|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | |
|  | | **Palo Alto Site to Site VPN with Shared Secret keys** | | | | |  | |
|  |  | | | | | | |  |
|  | | | |  |  | | | |
|  | | | | Weizhen Chen |  | | | |
|  | | | | —CCNP—Jeffery Mason &Michael Hansen |  | | | |
|  | | |  | | |  | | |

Purpose

The purpose of the lab was to learn how to set up setup a Site-To-Site VPN on Palo Altos with pre-shared keys.

Background information

Palo Alto Networks is an American Multinational cybersecurity company headquartered in Santa Clara, California. It is known to produce cloud-based firewalls that are highly used in the IT industry. With features such as identifying, controlling, and inspecting encrypted SSL traffic and applications. Including real time low latency content scanning to protect users from viruses, spyware, data leakage, and application vulnerability powered by a stream-based threat prevention engine. And its performance does not downgrade as more security features are enabled. Site-to-Site VPN is a virtual private network which allows you to connect between two or more networks. It allows you to configure route-based VPNs to connect Palo Alto firewalls at a different place to another device or firewall. For a site-to-site VPN to work, you would need the Palo Alto firewall to first create a route-based VPN which would make the firewall make routing decision of IP address based according to the VPN. It would be handled as VPN traffic if the traffic was routed using VPN tunnel. The IP Security (IPSec) set of protocols is required for VPN traffic to secure and encrypt information in the TCP/IP packet by setting up a secure tunnel for the traffic. These IP packets are embedded in another IP payload where a new header is applied to the packet and go through secured IPSec tunnel. After that the source IP address would be the local VPN peer and the destination IP address would be the VPN peer on the far end of the tunnel. When the packet reaches VPN destination the header of the IP packet would be removed and the original information of the Ip packet is delivered to the set destination. With a site-to-site VPN, a company can securely connect network to its remote offices to communicate and share resources as a single network. To set up the VPN tunnel, the peers that will be connected with site-to-site VPN would need to be authenticated using Internet Key Exchange (IKE) either use certificates or pre shared keys to set up the IPSec Security Associations (SAs) used to set all the parameters for the secure delivery trough the IPSec tunnel. The Pre-Shared Key (PSK) or shared secret is a secret pre shared key or password established between two firewalls, used as a form of password for your VPN gateway which authenticates and sets up on your device, that you enter when you configure your gateway.

Lab commands/Configurations

Peer 1 Configuration:

set deviceconfig system ip-address 192.168.20.10

set deviceconfig system netmask 255.255.255.0

set deviceconfig system update-server updates.paloaltonetworks.com

set deviceconfig system update-schedule threats recurring weekly day-of-week thursday

set deviceconfig system update-schedule threats recurring weekly at 12:00

set deviceconfig system update-schedule threats recurring weekly action download-and-install

set deviceconfig system timezone US/Pacific

set deviceconfig system service disable-telnet yes

set deviceconfig system service disable-http yes

set deviceconfig system hostname PaloLabo

set deviceconfig system device-telemetry device-health-performance yes

set deviceconfig system device-telemetry product-usage yes

set deviceconfig system device-telemetry threat-prevention yes

set deviceconfig system device-telemetry region Americas

set deviceconfig system type static

set deviceconfig system default-gateway 192.168.20.1

set deviceconfig system dns-setting servers primary 1.1.1.1

set deviceconfig system dns-setting servers secondary 8.8.8.8

set deviceconfig setting config rematch yes

set deviceconfig setting management hostname-type-in-syslog FQDN

d-hosts top-application-categories top-technology-categories bandwidth-trend risk-trend threat-trend top-users top-attacker-sources top-attacker-destinations top-victim-sources top-victim-destinations top-attackers-by-source-countries top-attackers-by-destination-countries top-victims-by-source-countries top-victims-by-destination-countries top-sources top-destinations top-destination-countries top-source-countries top-connections top-ingress-interfaces top-egress-interfaces top-ingress-zones top-egress-zones top-applications top-http-applications top-rules top-attacks top-spyware-threats top-viruses top-vulnerabilities wildfire-file-digests top-websites top-url-categories top-url-users top-url-user-behavior to

p-blocked-websites top-blocked-url-categories top-blocked-url-users top-blocked-url-user-behavior blocked-credential-post unknown-tcp-connections unknown-udp-connections top-denied-sources top-denied-destinations top-denied-applications risky-users "SaaS Application Usage" gtp-events-summary gtp-malicious-wildfire-submissions gtp-security-events gtp-v1-causes gtp-v2-causes gtp-users-visiting-malicious-url top-gtp-attacker-destinations top-gtp-attacker-sources top-gtp-victim-destinations top-gtp-victim-sources sctp-error-causes sctp-events-summary sctp-security-events ]

set network interface ethernet ethernet1/1 layer3 ndp-proxy enabled no

set network interface ethernet ethernet1/1 layer3 sdwan-link-settings upstream-nat enable no

set network interface ethernet ethernet1/1 layer3 sdwan-link-settings upstream-nat static-ip

set network interface ethernet ethernet1/1 layer3 sdwan-link-settings enable no

set network interface ethernet ethernet1/1 layer3 lldp enable no

set network interface ethernet ethernet1/1 layer3 interface-management-profile Management

