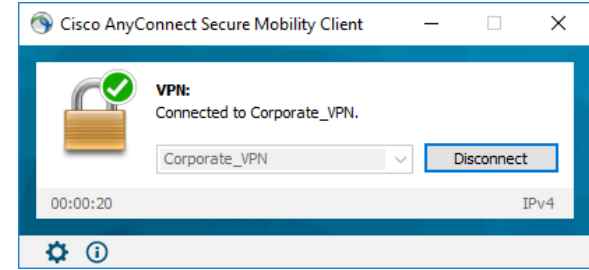
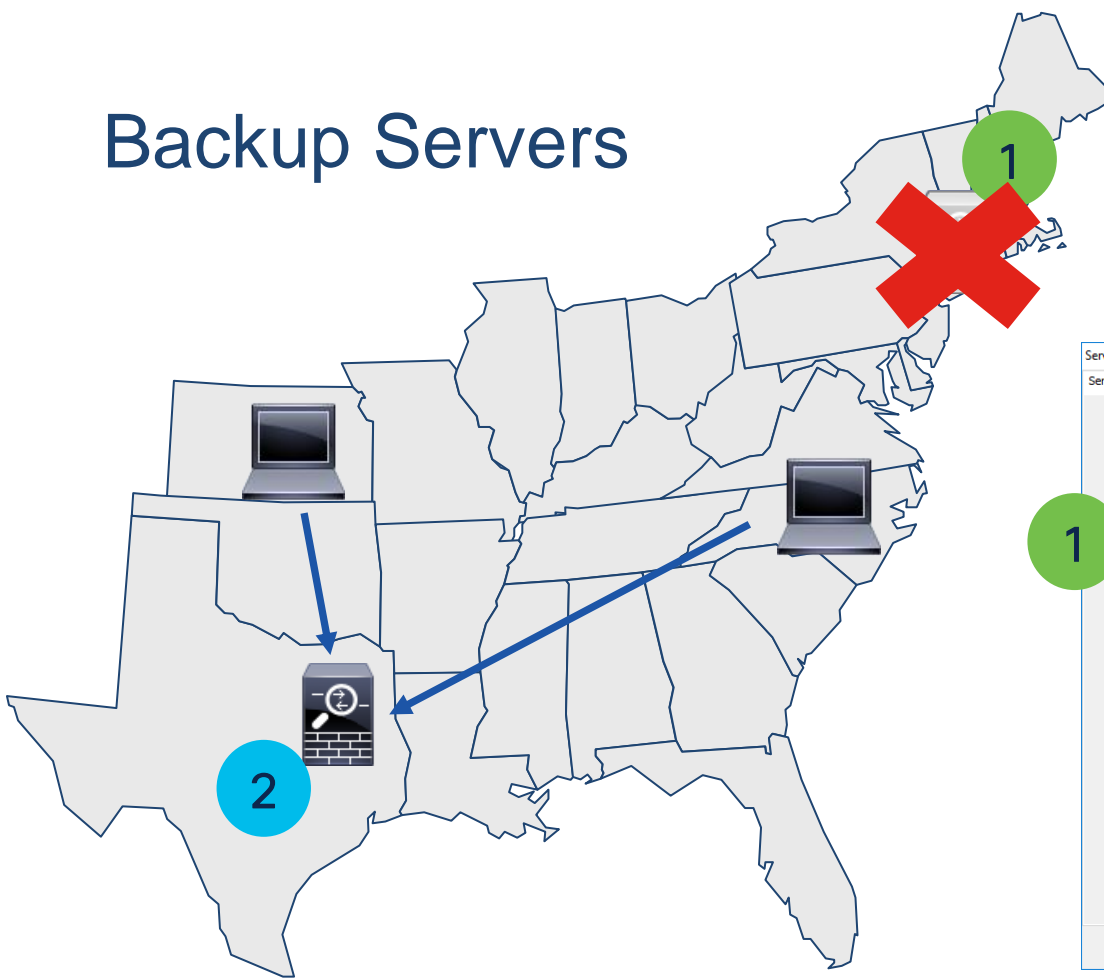
# Backup Servers



