



VPN - Routing and Remote Access



Obtaining a Certificate for K12.AR.US

- 1. You will need to get an A record created for the school for something.k12.ar.us through the UNIX Group.
- 2. You will need a 1-1 NAT to the VPN Server and open port 443. If you are going to setup L2TP for Mac OS and Chromebooks then you will need ports 50, 51, 500, 1701, 4500 on TCP and UDP open also.
- 3. Create a child incident for Arkansas .GOV Approvals Group
- 4. Request a SSL Certificate for the school A record.
- 5. Send an e-mail to DIS.Security.Architecture@arkansas.gov with the CSR info. (Direction to create CSR further down)
- 6. You will get an e-mail from Certificate Services Manager support@cert-manager.com with the links to download the Certificate. (Forward to the tech in case they need it later on.)
- 7. If the school is getting the certificate from another Signing Authority (Go-Daddy, Digicert, etc...) the directions should work for those too.

Example of ASA Rule: Put the Public and Private IP for your school: object network VPN_SVR_Public host 170.211.xxx.xxx object network VPN SVR Private host 10.xxx.xxx.xxx This creates a service group of the allowed ports: object-group service VPN_access_svcs service-object tcp destination eq 1701 service-object tcp destination eq pptp service-object tcp destination eq https service-object tcp destination eq 47 service-object tcp destination eq 51 service-object tcp destination eq 50 service-object tcp destination eq 500 service-object tcp destination eq 4500 service-object udp destination eq 51 service-object udp destination eq 50 service-object udp destination eq isakmp service-object udp destination eq 4500 service-object udp destination eq 1701 service-object tcp destination eq www service-object udp destination eq 443 service-object udp destination eq www

This uses the service group to allow access:

access-list acl-out extended permit object-group VPN_access_svcs any object VPN_SVR_Private

Install the RRAS Role

Step 1

Add the Remote Access role. Server Manage -> Manage -> Add Roles and Features -> Remote Access.

Select server ro		DESTINATION SERVER vpn.base.local
Before You Begin Installation Type Server Selection	Select one or more roles to install on the selected server. Roles Active Directory Certificate Services	Description Remote Access provides seamless
Server Roles Features Remote Access	Active Directory Domain Services Active Directory Federation Services Active Directory Lindtweight Directory Services	VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS
Role Services Confirmation	Active Directory Eight Management Services Application Server	provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Provy enables the
	UHCP Server DNS Server Fax Server Fax Server File and Storage Services (1 of 12 installed) Hyper-V	publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other
	Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services	connectivity options. RAS and Routing can be deployed in single- tenant or multi-tenant mode.

Step 2

Click Next a couple times, then just click **DirectAccess and VPN**. Click Add Features. We are not setting up DirectAccess at this time. There is a separate document for that.

b	Add Roles and Features Wizard	
Select role service	S	DESTINATION SERVER vpn.base.local
Before You Begin	Select the role services to install for Remote Access	
Installation Type	Role services	Description
Server Selection	DirectAccess and VPN (RAS)	DirectAccess gives users the
Server Roles	Routing	experience of being seamlessly connected to their corporate network
Features	Web Application Proxy	any time they have Internet access.
Remote Access		with DirectAccess, mobile computers can be managed any time the
Role Services		computer has Internet connectivity,
Web Server Role (IIS)		date with security and system health
		policies. VPN uses the connectivity of the Internet plus a combination of
Results		tunnelling and data encryption
		clients and remote offices.
	< <u>P</u> revious <u>N</u>	ext >Install Cancel

Next a couple times. It will install IIS, Click Next on IIS and IIS Role Services. Go ahead and click Install.

a	Add Roles and Features Wizard	_ 0	х
Installation progre	255	DESTINATION SER vpn.base.	RVER local
Before You Begin	View installation progress		
Installation Type	1 Starting installation		
Server Selection			
Server Roles			
Features	Group Policy Management		^
Remote Access	RAS Connection Manager Administration Kit (CMAK)		
Role Services	Remote Access		≡
Web Server Role (IIS)	DirectAccess and VPN (KAS)		
Role Services	Role Administration Tools		
Confirmation	Remote Access Management Tools		
Results	Remote Access GUI and Command-Line Tools		
	Remote Access module for Windows PowerShell		
	Web Server (IIS)		
	Wanagement 100is		~
	You can close this wizard without interrupting running tasks. View task progress again by clicking Notifications in the command bar, and then Task Details. Export configuration settings	; or open this p	age
	< Previous Next >	I Canc	el

Before we can continue with the RRAS setup we need to create the CSR and complete the certificate request. We are going to use IIS to complete the certificate, so we are going to wait on the configuration and finish the RRAS setup later.