set network interface ethernet ethernet1/1 layer3 dhcp-client

set network interface ethernet ethernet1/2 layer2 lldp enable no

set network interface ethernet ethernet1/3 layer2 lldp enable no

set network interface ethernet ethernet1/4 layer2 lldp enable no

set network interface ethernet ethernet1/5 layer2 lldp enable no

set network interface ethernet ethernet1/6 layer2 lldp enable no

set network interface ethernet ethernet1/7 layer3 ndp-proxy enabled no

set network interface ethernet ethernet1/7 layer3 sdwan-link-settings upstream-nat enable no

set network interface ethernet ethernet1/7 layer3 sdwan-link-settings upstream-nat static-ip

set network interface ethernet ethernet1/7 layer3 sdwan-link-settings enable no

set network interface ethernet ethernet1/7 layer3 ip 192.168.255.1/24

set network interface ethernet ethernet1/7 layer3 lldp enable no

set network interface loopback units

set network interface vlan ipv6 neighbor-discovery router-advertisement enable no

set network interface vlan ndp-proxy enabled no

set network interface vlan ddns-config ddns-vendor-config ztp-ddns-ttl value 30

set network interface vlan ddns-config ddns-hostname system-hostname

set network interface vlan ddns-config ddns-vendor paloalto-networks-ddns

set network interface vlan ddns-config ddns-enabled yes

set network interface vlan adjust-tcp-mss enable no

set network interface vlan units vlan.666 ipv6 neighbor-discovery router-advertisement enable no

set network interface vlan units vlan.666 ndp-proxy enabled no

set network interface vlan units vlan.666 ddns-config ddns-vendor-config ztp-ddns-ttl value 30

set network interface vlan units vlan.666 ddns-config ddns-hostname system-hostname

set network interface vlan units vlan.666 ddns-config ddns-vendor paloalto-networks-ddns

set network interface vlan units vlan.666 adjust-tcp-mss enable no

set network interface vlan units vlan.666 ip 192.168.20.1/24

set network interface tunnel units tunnel.666 interface-management-profile Management

set network interface tunnel units tunnel.666 ip 192.168.254.1/24

set network vlan Vlalto virtual-interface interface vlan.666

set network vlan Vlalto interface [ ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5 ethernet1/6 ]

set network virtual-wire

set network profiles monitor-profile default interval 3

set network profiles monitor-profile default threshold 5

set network profiles monitor-profile default action wait-recover

set network profiles monitor-profile "Tunnel Monitoring"

set network profiles interface-management-profile Management http no

set network profiles interface-management-profile Management https yes

set network profiles interface-management-profile Management ssh yes

set network profiles interface-management-profile Management ping yes

set network ike crypto-profiles ike-crypto-profiles default encryption [ aes-128-cbc 3des ]

set network ike crypto-profiles ike-crypto-profiles default hash sha1

set network ike crypto-profiles ike-crypto-profiles default dh-group group2

set network ike crypto-profiles ike-crypto-profiles default lifetime hours 8

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-128 encryption aes-128-cbc

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-128 hash sha256

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-128 dh-group group19

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-128 lifetime hours 8

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-256 encryption aes-256-cbc

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-256 hash sha384

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-256 dh-group group20

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-256 lifetime hours 8

set network ike crypto-profiles ike-crypto-profiles IKE\_Tunnel hash sha512

set network ike crypto-profiles ike-crypto-profiles IKE\_Tunnel dh-group group21

set network ike crypto-profiles ike-crypto-profiles IKE\_Tunnel encryption [ aes-256-cbc aes-192-cbc aes-128-cbc ]

set network ike crypto-profiles ike-crypto-profiles IKE\_Tunnel lifetime hours 8

set network ike crypto-profiles ipsec-crypto-profiles default esp encryption [ aes-128-cbc 3des ]

set network ike crypto-profiles ipsec-crypto-profiles default esp authentication sha1

set network ike crypto-profiles ipsec-crypto-profiles default dh-group group2

set network ike crypto-profiles ipsec-crypto-profiles default lifetime hours 1

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-128 esp encryption aes-128-gcm

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-128 esp authentication none

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-128 dh-group group19

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-128 lifetime hours 1

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-256 esp encryption aes-256-gcm

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-256 esp authentication none

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-256 dh-group group20

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-256 lifetime hours 1

set network ike crypto-profiles ipsec-crypto-profiles IPSec\_Tunnel esp authentication sha512

set network ike crypto-profiles ipsec-crypto-profiles IPSec\_Tunnel esp encryption aes-256-cbc

set network ike crypto-profiles ipsec-crypto-profiles IPSec\_Tunnel lifetime hours 1

set network ike crypto-profiles ipsec-crypto-profiles IPSec\_Tunnel dh-group group21

set network ike crypto-profiles global-protect-app-crypto-profiles default encryption aes-128-cbc

set network ike crypto-profiles global-protect-app-crypto-profiles default authentication sha1

set network ike gateway Tunnel\_Gateway authentication certificate local-certificate name Tunnel-Peer-1

set network ike gateway Tunnel\_Gateway authentication certificate certificate-profile STS\_Tunnel

ad-mismatch yes

set network ike gateway Tunnel\_Gateway protocol ikev1 dpd enable yes

set network ike gateway Tunnel\_Gateway protocol ikev1 ike-crypto-profile IKE\_Tunnel

set network ike gateway Tunnel\_Gateway protocol ikev2 dpd enable yes

set network ike gateway Tunnel\_Gateway protocol ikev2 ike-crypto-profile IKE\_Tunnel