# Backup Servers



# Backup Servers





# AnyConnect VPN Profile Editor

Full guide on the VPN Profile Editor, including Backup Server List

[https://www.cisco.com/c/en/us/td/docs/security/vpn\\_client/anyconnect/anyconnect\\_49/administration/guide/b\\_AnyConnect\\_Administrator\\_Guide\\_4-9/anyconnect-profile-editor.html](https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect_49/administration/guide/b_AnyConnect_Administrator_Guide_4-9/anyconnect-profile-editor.html)

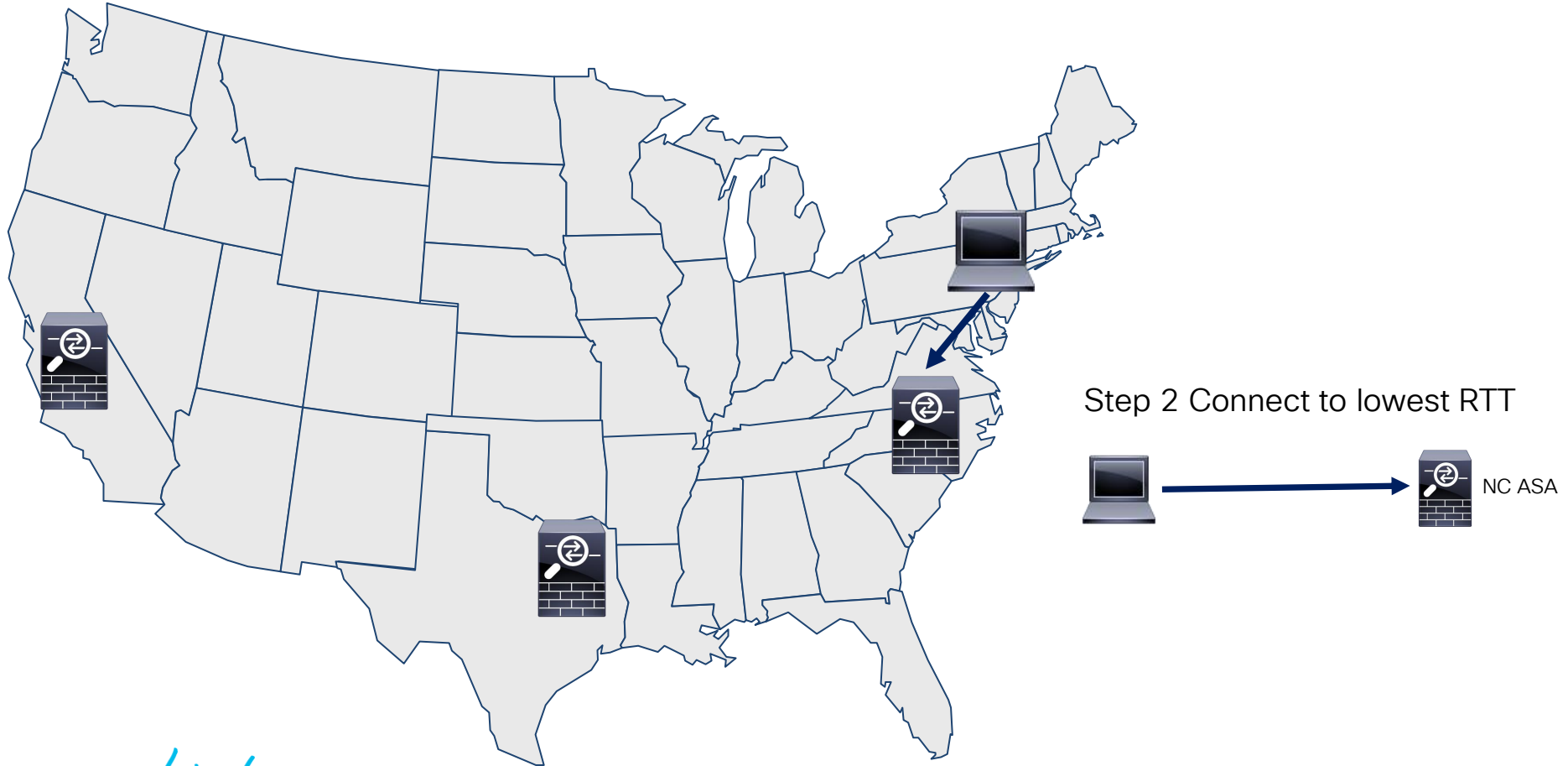


For Your  
Reference