Using IIS 10 to Create Your CSR

- 1. In the Windows start menu, type Internet Information Services (IIS) Manager and open it.
- 2. In **Internet Information Services (IIS) Manager**, in the **Connections** menu tree (left pane), locate and click the server name.

Internet Information Services (IIS) Manager	- 🗆 X
- → ¶i + SERVER +	🖬 🖄 🚱 🔞
File View Help	
onnections	Actions
SERVER HOITIE	Open Feature
Start Page Filter: • 🐨 Go - 🖳 Show All Group by: Area • 📰 •	Manage Server
ASP.NET	A Restart
📄 🛓 😓 🌒 👰 🕞 🖍 🎼 🧱	Stop
.NET .NET INET Error .NET .NET Trust Application Connection Machine Key Pages and Providers	View Application Pools
Authorizat Compilation Pages Globalization Levels Settings Strings Controls	View Sites
	Get New Web Platform Components
Session State SMTP E-mail	Help
· · · · · · · · · · · · · · · · · · ·	
ASP Authentic CGI Compression Default Directory Error Pages Failed FastCGI Handler Document Browsing Request Tra Settings Mappings	
🗈 🔮 🖫 🌢 📗 🌬 🛃 😰 😭	
HTTP HTTP ISAPI and ISAPI Filters Logging MIME Types Modules Output Request Server	
Redirect Respon CGI Restri Caching Filtering Certificates	
Worker	
Processes	v
Features View 💦 Content View	
ady	•

- 3. On the server name **Home** page (center pane), in the **IIS** section, double-click **Server Certificates**.
- 4. On the **Server Certificates** page (center pane), in the **Actions** menu (right pane), click the **Create Certificate Request...** link.

💐 Internet Information Services (IIS) N	Manager							- 🗆 X
← → € SERVER →								📴 🖂 🏠 🔞 •
File View Help								
Connections	Convertifier						Actions	
😪 - 🔒 🖄 🕵	Server Certificates							
Start Page	Use this feature to request and m	Create	Certificate Request					
Application Pools	Filter:							zte Certificate Request
> 📓 Sites	Name Issued Issued By Expiration Date Certificate Continues		Create	Domain Certificate				
	WMSVC-SHA2	WMS	WMSvc-SHA2-WIN-10U475M	9/26/2026 8:28:45	6F2CCAA	Personal	Create Self	Self-Signed Certificate
						Enable Renewe	Automatic Rebind of ed Certificate	
							Hep	
Ready	terre terr							Q

5. In the **Request Certificate** wizard, on the **Distinguished Name Properties** page, provide the information specified below and then click **Next**:

Common name:	Type the fully-qualified domain name (FQDN) (e.g., www.example.com).
Organization:	Type your company's legally registered name (e.g., YourCompany, Inc.).
Organizational unit:	The name of your department within the organization. Frequently this entry will be listed as "IT", "Web Security," or is simply left blank.
City/locality:	Type the city where your company is legally located.
State/province:	Type the state/province where your company is legally located.
Country:	In the drop-down list, select the country where your company is legally located.

?

×

Request Certificate

			5	11
				414
	11			11
	- 0			\mathbf{P}
	- 66	л.	ч.	

Distinguished Name Properties

ommon name:	www.yourdomain.com	
rganization:	Your Company, Inc.	
rganizational unit:	IT	
ity/locality	Lehi	
ate/province:	UT	
ountry/region:	US	~
	L	

6. On the **Cryptographic Service Provider Properties** page, provide the information below and then click **Next**.

Cryptographic	In the drop-down list, select Microsoft RSA SChannel Cryp Provider,	otogra	phic
service provider:	unless you have a specific cryptographic provider.		
Bit length:	In the drop-down list select 2048 , unless you have a speci for opting for larger bit length.	fic rea	son
Certificate		?	×

Request Certificate

P	Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic ser	vice provider:				
Microsoft RSA SC	hannel Cryptograph	ic Provider	~		
Bit length:					
2048	~				
		Previous	Next	Finish	Cancel

7. On the **File Name** page, under **Specify a file name for the certificate request**, click the ... box to browse to a location where you want to save your CSR.

Note: Remember the filename that you choose and the location to which you save your csr.txt file. If you just enter a filename without browsing to a location, your CSR will end up in C:\Windows\System32.

Request Certificate	?	\times
File Name		
Specify the file name for the certificate request. This information can be sent to a certification authority for signing. Specify a file name for the certificate request:		
C:\Users\Administrator\Desktop\csr.txt		
Previous Next Finish	Cancel	

- 8. When you are done, click **Finish**.
- Use a text editor (such as Notepad) to open the file. Then, copy the text, including the ----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST----- tags,
 and this is what you will send to Security Architecture or paste in a third party order form.