set network ike gateway Tunnel\_Gateway protocol version ikev2

set network ike gateway Tunnel\_Gateway protocol-common nat-traversal enable no

set network ike gateway Tunnel\_Gateway protocol-common fragmentation enable no

set network ike gateway Tunnel\_Gateway protocol-common passive-mode yes

set network ike gateway Tunnel\_Gateway local-address interface ethernet1/7

set network ike gateway Tunnel\_Gateway local-address ip 192.168.255.1/24

set network ike gateway Tunnel\_Gateway peer-address ip 192.168.255.254

set network ike gateway Tunnel\_Gateway local-id id CN=Tunnel\_P1,ST=Washington,C=US

set network ike gateway Tunnel\_Gateway local-id type dn

set network ike gateway Tunnel\_Gateway peer-id id CN=Tunnel\_P2,ST=Washington,C=US

set network ike gateway Tunnel\_Gateway peer-id type dn

set network ike gateway Tunnel\_Gateway peer-id matching exact

set network qos profile default class-bandwidth-type mbps class class1 priority real-time

set network qos profile default class-bandwidth-type mbps class class2 priority high

set network qos profile default class-bandwidth-type mbps class class3 priority high

set network qos profile default class-bandwidth-type mbps class class4 priority medium

set network qos profile default class-bandwidth-type mbps class class5 priority medium

set network qos profile default class-bandwidth-type mbps class class6 priority low

set network qos profile default class-bandwidth-type mbps class class7 priority low

set network qos profile default class-bandwidth-type mbps class class8 priority low

set network virtual-router default protocol bgp enable no

set network virtual-router default protocol bgp dampening-profile default cutoff 1.25

set network virtual-router default protocol bgp dampening-profile default reuse 0.5

set network virtual-router default protocol bgp dampening-profile default max-hold-time 900

set network virtual-router default protocol bgp dampening-profile default decay-half-life-reachable 300

set network virtual-router default protocol bgp dampening-profile default decay-half-life-unreachable 900

set network virtual-router default protocol bgp dampening-profile default enable yes

set network virtual-router RouterAlto ecmp algorithm ip-modulo

set network virtual-router RouterAlto protocol bgp routing-options graceful-restart enable yes

set network virtual-router RouterAlto protocol bgp enable no

set network virtual-router RouterAlto protocol rip enable no

set network virtual-router RouterAlto protocol ospf enable no

set network virtual-router RouterAlto protocol ospfv3 enable no

set network virtual-router RouterAlto interface [ ethernet1/1 ethernet1/7 tunnel.666 vlan.666 ]

set network virtual-router RouterAlto routing-table ip static-route "Default Route" nexthop ip-address 192.168.40.1

set network virtual-router RouterAlto routing-table ip static-route "Default Route" bfd profile None

set network virtual-router RouterAlto routing-table ip static-route "Default Route" interface ethernet1/1

set network virtual-router RouterAlto routing-table ip static-route "Default Route" metric 10

set network virtual-router RouterAlto routing-table ip static-route "Default Route" destination 0.0.0.0/0

set network virtual-router RouterAlto routing-table ip static-route "Default Route" route-table unicast

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" nexthop ip-address 192.168.254.1

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" bfd profile None

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" interface tunnel.666

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" metric 10

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" destination 192.168.10.0/24

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" route-table unicast

set network dhcp interface vlan.666 server option dns primary inherited

set network dhcp interface vlan.666 server option dns secondary inherited

set network dhcp interface vlan.666 server option inheritance source ethernet1/1

set network dhcp interface vlan.666 server option lease timeout 120

set network dhcp interface vlan.666 server option gateway 192.168.20.1

set network dhcp interface vlan.666 server option subnet-mask 255.255.255.0

set network dhcp interface vlan.666 server option wins primary inherited

set network dhcp interface vlan.666 server option wins secondary inherited

set network dhcp interface vlan.666 server option nis primary inherited

set network dhcp interface vlan.666 server option nis secondary inherited

set network dhcp interface vlan.666 server option ntp primary inherited

set network dhcp interface vlan.666 server option ntp secondary inherited

set network dhcp interface vlan.666 server option pop3-server inherited

set network dhcp interface vlan.666 server option smtp-server inherited

set network dhcp interface vlan.666 server ip-pool 192.168.20.2-192.168.20.254

set network dhcp interface vlan.666 server reserved 192.168.20.10

set network dhcp interface vlan.666 server reserved 192.168.20.254

set network dhcp interface vlan.666 server mode enabled

set network tunnel ipsec IPSEC\_TUNNEL auto-key ike-gateway Tunnel\_Gateway

set network tunnel ipsec IPSEC\_TUNNEL auto-key ipsec-crypto-profile IPSec\_Tunnel

set network tunnel ipsec IPSEC\_TUNNEL tunnel-monitor enable yes

set network tunnel ipsec IPSEC\_TUNNEL tunnel-monitor destination-ip 192.168.255.254

set network tunnel ipsec IPSEC\_TUNNEL tunnel-monitor tunnel-monitor-profile "Tunnel Monitoring"