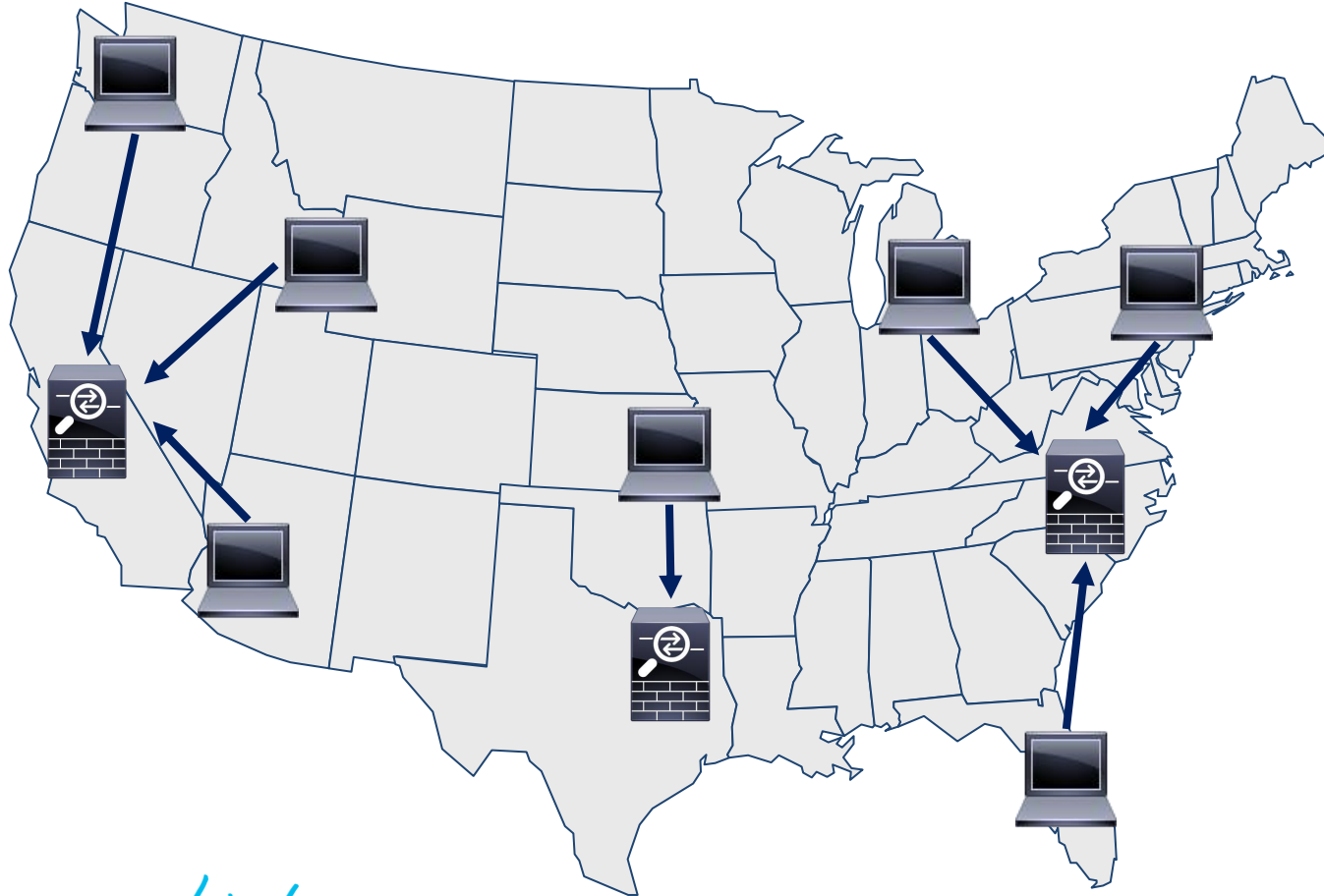
# Optimal Gateway Selection



# Optimal Gateway Selection



# Optimal Gateway Selection



# More on Optimal Gateway Selection

Information, troubleshooting, and FAQ

<https://community.cisco.com/t5/security-documents/anyconnect-optimal-gateway-selection-operation/ta-p/3124296>

Additional Troubleshooting

<https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/116721-technote-ogs-00.html>



For Your  
Reference

# Another Deployment Type: DNS

All AnyConnect clients connect to the same FQDN.