22. When you get the email from Certificate Service Manager, download the file as **X509 Certificate only**, **Base64 encoded** and save on the server.

How to install your SSL certificate and configure the server to use it

Install Your SSL Certificate

- 1. From the Administrative Tools, find Internet Information Services (IIS) Manager and open it.
- 2. In the **Connections** pane, locate and click the **server**.
- 3. In the server Home page (center pane) under the IIS section, double-click Server Certificates.

8		Interr	net Informa	ation Service	s (IIS) Man	ager		_	D X	
🛞 🔋 🖌 WIN-C	93AKUOJKPD	•						5 🛛	🔄 I 🕐 ·	•
<u>F</u> ile <u>V</u> iew <u>H</u> elp										
Connections				Llama			Ac	tions		
😪 - 🔒 🖄 🥵		N-C93AK	JOJKPD	Home				Open Feature		
Start Page Image Image	Filter:		• 🦉 <u>G</u> o - (Show <u>A</u> ll	Group by:	Ŧ		Manage Server		
		A	4					Start		
		Y	Ø		404	8		Stop		
	Authentic	Compression	Default Document	Directory Browsing	Error Pages	Failed Request Tra		View Application Po View Sites	ols	
	2			1	-	<u>ě</u>		Change .NET Frame Version	work	-
	Handler Mappings	Redirect	Respon	and Doma	CGI Restri	ISAPI Filters	0	Get New Web Platfo Components	rm	_
		j 12			e	P	0	Help Online Unio		
	Logging	MIME Types	Modules	Output Caching	Request Filtering	Server Certificates		Unline Help		
	2									
	Worker									
	Manage									
	ivianageme	illes	(a	(a)						
			N.W.	N.M.	1111 Ŷ					
< III >	Features Vie	ew 🕂 Content	t View							
Ready									•	

4. In the Actions menu (right pane), click **Complete Certificate Request**.

8]	🖣 Internet Information Services (IIS) Manager 📃 🗖 🗙			
€ WIN-C	93AKUOJKPD 🕨			🖸 🛛 🔂 🕡 🕶
<u>F</u> ile <u>V</u> iew <u>H</u> elp				
Connections	Server Certification Use this feature to request and m websites configured for SSL. Filter:	ates nanage certificates that the Web se I sound To I sound To	erver can use with F	Actions Import Create Certificate Request Complete Certificate Request Create Domain Certificate Create Self-Signed Certificate Help Online Help
< III > Ready	< الله Features View من Content View	EW	2	Qa.:
кеаду				*1 .:

5. In the Complete Certificate Request wizard, on the Specify Certificate Authority Response page, provide the following information:

File name containing the certificate authority's response:	Click the button to locate the .crt file you received from Certificate Service Manager.
Friendly name:	Type a friendly name for the certificate. This is not part of the certificate; instead, it is used to identify the certificate. I would use the domain name.
Select a certificate store for the new certificate:	In the drop-down list, select Personal.

Complete Certificate Request ? ×
Specify Certificate Authority Response
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.
File name containing the certification authority's response:
C:\Users\Administrator\Desktop\your_domain_name.cer
Friendly name:
yourdomain.com
Select a certificate store for the new certificate:
OK Cancel

- 6. Click OK to install the certificate.
- 7. Check that it completed and kept the certificate in IIS by clicking the refresh button or going out of Server Certificates and back in. If your certificate doesn't show in the list you may need to do a repair on the certificate store (See Below). Now that you've successfully installed your SSL certificate, you need to configure your site to use it.

Commands for certificate store repair only needed if cert doesn't show in the server cert list in IIS: This command will give you a list of certificates installed and their Thumbprint: Get-ChildItem -path cert:\LocalMachine\My

This command uses the ThumbprintNumber for your certificate to repair the store. Your certificate should show in the server certificate list in IIS after the command completes successfully. If it fails then you will have to troubleshoot why:

certutil -repairstore my "ThumbprintNumber"

Assign Your SSL Certificate

- 8. In **Internet Information Services (IIS) Manager**, in the Connections pane, expand the name of the server on which the certificate was installed. Then expand Sites and click the site you want to secure using the SSL certificate.
- 9. In the Actions menu (right pane), click **Bindings**.



10. In the Site Bindings window, click Add.

			Site Bir	ndings	? X
Type	Host Name	Port	IP Address	Binding Informa	 Add
http		80	*		Edit
					Remove
					Browse
					Close

11. In the Add Site Binding window, do the following and then click OK.

Туре:	In the drop-down list, select https.
IP address:	In the drop-down list, select the IP address of the site or select All Unassigned.
Port:	Type 443. (SSL uses port 443 to secure traffic.)