set network tunnel ipsec IPSEC\_TUNNEL tunnel-interface tunnel.666

set network tunnel ipsec IPSEC\_TUNNEL disabled no

set shared application

set shared application-group

set shared service

set shared service-group

set shared botnet configuration http dynamic-dns enabled yes

set shared botnet configuration http dynamic-dns threshold 5

set shared botnet configuration http malware-sites enabled yes

set shared botnet configuration http malware-sites threshold 5

set shared botnet configuration http recent-domains enabled yes

set shared botnet configuration http recent-domains threshold 5

set shared botnet configuration http ip-domains enabled yes

set shared botnet configuration http ip-domains threshold 10

set shared botnet configuration http executables-from-unknown-sites enabled yes

set shared botnet configuration http executables-from-unknown-sites threshold 5

set shared botnet configuration other-applications irc yes

set shared botnet configuration unknown-applications unknown-tcp destinations-per-hour 10

set shared botnet configuration unknown-applications unknown-tcp sessions-per-hour 10

set shared botnet configuration unknown-applications unknown-tcp session-length maximum-bytes 100

set shared botnet configuration unknown-applications unknown-tcp session-length minimum-bytes 50

set shared botnet configuration unknown-applications unknown-udp destinations-per-hour 10

set shared botnet configuration unknown-applications unknown-udp sessions-per-hour 10

maximum-bytes 100

set shared botnet configuration unknown-applications unknown-udp session-length minimum-bytes 50

set shared botnet report topn 100

set shared botnet report scheduled yes

set shared certificate Tunnel-CA subject-hash be30ce7e

set shared certificate Tunnel-CA issuer-hash be30ce7e

set shared certificate Tunnel-CA not-valid-before "Mar 13 19:11:24 2023 GMT"

set shared certificate Tunnel-CA issuer "issuer=C = US, ST = Washington, CN = SSL\_Tunnel"

set shared certificate Tunnel-CA not-valid-after "Mar 12 19:11:24 2024 GMT"

set shared certificate Tunnel-CA common-name SSL\_Tunnel

set shared certificate Tunnel-CA expiry-epoch 1710270684

set shared certificate Tunnel-CA ca yes

set shared certificate Tunnel-CA subject "subject=C = US, ST = Washington, CN = SSL\_Tunnel"

set shared certificate Tunnel-CA public-key "-----BEGIN CERTIFICATE-----

MIIFGTCCAwGgAwIBAgIUTDKsE31mZkfXMZgmNMgB4KE4lgkwDQYJKoZIhvcNAQEN

BQAwNzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCldhc2hpbmd0b24xEzARBgNVBAMM

ClNTTF9UdW5uZWwwHhcNMjMwMzEzMTkxMTI0WhcNMjQwMzEyMTkxMTI0WjA3MQsw

CQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGluZ3RvbjETMBEGA1UEAwwKU1NMX1R1

bm5lbDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALRpfLnAbY4rR8Ha

zpaNerb3D98f68/6P8CJjQnTmgHAPWlWqmns4NL9ETbnsGTmQjh4lVPAK3a90JBx

3D3m/8VoH528Fyw8DT5Ndg+tSf3qVbRi5yS2prZ//ttjrwJ/jGi6JSGkUV5gALMI

XJx4VpxFE5m7v9Mjm+wMhTYLm1GVxgl+IoW4piBmnQr8zClFvhfw4ALmCi7C9UjC

t/RqVdCBKq9vTuThFBws9ZxfIPmE98dOSFwKrKk102L2Uwsezd+vwds6qPeQDV6O

XqhxtQeVtzUZowA+ch7L4UXbnak/62iBz72sLTNYp8/Kzl++FpT5Qrke2t4btoug

wEUJW7Iqti+AFm+//ShLnxbtWd9UFmq+gWY21WHu5ToZgEP6uM2iDuIf5feuJzMJ

v7JZGPPaIwKp1m7B+tywISRjGtGZ69o1PjIfDrXVgNNqgUfIaKmjCdyVjyxc1hFB

tIJCYU4Oy9RCVfgRl1wWybYYC1yWNz7NSeHEepJ0or13c/XMHjCA/ASAcRUR85Jh

ypvG3NplW4du1SJebDEGYz2ZTbnNWUnM62WHPGejY0H+RM/7wzYJv6XfFEZaQuV+

fC7bJ1FqXzGsjJO++0jKrPOoWQqUYc0B8U020oFEZB9jH6CxzZBg9T7JU7x6SRk6

0qXRYZkZvRSefS8Pjsxw758sTzYPAgMBAAGjHTAbMAwGA1UdEwQFMAMBAf8wCwYD

VR0PBAQDAgIEMA0GCSqGSIb3DQEBDQUAA4ICAQCtSjeT/aN1h8V5Afp+bYcDmlDt

DIsLNYQA3OOMu3Cnw+7XXVr/Mi7/JAwMW/bDOBq7s96s9c1YzcZWWcFny72s3CwF

6WNb7r60qBxuADU+ACa7661FOvHT6r4bXES06xwBKR6rxPS5zZ3jZWisJLU9jNtS

s/6BJsFUj7h8t/fJJNsO/y+UIsVgYH+YL0PkTg9Gc8dz55/In1vi/4QArhSV+b1d

ksMsOVSzeKFCHZAOaL0ynu/aJclW0ZK22zeXm94yYDEY+OtwYEapALRAg8Z/5TFB

41+hqXGCyLKcu1OMesdKpmLMuPy5YFvqyE7+pmOs/mG5GCUFiLmr61zhAhV0mts2

RaMlEgyL+BTnUcIV88/BgrMPN3jzDEnU4sk9n5bks3WklTcE7oSjnOfro92cKjPT

xWfNpG/nHw/mDW4YC0LTbhk+ILRBq6JnOI5mX8aq4bmZ8xVWdSzbZaNc09dHmvQf

5ax53FTNv700hPwbkPPOJ47vv2ij8ACrEfzQLaWETUl8IcI19Sry/TsvFQ+TOv7A

Lm7+J3TKzqTIxr335MDVmFadn4FxwEcPnEqOz3SbcLjnFLcPUVuXi/QioBluaAxn

tc35UUGFinMjZwmJp9LsoLn9JkVj60mM2k4n4qARS1CKOdHC5e1hjAd8qwslHGih

ePz4yW7g6elqUiinvA==

-----END CERTIFICATE-----

"