- DNS Server performs round robin assignment.
- DNS Servers in different geographical locations provide IP address of ASA in that region for the same FQDN.

Management and control completely removed from ASA/AnyConnect.



For Your  
Reference



# Maximizing the Performance

# Full Tunnel



Webex Meetings

# Split Tunnel



# More on AnyConnect Split Tunnel

Implementing Split Tunnel for Cisco AnyConnect to Improve Performance

DGTL-TSCSEC-509



For Your  
Reference

# End Point Security

Posture – Endpoint compliance

Umbrella – DNS Security

AMP – Malware protection

NVM – Visibility

... and more



# More on AnyConnect Security Modules

## Endpoint Security, Your Last Line of Defense

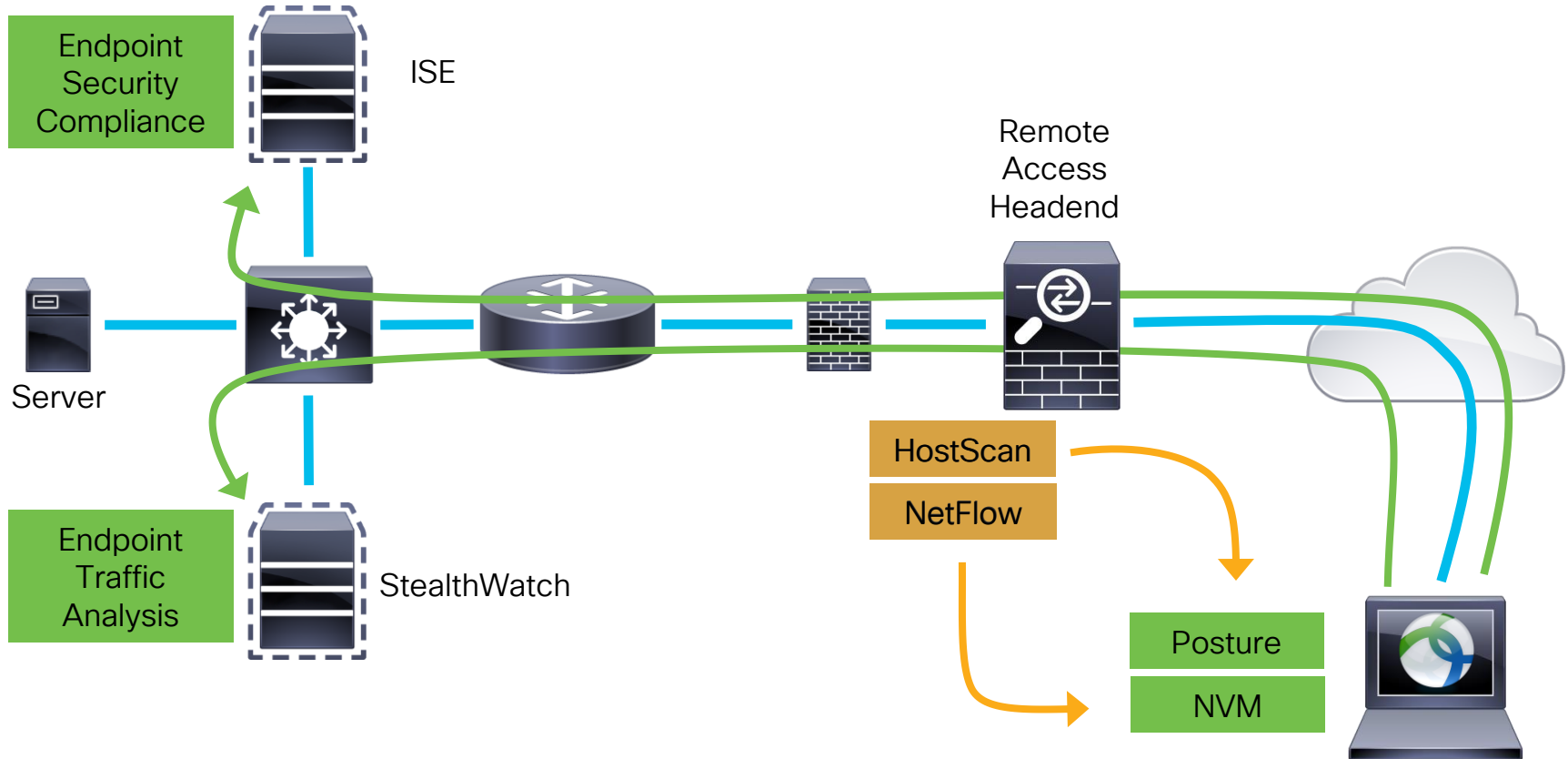
BRKSEC-3446

DGTL-BRKSEC-3446



For Your  
Reference

# Optimize Configuration



# More on ISE and AnyConnect Deployment

Deploying AnyConnect on Firepower Threat Defense with Posture and MFA

DGTL-BRKSEC-2003



For Your  
Reference



# Fine Tuning

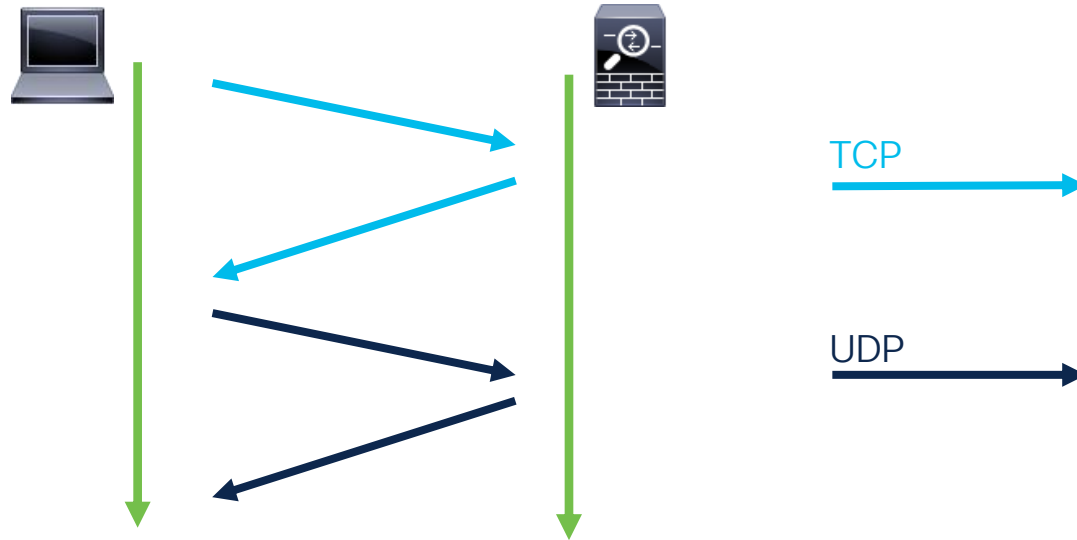


# AnyConnect Protocols

- 3 Supported Protocols
  - DTLS
  - TLS
  - IPsec-IKEv2

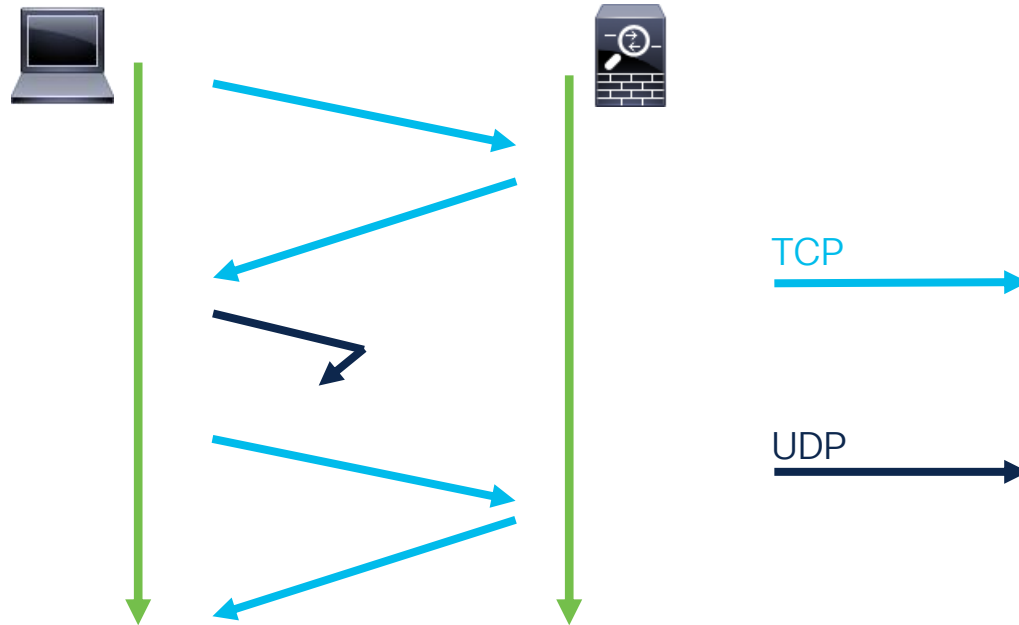
# AnyConnect Protocol - DTLS

- UDP based TLS
- Initial handshake uses TCP, switch to UDP during connection process



# AnyConnect Protocol - DTLS

- Switch to UDP fails? Continue to use TCP for TLS.



# AnyConnect Protocol - DTLS

- DTLS v1.2 implemented in AnyConnect 4.7 and ASA 9.10

```