SSL certificate: In the drop-down list, select your new SSL certificate (e.g., yourdomain.com).

Add Site Bind	ling ? ×
Type: IP address: https V All Unassigned	Port:
Host name:	
SSL certificate:	
yourdomain.com	Select View
	OK Cancel

12. Your SSL certificate is now installed, and the website is configured to accept secure connections. The certificate will now show in RRAS server configuration.

Configure RRAS

Step 4

Once the SSL Certificate has been installed, click the flag thing at the top of Server Manager, and then **Open the Getting Started Wizard**.

a	Server	Manager		_ 0 ×
🗲 🕘 🕌 애 Dashb	oard	• 🕲	Manage To	pols View Help
 i Dashboard i Local Server ii All Servers iii File and Storage Services ▷ iii IIS iii Remote Access 	Post-deployment Confi Configuration required (RAS) at VPN Open the Getting Starte Configuration required. vpn.base.local. Add Roles and Features Task Details LEARN MORE ROLES AND SERVER G Roles: 3 Server groups: File and Stora Services	gura TASKS for DirectAccess and VPM ed Wizard Installation succeeded o 5 Connec ROUPS 1 Servers total: 1 ge 1	s local se s local se rvers to ma er group t this server to clo	rver = nage oud services Hide

Step 5

Select Deploy VPN Only.



If clicking the Open Getting Started Wizard doesn't open, you can go to Administrative Tools and Open Routing and Remote Access. Once the new window pops up, right click your server name (mine is VPN (local)) then **Configure and Enable Routing and Remote Access**.

F	Server Manager	- Č	j x	
€∋∙	Routing and Remote Access		Help	
	File Action View Help			^
🔛 Dashboar				
Local Serv	Routing and Remote Access Routing and Remote Access			
All Server		~		
File and S	Configure and Enable Routing and Remote Access s secure remote access to			≡
	Disable Routing and Remote Access			
Remote A	All Tasks bothgure the following:			
in the second second	Delete ateway.			
	Refresh			
	Properties .			
	Help			
	A pasic tirewail.		s	
	To add a Routing and Remote Access server, on the Action menu, click Add Server.			
		Ē		
		Ť		
	Configures Routing and Remote Access for the selected server			
· ·				
	File and Storage 1 IIS	1		
		-		~

Step 7

We're trying to keep our surface area as small as possible, so click on **Custom Configuration**.



Next, only check **VPN Access**. Click **Next** and **Finish**. If the Windows Firewall is on, you may get a popup that you need to enable Routing and Remote Access, but the only exception needed is Secure Socket Tunneling Protocol (SSTP-In).



Step 9

The RRAS Service will configure itself, and start the service. It may popup an option to start the service. Click **Start**. *If the service doesn't start it is likely due to IPV6 being disabled in the registry and you will have to remove the Disabled Component entry that we normally configure*. You will then be returned to the RRAS config window. Right click your server name, then **Properties**.



Check that your SSL Certificate binding is the newly installed certificate.

2	VPN (local) Properties ? X	
Windows PowerShell Copyright (C) PS C:\Users\a	General Security IPv4 IPv6 IKEv2 PPP Logging	_ _ X
File Action Vie	The Authentication provider validates credentials for remote access clients and demand dial routers. Authentication provider: Windows Authentication Configure	
◆	Authentication Methods The accounting provider maintains a log of connection requests and	s ^
	sessions. Accounting provider:	ving:
> ☐ Trusted f > ☐ IPv4 > ☐ Enterpris > ☐ IPv6 > ☐ Intermed > ☐ IPv6 > ☐ Trusted f > ☐ Intermed > ☐ Trusted f > ☐ Intermed > ☐ Trusted F > ☐ Intermed > ☐ Trusted F > ☐ Intermed	Windows Accounting	
 ▷ Client Au ▷ Other Pe ▷ Remote I 	Preshared <u>K</u> ey: SSL Certificate Binding: Use H <u>I</u> TP	ction menu,
Certificat Smart Ca Smart Ca Trusted I Done Web Hos	Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener) Certificate:	
<		

Step 11

Next, click on IPv4. Here, you can either do a DHCP forwarding or just give RRAS a few IP addresses to hand out. Click Apply then Okay. You'll be returned again to the RRAS window.

🚇 l ⊋ 🚯 = l	VPN (local) Properties ? X	_ 🗆 X
File Home Chare View	General Security IPv4 IPv6 IKEv2 PPP Logging IPv6 IKEv2 PPP Logging Image IPv4 Forwarding Image IPv4 Image IPv	- C X P
Arvorites Favorites Favorites Posktor Desktor Downlo Dewnlo Recent Ports Ports Ports Ports Ports Ports Ports Ports Ports Remote, Network P IPv4	IPv4 address assignment This server can assign IPv4 addresses by using:	KB KB kccess to king:
▶ 真 IPv6 < Ⅲ Done	Add Edt Remove ✓ Enable broadgast name resolution Use the following adapter to obtain DHCP, DNS, and WINS addresses for dial-up clients. Adagter: Allow RAS to select adapter	uction menu,
4 items		

At this point, your RRAS server is setup!