set shared certificate Tunnel-CA algorithm RSA

set shared certificate Tunnel-CA private-key -AQ==9lTjtP2r9URDkt9P/JZr1eScHrc=

yfZzhH1buY2Hdtp6/0DuN6VycBeu7jW6qlxeOpLMAOvOLM54qqEPrhIa0F9Z7O3HoUZgGkKo2JLuHXtD+h8eULMBvaz9mbAd8aisGG3xBVzXoE616p12DAUQNYcCRHlwK0S+rckT7pY+QBIwmTWsEHlleg62+JovE3z5KNhsKBsdAV7EEooRJBV8JMaSvlOih7A9I6TykJ0a4iG6Px7jbsj7L8AJ5JQxtj2IHvxC5bPiESZf/VJmzVK6zuuLToRGenqbHLKXFrwiC6lj4HDbcnGg95zRip2rpsEd1LGujlLjbcyNFn+DeFn9XYnYrCMw0BwlpBfjHRebmd89ahfSt8EheOarDfH+hVBS0fUQ+GbQRvDQQ2HL4tvmClr9aTLuPum3YuxXsfxhoNEuomgwIR++vWbGfpcjfH30ck0XVE/SEUsrTUhAM0LUCDyq5lf4RZx6/kFsAMb55iQ/6r4fEgk9MCBvDDdc



bW9oVLZfOj7sUYrQgksrbsmU43vtmnoMllqlIvrkLQ/0zEcuGfn5ZZAXwmDDIxtrzpmuEayCkfwEkGra9+9Mxi1Z3uBHS8Tj+QCBNN6oDXff77Zlp6rzQg0FFqNa0Umh92yA3bDyyxrQTEMots69amXTZOaqRXRDnkNZU1g+3CpX1lEXE8gP+EYXusejMY4sv/g4/QlYcQ6ehRZua8LAPjIZAU12+Rzx51xcfIRh0jHJdsadSNqgmFY8Qf7k0OfOdAjOJtUMNAWDWjzGczQQohfQjjzJn/Nwg4Ub76ENcreJbP8LNYZyRPMmUHZORdIc7TD5zC9zseVVD0U5GulQtDhYyQ8Vp020VUpJIK0M/OzzrN5KNJNbVU36rp5CJazFlUpVOdHFjiYeDUWyL68kNvkXc=

set shared certificate Tunnel-Peer-1 subject-hash 901bdc0d

set shared certificate Tunnel-Peer-1 issuer-hash be30ce7e

set shared certificate Tunnel-Peer-1 not-valid-before "Mar 15 14:22:12 2023 GMT"

set shared certificate Tunnel-Peer-1 issuer "issuer=C = US, ST = Washington, CN = SSL\_Tunnel"

set shared certificate Tunnel-Peer-1 not-valid-after "Mar 14 14:22:12 2024 GMT"

set shared certificate Tunnel-Peer-1 common-name Tunnel\_P1

set shared certificate Tunnel-Peer-1 expiry-epoch 1710426132

set shared certificate Tunnel-Peer-1 ca no

set shared certificate Tunnel-Peer-1 subject "subject=C = US, ST = Washington, CN = Tunnel\_P1"