ASAv# show vpn-sessiondb detail anyconnect filter name CiscoLiveUser

Username      : CiscoLiveUser          Index      : 983
Assigned IP   : 10.0.0.1              Public IP   : 192.168.1.1
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384

...

DTLS-Tunnel:
Tunnel ID     : 983.3
Assigned IP   : 10.0.0.1              Public IP   : 192.168.1.1
Encryption    : AES-GCM-256           Hashing     : SHA384
Ciphersuite   : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2              UDP Src Port : 50478
UDP Dst Port  : 443                  Auth Mode   : Certificate
```

AES-GCM  
added  
in DTLSv1.2

Shows the exact protocol and version client is using

# AnyConnect Protocol – IPsec-IKEv2

- AnyConnect IPsec uses IKEv2 for key management and authentication.
- For throughput performance, IPsec is better than DTLS or TLS.
- IPsec does require some additional overhead management (AnyConnect VPN profile).
- IPsec is a Layer 3 tunneling protocol, while DTLS and TLS are Layer 4 tunneling protocols.
- AnyConnect will use NAT-T IPsec, ESP packet will be encapsulated in a UDP header.



For Your  
Reference

# AnyConnect Protocol – IPsec-IKEv2

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) Corporate\_VPN

FQDN or IP Address User Group

vpn.mycompany.com /

Connection Information

Primary Protocol IPsec

☒ ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

- IPsec must be enabled in the AnyConnect VPN XML profile deployed to user computer