If you don't want to give permission individually to each user that will need VPN access I suggest going through the next section. You will create a VPN group in AD and use it to allow VPN access.

Setup Network Policy Server

Step 1

Once you've returned to the RRAS window, *left-click* **Remote Access Logging and Policies**. Then right-click and **Launch NPS**.

-	vpn - Remote Desktop Connection – 🗖 🗙
<u>9</u>	Routing and Remote Access
File Action View Help	
🗢 🔿 🙍 🖬 🙆 👘	
Image: Server Status Image: Server Status <th>Remote Access Logging & Policies To configure remote access logging or network policies (formerly named remote access policies), right-click the Remote Access Logging and Policies node. For more information about setting up a Network Policy Server (NPS), or about deploying and troubleshooting remote access network policies, see <u>NPS Help</u>. To remotely configure Internet Authentication Service (IAS) for prior Windows versions such as two Server 2003, see Terminal Server Help.</th>	Remote Access Logging & Policies To configure remote access logging or network policies (formerly named remote access policies), right-click the Remote Access Logging and Policies node. For more information about setting up a Network Policy Server (NPS), or about deploying and troubleshooting remote access network policies, see <u>NPS Help</u> . To remotely configure Internet Authentication Service (IAS) for prior Windows versions such as two Server 2003, see Terminal Server Help.
Launch NPS	

Step 2

A new Network Policy Server window will pop-up. Here, we can set which users can access the VPN, set the type of authentication encryption, and restrict network access.



We'll start by creating a new Network Policy. Right click **Network Policy** and click **New**.

ø			Network Policy Server			_ 0	X	
<u>File</u> <u>A</u> ction	<u>V</u> iew <u>H</u> elp							
🗢 🔿 🙍	•							
NPS (Local)	ing	Network Policies	allow you to designate who is authorized t	to connect t	to the network and t	he circumstance	s	-
IP Fi	New	under which they	can or cannot connect.					
	View	licy Name	A Duties and Danuals Assessments	Status	Processing Order	Access Type	So	
	Refresh	Connections to Microso	off Routing and Remote Access server ccess servers	Enabled	999999	Deny Access Deny Access	Un Un	
	Help	_						
		Conditions If the follow	ing and diana any mate					^
		Condition	Ing conditions are met:					=
		Settings - Then the follo	wing settings are applied:					
		Setting	Value					~
		<	III				>	

Step 4

Name your Policy, and select **Remote Access Server (VPN/Dial-up)**.

	New Network Policy	x
File A	Specify Network Policy Name and Connection Type You can specify a name for your network policy and the type of connections to which the policy is applied.	
	Policy name: VPN Policy Very Policy Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.	s S U U
	Type of network access gerver: Remote Access Server(VPN-Dial up) Vendor specific: 10	
Action:	Previous Next Enish Cancel	>

Leave this window for a moment, go into AD Users and Computers, create a Group and name it VPN Access or whatever you wish, and add some users. Come back, and add that Windows Group by clicking **Add** -> **Windows Group**.



Step 6

Confirm and click Next

	New Network Policy	x
File A	Specify Conditions Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.	
	Conditions:	
	Condition Value	
	Windows Groups BASE/VPN Group	S U U
	Condition description: The Windows Groups condition specifies that the connection user or computer must belong to one of the selected omune	
	Agd Edit Remove	
Action:	Previous Next Enish Cancel	>

Grant this group access.

I	New Network Policy	x
File A	Specify Access Permission Configure whether you want to grant network access or deny network access if the connection request matches this policy.	
	 Access granted Grant access if client connection attempts match the conditions of this policy. Access denied Deny access if client connection attempts match the conditions of this policy. 	S U U
	Access is determined by User Dial-in properties (which override NPS policy) Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.	
Action:	Previous Next Enish Cancel	× >

Step 8

Here, you can choose your Authentication Encryption. I disabled all the weaker ones, and only enabled the stronger **Microsoft: Secured Password (EAP-MSCHAP v2)**.

()	New Network Policy	x
File A	Configure Authentication Methods Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.	35
	EAP types are negotiated between NPS and the client in the order in which they are listed.	S
	Microsoft: Secured password (EAP-MSCHAP v2) Move Up Move Down	U U
	Add Edit Remove	^
	Less secure authentication methods:	=
	Unercypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method. Perform machine health check only	
Action:	Previous Next Enish Cancel	>

Here you can set some restrictions if you like. (Optional) Click Next.