set shared certificate Tunnel-Peer-1 public-key "-----BEGIN CERTIFICATE-----

MIIFWDCCA0CgAwIBAgIEdupDQDANBgkqhkiG9w0BAQ0FADA3MQswCQYDVQQGEwJV

UzETMBEGA1UECAwKV2FzaGluZ3RvbjETMBEGA1UEAwwKU1NMX1R1bm5lbDAeFw0y

MzAzMTUxNDIyMTJaFw0yNDAzMTQxNDIyMTJaMDYxCzAJBgNVBAYTAlVTMRMwEQYD

VQQIDApXYXNoaW5ndG9uMRIwEAYDVQQDDAlUdW5uZWxfUDEwggIiMA0GCSqGSIb3

DQEBAQUAA4ICDwAwggIKAoICAQCiHNR4wSH22r3Yif8hjsHgkLYz/pBXtlPk4bDv

hnrelHpN1tXM5fjayqESsymKk53aVkVTviP2EhtnkIGmvlrz9ZI79f3+so7YaAE4

eMAAN7hdewdLUxbBgPVdCyA8c3zAWRou+xrYi2HooeINPHvPmHBLxKznWPkfR7O+

EacyFFW/7zMV0AbDvVE16UNsvpK6EiDvsEgLRv42HmnI5sZ9/6BdPjLX9J/RI29I

Sgbzq7P/k0N+GnJq0m6WsOJ+Xn5BGwdvbZd45mcj+NOZyMEis+HDwc7Qvh8ZNIJS

YtIoT5a6L0SvJpt/PePEmyzrDGNNz+gOJzKPQSy3oosGlS42bGaO0EB31oGPGkEk

LqhKSt+LRPdctxaToaFvjA6+MgMJng/nt7nsix2fqkZO4Cy7XWdQHsZqO4b0/bam

vg3vRMTjUX/zgkJh7NI7TMd3wVJO0fXvz3h1WFR7OKXgyqh8cYg4mzgRgGhxavyJ

JLlIceckPCpd2NPkq1FCl+VlWAu+VM/7PeUpG6lZXx94F629q/rS64OGgktUm4mi

LOkzRsru8B1oX1ro31bCZ8uCWe/+7vYO1iW4h+YJunv9ZoND7FzadwjRIKEOuE5v

WsQJjShYbQoiNzQqFv3WCWXCyGuDq8Jc8e7AXYi7sbzc8qmzM+QVNI0w7c/mi2Cm

qLl2HQIDAQABo20wazAJBgNVHRMEAjAAMAsGA1UdDwQEAwIDuDAnBgNVHSUEIDAe

BggrBgEFBQcDAQYIKwYBBQUHAwIGCCsGAQUFBwMFMAkGA1UdIwQCMAAwHQYDVR0O

BBYEFMhtuaPvmCJFsgdhHwyN/CPV4wbuMA0GCSqGSIb3DQEBDQUAA4ICAQApGce7

RA/F7cgTy72mcyAYMwrfvn3zGmqbYnnXDsBPoOeH5QiBiAZdT/+FR5RMvK4/Mx1I

QUS9ryPA3UYK/K+Zpc0A4yNy/YhJt+i6cwM/zdaG9wGZxJuZhb8n0NzAl4eTAbBi

QW7fahuauz1Bj1DCivAn6lEhG0wZf7Gf8Id0Abw9JoUSpCj9RbKprvZpBGDBsQq1

r/nmr1iR/IDHEyfwzta6SJ5iTi6VDgIMn8yibtuyLfBHZL7CKWd2/BcZdb7smYd8

iEkRuTNclNrz9bwqtPkAVMeunXUXuwLUqKwtvGRAFawcHbs1DGxdtGLSUF+nzZRz

B9LYxl4ajNZkhZFHgRipIzv+vaTO/KfT/a1xBDVFowXSOwxlwOA/GocRxSemmbND

xHrgGhEV/FDvXRItnaE5MyieiuF6VIop+eiR4x4Xf0Cj+kK2nAF4G7lNA5gFvVQ0

x0COQK/o+t6FdGxI1CneMJpJ0m38oF03BjBcUkHCHS0HufsiIfo25lnZgLecrRn8

CfFVbx9jnTTRPZ9HUaGgpLdXm0DSsfZnkRfnxxhIzM+Pt2MgfKROi7EcY3kh0J+H

cZqZFRiDongQqXUpx6ys2ME5q3TaZ7rXKttJF78UHebcR1+qCgRrHLxhNykBQaNs

hipsW7lL/YtpeOcy9WS26tyhovmp+SF1qNFkDA==

-----END CERTIFICATE-----

"

set shared certificate Tunnel-Peer-1 algorithm RSA

set shared certificate Tunnel-Peer-1 private-key -AQ==SvQ2vvLCmzjHMwWwo5fGekSRMR0=





set shared certificate-profile STS\_Tunnel CA Tunnel-CA

set zone trust network virtual-wire

set zone untrust network virtual-wire

set zone Trust-L3 network layer3 vlan.666

set zone Untrust-L3 network layer3 [ ethernet1/1 ethernet1/7 ]

set zone Trust-L2 network layer2 [ ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5 ethernet1/6 ]

set zone VPN\_Tunnel network layer3 tunnel.666

set service-group

set service

set schedule

set rulebase security rules rule1 from trust

set rulebase security rules rule1 to untrust

set rulebase security rules rule1 source any

set rulebase security rules rule1 destination any

set rulebase security rules rule1 service any

set rulebase security rules rule1 application any

set rulebase security rules rule1 action allow

set rulebase security rules rule1 log-end yes

set rulebase security rules "Internet Outgoing" profile-setting group Internet

set rulebase security rules "Internet Outgoing" to Untrust-L3

set rulebase security rules "Internet Outgoing" from Trust-L3

set rulebase security rules "Internet Outgoing" source any

set rulebase security rules "Internet Outgoing" destination any

set rulebase security rules "Internet Outgoing" source-user any

set rulebase security rules "Internet Outgoing" category any

set rulebase security rules "Internet Outgoing" application any

set rulebase security rules "Internet Outgoing" service application-default

set rulebase security rules "Internet Outgoing" source-hip any

set rulebase security rules "Internet Outgoing" destination-hip any

set rulebase security rules "Internet Outgoing" action allow

set rulebase security rules "Internet Outgoing" description "Traffic going out to the internet"

set rulebase security rules "VPN Tunnel" to [ Trust-L3 Untrust-L3 VPN\_Tunnel ]

set rulebase security rules "VPN Tunnel" from [ Trust-L3 Untrust-L3 VPN\_Tunnel ]

set rulebase security rules "VPN Tunnel" source any

set rulebase security rules "VPN Tunnel" destination any

set rulebase security rules "VPN Tunnel" source-user any

set rulebase security rules "VPN Tunnel" category any

set rulebase security rules "VPN Tunnel" application any

set rulebase security rules "VPN Tunnel" service application-default

set rulebase security rules "VPN Tunnel" source-hip any

set rulebase security rules "VPN Tunnel" destination-hip any

set rulebase security rules "VPN Tunnel" action allow

set rulebase security rules "VPN Tunnel" description "Allows VPN Traffic between the 2 peers."