- Profile is either pre-deployed, or the user can first connect with SSL to obtain this profile.



For Your  
Reference

# Crypto Engine Bias

## Possible Settings:

- IPsec
- SSL (TLS and DTLS)
- Balanced

## Supported on:

- ASA 5545/5555/5585
- FPR 4100\* and 9300\*



# Crypto Engine Bias Notes

\*Currently not supported on newer models of FPR 4100 (4115/4125/4145) or FPR 9300 with module SM-40/48/56, although an enhancement has been filed.

## More Information

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa914/configuration/vpn/asa-914-vpn-config/vpn-params.html?bookSearch=true#ID-2443-00000319>



For Your  
Reference



# Single Client Optimization

## Problem:

Individual user not able to achieve high throughput (100 Mbps+) when connected with AnyConnect.

- TunnelOptimization introduced in AnyConnect 4.7 and ASA 9.10(1) – manual configuration.
- Increases throughput limitation on the AnyConnect client application.
- Enabled by default in AnyConnect 4.9 – manual configuration no longer needed.

# TunnelOptimization Configuration

Manual configuration for AnyConnect v4.7 and v4.8:

```
webvpn
```

```
    anyconnect-custom-attr TunnelOptimizationsEnabled description Optimizations Enabled
```

```
anyconnect-custom-data TunnelOptimizationsEnabled False false
```

```
anyconnect-custom-data TunnelOptimizationsEnabled True true
```

```
group-policy <GP-Name> attributes
```

```
    anyconnect-custom TunnelOptimizationsEnabled value True
```