		New Network Policy	×
File A	Configure Co Constraints are addi constraint is not mat if you do not want to	nstraints tional parameters of the network policy that are required to match the connection request. If a ched by the connection request, NPS automatically rejects the request. Constraints are optional; configure constraints, click Next.	es
	Configure the constraints for this network of all constraints are not matched by the Constraints :	rk policy. e connection request, network access is denied.	S U
	Constraints	Specify the maximum time in minutes that the server can remain idle before the connection is disconnected	U
	Session Inneout	<u>Disconnect atter the maximum idle time</u>	
	SINCONS NAS Port Type		
			=
			~
Action:		Previous Next Enish Cancel	

Step 10

Click on IP Filter.

•	New Network Policy	x
File A	Configure Settings NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.	
	Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied.	s
	RADIUS Attributes Standard Vendor Specific Vendor Specific	U U
	Houting and Hende IPv4 Access To control the IPv4 packets this interface sends, click input Filters Multilink and Bandwidth Allocation Protocol (BAP) To control the IPv4 packets this interface receives, click Output Filters IP Filters To control the IPv4 packets this interface receives, click Output Filters	
	IP Settings IPv6 To control the IPv6 packets this interface sends, click Input Filters. Input Filters To control the IPv6 packets this interface receives, click Output Filters	=
Action:	Previous Next Enish Cancel	~

Specify a Filter. I set mine to only allow access to my lab's subnet.

I			New Net	work Policy			x	x
File A	NPS app matched	igure Sett blies settings to d.	ings the connection request i	f all of the network poli	icy conditions and constra	ints for the po	icy are	
	Configure the set f conditions and Settings: RADIUS Attr Saturdard Standard Vendor Sr Bouting and Access Multiink a Bandwidt Pf Rers Multiink a Bandwidt Pf Rers Provention Pf Refs Pf Pf Refs Pf Refs Pf Refs Pf Refs Pf Refs Pf Refs Pf Pf	se filters control v r action: Dg not permit parc Permit only the pa rs: surce Address ser's address	Inbour which packets are forward ackets listed below ackets listed below Source Network Mask User's mask	Destination Address 172.16.0.0	P Z S Z	> S PS		35 S U U E
Action:				<u>Previous</u>	K Cancel	ars	~	×

Step 12

Click OK, next, and you're done setting up NPS!

There's more you can filter by, but this is the basics. You can also configure the Network Policy Server which can lock down your network so that only clients with Firewalls enabled and AVs installed will be allowed to connect.

		Network Policy Server			- 4) X
<u>File Action View H</u> elp						
🧇 🏟 🞽 📊 👔 🖬						
NPS (Local)	Network Policies					
Accounting Petwork Policies IP Filters	Network polici under which th	es allow you to designate who is authorized rey can or cannot connect.	to connect t	to the network and t	he circumstan	ces
	Policy Name		Status	Processing Order	Access Type	S
	VPN Policy		Enabled	1	Grant Acce.	. R
	Connections to Mici	rosoft Routing and Remote Access server	Enabled	999998	Deny Acces	s U
	Connections to othe	er access servers	Enabled	999999	Deny Acces	s U
	Conditions - If the foll	owing conditions are met:				<u>^</u>
	Settings - Then the fi	ollowing settings are applied:				=
1	Setting	Value				
	4					~
	<	ш				>

Setup L2TP for Mac OS and Chromebook

If you are going to enable L2TP for Mac OS and Chromebook access then you need to create a second Network Policy with these additions. On the Properties of the Routing Remote Access Server, click the box for Allow custom IPsec policy for L2TP/IKEv2 connection and enter a Preshared Key. I would suggest a key that is long and complex. The more simple the key, the more easy it can be hacked.

ASD-VPN	l (local) Pr	opertie	s				?	\times
General	Security	IPv4	IPv6	IKEv2	PPP	Logging		
The Aur and der Authent Windo	thentication mand-dial re tication pro ws Authen	n provide outers. vider: tication	er validate	es creden	tials for re	emote acc	ess clien hfigure	ts
Auth	entication	Methods						
The acc sessions	counting pros.	ovider m	aintains a	log of co	onnection	requests	and	
Accourt	ting provid	er:				-		
Windo	ws Accour	iting			-	Cor	nfigure	
The cus connect set this certifica	stom IPsec tions. The option. IKE ite will not t w custom I	policy s Routing 22 initiat be able t Psec po	pecifies a and Rem tors confi o connec licy for L2	preshare ote Acce gured to a t. 2TP/IKEv	ed key for ss servic authentic 2 connec	L2TP/IKE e should b ate this se	Ev2 e started rver usin	l to g
Presha	red Key:							_
SSLO	Certificate E	Binding: -						- I
F U	se HTTP							
Selec	t the certifi r should us	cate the e to bind	Secure S with SS	Socket Tu L (Web Li	unneling l istener)	Protocol (S	STP)	
Certifi	cate: as	d-vpn.k	12.ar.us		-	View	'	
			(ж	Can	icel	Appl	y

Next follow steps 1-6 of Network Policy Setup, to setup a second Network Policy named L2TP.