set rulebase nat rules "Internet Outgoing" source-translation dynamic-ip-and-port interface-address interface ethernet1/1

set rulebase nat rules "Internet Outgoing" to Untrust-L3

set rulebase nat rules "Internet Outgoing" from Trust-L3

set rulebase nat rules "Internet Outgoing" source any

set rulebase nat rules "Internet Outgoing" destination any

set rulebase nat rules "Internet Outgoing" service any

set rulebase nat rules "Internet Outgoing" to-interface ethernet1/1

set profile-group Internet virus default

set profile-group Internet spyware strict

set profile-group Internet vulnerability strict

set profile-group Internet url-filtering default

set import network interface [ ethernet1/1 ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5 ethernet1/6 ethernet1/7 vlan vlan.666 tunnel.666 ]

set application-group

set application

set mgt-config users admin phash $5$eftfahiv$lEx2H1biYTXVvPnkHwCice.wV8MEFpjts0J2y2f/HU8

set mgt-config users admin permissions role-based superuser yes

set mgt-config password-complexity enabled yes

set mgt-config password-complexity minimum-length 8

Peer 2 Configuration:

set deviceconfig system ip-address 192.168.10.10

set deviceconfig system netmask 255.255.255.0

set deviceconfig system update-server updates.paloaltonetworks.com

set deviceconfig system update-schedule threats recurring hourly at 5

set deviceconfig system update-schedule threats recurring hourly action download-and-install

set deviceconfig system update-schedule global-protect-clientless-vpn recurring hourly at 15

set deviceconfig system update-schedule global-protect-clientless-vpn recurring hourly action download-and-install

set deviceconfig system update-schedule global-protect-datafile recurring hourly at 5

set deviceconfig system update-schedule global-protect-datafile recurring hourly action download-and-install

set deviceconfig system update-schedule wildfire recurring real-time

set deviceconfig system timezone US/Pacific

set deviceconfig system service disable-telnet yes

set deviceconfig system service disable-http yes

set deviceconfig system service disable-userid-service yes

set deviceconfig system hostname LaboAlto

set deviceconfig system type static

set deviceconfig system default-gateway 192.168.10.1

set deviceconfig system dns-setting servers primary 1.1.1.1

set deviceconfig system dns-setting servers secondary 8.8.8.8

set deviceconfig system device-telemetry device-health-performance yes

set deviceconfig system device-telemetry product-usage yes

set deviceconfig system device-telemetry threat-prevention yes

set deviceconfig system device-telemetry region Americas

set deviceconfig setting config rematch yes

set deviceconfig setting management hostname-type-in-syslog FQDN

set deviceconfig setting management auto-acquire-commit-lock no

set deviceconfig setting ctd hold-client-request no

set deviceconfig setting ctd url-coach-timeout 10

set deviceconfig setting ctd url-admin-timeout 5

set deviceconfig setting ctd url-wait-timeout 5

set network interface ethernet ethernet1/1 layer3 ndp-proxy enabled no

set network interface ethernet ethernet1/1 layer3 sdwan-link-settings upstream-nat enable no

set network interface ethernet ethernet1/1 layer3 sdwan-link-settings upstream-nat static-ip

set network interface ethernet ethernet1/1 layer3 sdwan-link-settings enable no

set network interface ethernet ethernet1/1 layer3 lldp enable no

set network interface ethernet ethernet1/1 layer3 interface-management-profile Tunnel

set network interface ethernet ethernet1/1 layer3 dhcp-client

set network interface ethernet ethernet1/2 layer2 lldp enable no

set network interface ethernet ethernet1/3 layer2 lldp enable no

set network interface ethernet ethernet1/4 layer2 lldp enable no

set network interface ethernet ethernet1/5 layer2 lldp enable no

set network interface ethernet ethernet1/6 layer2 lldp enable no

set network interface ethernet ethernet1/7 layer2 lldp enable no

set network interface ethernet ethernet1/8 layer3 ndp-proxy enabled no

set network interface ethernet ethernet1/8 layer3 sdwan-link-settings upstream-nat enable no

set network interface ethernet ethernet1/8 layer3 sdwan-link-settings upstream-nat static-ip

set network interface ethernet ethernet1/8 layer3 sdwan-link-settings enable no

set network interface ethernet ethernet1/8 layer3 ip 192.168.255.254/24

set network interface ethernet ethernet1/8 layer3 lldp enable no

set network interface loopback units

set network interface vlan units vlan.666 ipv6 neighbor-discovery router-advertisement enable no

set network interface vlan units vlan.666 ipv6 address 2001:DB8:ACAD:1::1/64 advertise enable no

set network interface vlan units vlan.666 ipv6 address 2001:DB8:ACAD:1::1/64 advertise valid-lifetime 2592000

set network interface vlan units vlan.666 ipv6 address 2001:DB8:ACAD:1::1/64 advertise preferred-lifetime 604800

ertise onlink-flag yes

set network interface vlan units vlan.666 ipv6 address 2001:DB8:ACAD:1::1/64 advertise auto-config-flag yes

set network interface vlan units vlan.666 ipv6 address 2001:DB8:ACAD:1::1/64 enable-on-interface yes