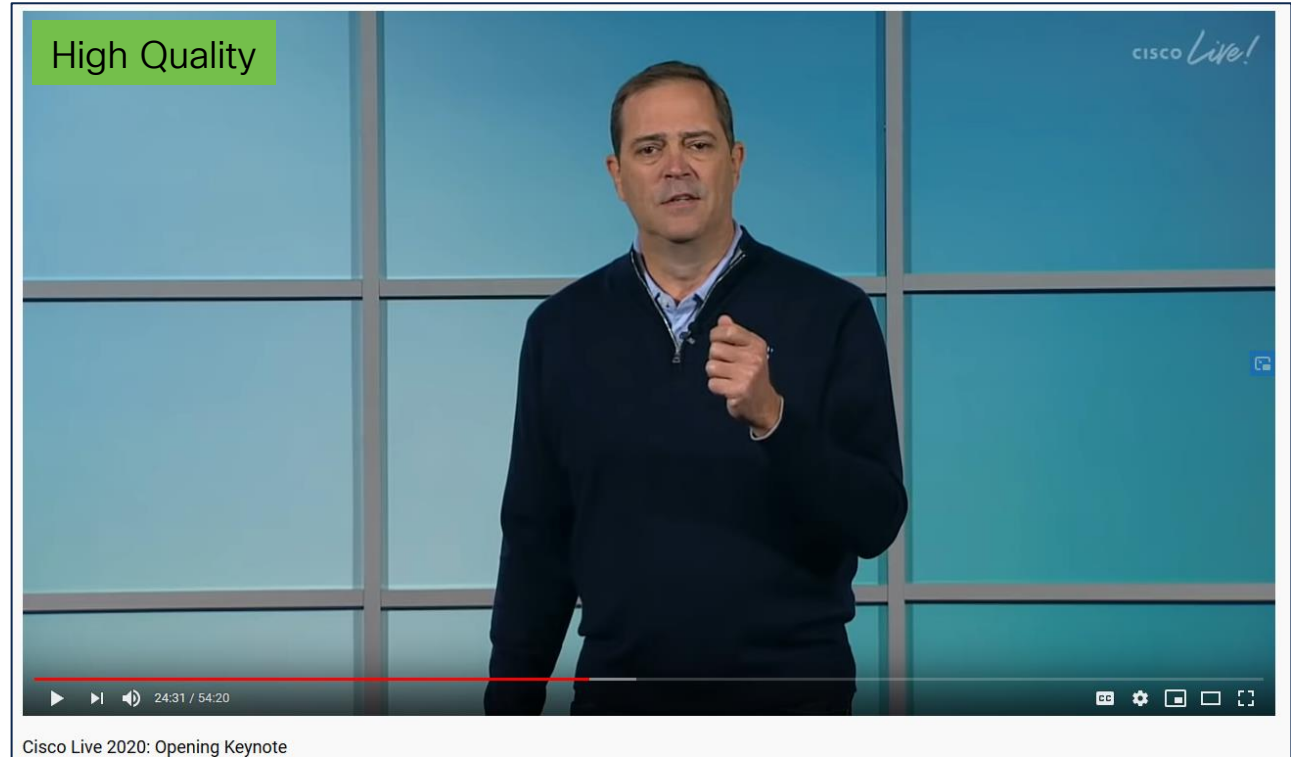
For Your  
Reference

# Conclusion

# What's next?

- Follow up with additional information in the PDF.
- Check out other DGTL-BRKSEC and DGTL-TSCSEC videos:
  - Advanced ASA troubleshooting
  - ISE
  - Umbrella
  - Endpoint Security

# Summary



# Additional AnyConnect Resources

## Tips on Scaling out AnyConnect Deployment

<https://community.cisco.com/t5/security-documents/asa-best-practices-for-remote-access-vpn-performance/ta-p/4070579#toc-hld--135850061>

<https://community.cisco.com/t5/security-documents/episode-57-maximizing-anyconnect-performance-during-the-covid-19/ta-p/4053676>

[https://www.cisco.com/c/en/us/td/docs/security/asa/misc/anyconnect-faq/anyconnect-faq.html#Cisco\\_Reference.dita\\_5b933072-bfc6-49bd-a3ad-cea44703fe15](https://www.cisco.com/c/en/us/td/docs/security/asa/misc/anyconnect-faq/anyconnect-faq.html#Cisco_Reference.dita_5b933072-bfc6-49bd-a3ad-cea44703fe15)

<https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/215331-anyconnect-implementation-and-performanc.html#anc8>



For Your  
Reference



Thank you



# Possibilities

#CiscoLive