Select condition	x
Select a condition, and then click Add.	
Authentication Type The Authentication Type condition specifies the authentication methods required to match this policy.	^
Allowed EAP Types The Allowed EAP Types condition specifies the EAP types required for client computer authentication method configuration to match this policy. Use of this condition requires that EAP is also configured in connection request policy.	
Framed Protocol The Framed Protocol condition restricts the policy to only clients specifying a certain framing protocol for incoming packets, such as PPP or SLIP.	=
Service Type The Service Type condition restricts the policy to only clients specifying a certain type of service, such as Telnet or Point to Point Protocol connections.	
Tunnel Type The Tunnel Type condition restricts the policy to only clients that create a specific type of tunnel, such as PPTP or L2TP.	
RADIUS Client Properties	
Callino Station ID	\mathbf{r}
Add Cancel	

Click Add. Select Tunnel Type and Add.

Tunnel Type
Specify the tunnel types to required to match this policy.
Common dial-up and VPN tunnel types
Generic Route Encapsulation (GRE) IP Encapsulating Security Payload in the Tunnel-mode (ESP) ✓ Layer Two Tunneling Protocol (L2TP)
Point-to-Point Tunneling Protocol (PPTP)
Secure Socket Tunneling Protocol (SSTP)
Common 802.1X connection tunnel types
Virtual LANs (VLAN)
Others
Ascend Tunnel Management Protocol (ATMP) Bay Dial Virtual Services (DVS) Generic Route Encapsulation (GRE) IP-in-IP Encapsulation (IP-IP)
OK Cancel

Click box for Layer Two Tunneling Protocol (L2TP), Click OK.

w Network Policy	X
Specify condition	cify Conditions r the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one on is required.
Conditions:	
Condition	Value
Tunnel Type	Layer Two Tunneling Protocol (L2TP)
🝏 Windows Groups	SCHOOL\vpn_access
Condition description:	
Condition description: The Windows Groups co	ondition specifies that the connecting user or computer must belong to one of the selected groups.

Click Next and Next on Access Granted.

New Network P	olicy
	Configure Authentication Methods Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.
EAP types are no	egotiated between NPS and the client in the order in which they are listed.
Add Add Less secure V Microsoft End User can Encrypted at Unencrypted Allow clients	Move Up Move Down Edit Remove authentication methods: crypted Authentication (MS-CHAP-v2) change password after it has expired crypted Authentication (MS-CHAP) change password after it has expired uthentication (CHAP) Lauthentication (CPAP) I authentication (PAP, SPAP) to connect without negotiating an authentication method.
	Previous Next Finish Cancel

Only Check boxes for MS-CHAP-V2 and User can change password after it has expired. Then Click Next.

Click Next on Configure Constraints and Next on Configure Settings and Finish.

e
e

Make sure that the L2TP Rule is first or you will get an error with Authentication.

Setup a Windows 7 Client to Connect

Step 1

Log into a Windows machine. SSTP was introduced in Windows Vista, so the OS must be Vista or Greater (or Server 2008 and greater). Go to **Network and Sharing Center**. Click **Setup New Connection or Network**. Steps 2-9 are for Windows 7 and step 10 is for Windows 10.

Step 2

Click Connect to a workplace.

💐 Se	t Up a Co	nnection or Network	_ 🗆 🗙
\bigcirc	😨 Set l	Jp a Connection or Network	
	Choose a	a connection option	
		Connect to the Internet Set up a wireless, broadband, or dial-up connection to the Internet.	
	2	Set up a new network Configure a new router or access point.	
		Connect to a workplace Set up a dial-up or VPN connection to your workplace.	
		Set up a dial-up connection Connect to the Internet using a dial-up connection.	
		Next	Cancel

Step 3

Click Use Internet Connection (VPN).



Fill in your info, and click **Don't connect now; just setup so I can connect later**.

Connect to a Workplace	
🌀 🗽 Connect to a Workplace	
Type the Internet address	to connect to
Your network administrator o	can give you this address.
Internet address:	vpn.mydomain.com
D <u>e</u> stination name:	Home Lab
🔲 Use a <u>s</u> mart card	
🛞 🥅 Allow other people t This option allows an	o use this connection yone with access to this computer to use this connection.
🔽 Don't connect now; j	ust set it up so I can connect later

Step 5

Enter your user information. Don't forget that if you didn't setup a Group to access the VPN using NAP, you'll need to enable Dial-In access within Active Directory Users and Computers for that user.

🔣 🛛 Connect to a Workplace		
🌀 🔚 Connect to a Workpl	ace	
Type your user name an	d password	
<u>U</u> ser name:	test-vpn	
<u>P</u> assword:	•••••	
	Show characters	
<u>D</u> omain (optional):	AD.LOCAL	
		<u>C</u> reate Cancel

We still need to configure a couple more things. Click on your connection -> Properties.



Step 7

Click the Security Tab -> Change type of VPN to SSTP. By default, it detects the type of VPN automatically, but slightly slows down the process.

Also change your authentication as seen below. That's all you need. Note that, by default, Windows VPNS will use the remote gateway. If you want to modify that, go to Properties -> Networking -> IPv4 -> Advanced -> Uncheck Use Default Gateway on Remote Network.



Right-click -> Connect.



Windows 10 VPN Client Setup

In Windows 10 click Settings> Network & Internet> VPN and click add a VPN connection. Select Windows (built-in) as the VPN provider and give the connection a name of your choosing. Enter the external DNS name of your VPN server and choose the VPN type as SSTP.

You can then enter the credentials of the VPN user account, then save the connection.

Add a VPN connection	
Windows (built-in)	V
Connection name	
VPNLAB	
Server name or address	
duckdns.org	
VPN type	
Secure Socket Tunneling Protocol (SSTP)	
Type of sign-in info	
User name and password	✓
User name (optional)	
vpn	
Password (optional)	
•••••	
	Save Cancel

If you are going to use L2TP on Windows you have to add the following Registry DWORD:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent

Create a new DWORD parameter with the name AssumeUDPEncapsulationContextOnSendRule and the value 2. Restart the server and the machine in order to apply changes.

This needs to be added on the server and the client machine.

Setup L2TP VPN on Mac OSx



- 1. Open System Preferences.
- 2. Open Network.



- 3. Click the +
- 4. Choose VPN for Interface Type.
- 5. Choose L2TP over IPSec for VPN Type.
- 6. Click Create.

	Network	Q Search
Loca	ition: Automatic	0
 Wi-Fi Connected Bluetooth PAN Not Connected Thundethernet Not Connected ThundeIt Bridge Not Connected VPN (L2TP) Not Configured 	Status: Not Connec Configuration: asd-vpn Server Address: asd-vpn.k1: Account Name: faysala Authentica Connect	ted 7 8 2ar.us 9 ation Settings 10
+ - *	🔲 Show VPN status in menu bar	Advanced ?
		Revert Apply

- 7. You can leave it Default or choose add a configuration and give it a name.
- 8. Enter the FQDN URL of the VPN Server.
- 9. Enter the AD username. You don't need to enter the domain.
- **10.** Click Authentication Settings.

	Network	Q Search
User	Authentication:	
· •	Password:	
• Wi-Fi	RSA SecurID	
	Certificate Select	
Not Connected	Kerberos	
Thundethernet Not Connected	CryptoCard	
Thundelt Bridge Mac	nine Authentication:	
Not Connected	Shared Secret:	12
VPN (L2TP) Not Configured	Certificate	Select
	Group Name:	
	Cancel	OK
		13
+ - & -	Show VPN status in menu bar	Advanced ?
		Revert Apply

- **11.** Enter the AD Password.
- **12.** Enter the Preshared Key from the Server Setup. Click OK.
- 13. Click Advanced.

	Network	Q Search
VPN (L2TP)		
	Options TCP/IP DNS Proxies	
	Session Options:	
	Disconnect when switching user accounts	
	Disconnect when user logs out	
14	Advanced Options:	
and a state of the second second	Use verbose logging	
		Cancel
S		Cancel OK

14. Click Send all traffic over VPN connection.



- 15. Click Apply.
- 16. Click Connect and it should show Connected.

Show All		Network		9	
	Location:	Automatic		:	
Wi-Fi Connected VPN (U2777) Connected	() ()	Status: Connect Time IP Address	Connected 00:01:15 10:211.1.1	Sent: Received:	00000022300 00000000000
Thundthernet Not Connected Bluetooth PAN Not IP Address	↔	Configuration: Server Address: Account Name:	Default para 21. openg vpn Authenticatio Disconnect	n Settings	•
+ - 0+		Show VPN status i	n menu bar	A	fvanced] (7
+ - &+	prevent further	Show VPN status i	n menu bar Assist me	Reve	fvanced