set network interface vlan units vlan.666 ipv6 address 2001:DB8:ACAD:1::1/64 prefix

set network interface vlan units vlan.666 ipv6 enabled yes

set network interface vlan units vlan.666 ndp-proxy enabled no

set network interface vlan units vlan.666 adjust-tcp-mss enable no

set network interface vlan units vlan.666 ip 192.168.10.1/24

set network interface vlan units vlan.666 interface-management-profile "URL Overrider"

set network interface tunnel units tunnel.666 interface-management-profile Tunnel

set network interface tunnel units tunnel.666 ip 192.168.254.254/24

set network vlan VlanAlto virtual-interface interface vlan.666

set network vlan VlanAlto interface [ ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5 ethernet1/6 ethernet1/7 ]

set network virtual-wire

set network profiles monitor-profile default interval 3

set network profiles monitor-profile default threshold 5

set network profiles monitor-profile default action wait-recover

set network profiles monitor-profile "Tunnel Monitoring"

set network profiles interface-management-profile "URL Overrider" https yes

set network profiles interface-management-profile "URL Overrider" ssh no

set network profiles interface-management-profile "URL Overrider" ping yes

set network profiles interface-management-profile "URL Overrider" response-pages yes

set network profiles interface-management-profile "URL Overrider" http yes

set network profiles interface-management-profile Tunnel http no

set network profiles interface-management-profile Tunnel https yes

set network profiles interface-management-profile Tunnel ssh yes

set network profiles interface-management-profile Tunnel ping yes

set network ike crypto-profiles ike-crypto-profiles default encryption [ aes-128-cbc 3des ]

set network ike crypto-profiles ike-crypto-profiles default hash sha1

set network ike crypto-profiles ike-crypto-profiles default dh-group group2

set network ike crypto-profiles ike-crypto-profiles default lifetime hours 8

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-128 encryption aes-128-cbc

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-128 hash sha256

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-128 dh-group group19

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-128 lifetime hours 8

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-256 encryption aes-256-cbc

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-256 hash sha384

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-256 dh-group group20

set network ike crypto-profiles ike-crypto-profiles Suite-B-GCM-256 lifetime hours 8

set network ike crypto-profiles ike-crypto-profiles IKE\_Key hash sha512

set network ike crypto-profiles ike-crypto-profiles IKE\_Key dh-group group21

set network ike crypto-profiles ike-crypto-profiles IKE\_Key encryption aes-256-cbc

set network ike crypto-profiles ike-crypto-profiles IKE\_Key lifetime hours 8

set network ike crypto-profiles ipsec-crypto-profiles default esp encryption [ aes-128-cbc 3des ]

set network ike crypto-profiles ipsec-crypto-profiles default esp authentication sha1

set network ike crypto-profiles ipsec-crypto-profiles default dh-group group2

set network ike crypto-profiles ipsec-crypto-profiles default lifetime hours 1

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-128 esp encryption aes-128-gcm

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-128 esp authentication none

roup19

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-128 lifetime hours 1

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-256 esp encryption aes-256-gcm

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-256 esp authentication none

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-256 dh-group group20

set network ike crypto-profiles ipsec-crypto-profiles Suite-B-GCM-256 lifetime hours 1

set network ike crypto-profiles ipsec-crypto-profiles IPSEC\_Profile esp authentication sha512

set network ike crypto-profiles ipsec-crypto-profiles IPSEC\_Profile esp encryption aes-256-cbc

set network ike crypto-profiles ipsec-crypto-profiles IPSEC\_Profile lifetime hours 1

set network ike crypto-profiles ipsec-crypto-profiles IPSEC\_Profile dh-group group21

set network ike crypto-profiles global-protect-app-crypto-profiles default encryption aes-128-cbc

set network ike crypto-profiles global-protect-app-crypto-profiles default authentication sha1

set network ike gateway Tunnel authentication certificate local-certificate name Tunnel-Peer-2

set network ike gateway Tunnel authentication certificate certificate-profile STS-Profile

set network ike gateway Tunnel authentication certificate allow-id-payload-mismatch yes

set network ike gateway Tunnel protocol ikev1 dpd enable yes

set network ike gateway Tunnel protocol ikev1 ike-crypto-profile IKE\_Key

set network ike gateway Tunnel protocol ikev2 dpd enable yes

set network ike gateway Tunnel protocol ikev2 ike-crypto-profile IKE\_Key

set network ike gateway Tunnel protocol version ikev2

set network ike gateway Tunnel protocol-common nat-traversal enable no

set network ike gateway Tunnel protocol-common fragmentation enable no

set network ike gateway Tunnel protocol-common passive-mode no

set network ike gateway Tunnel local-address interface ethernet1/8

set network ike gateway Tunnel local-address ip 192.168.255.254/24

set network ike gateway Tunnel peer-address ip 192.168.255.1

set network ike gateway Tunnel disabled no

set network ike gateway Tunnel local-id type dn

set network ike gateway Tunnel local-id id CN=Tunnel\_P2,ST=Washington,C=US

set network ike gateway Tunnel peer-id id CN=Tunnel\_P1,ST=Washington,C=US

set network ike gateway Tunnel peer-id type fqdn

set network ike gateway Tunnel peer-id matching exact

set network qos profile default class-bandwidth-type mbps class class1 priority real-time

set network qos profile default class-bandwidth-type mbps class class2 priority high

set network qos profile default class-bandwidth-type mbps class class3 priority high

set network qos profile default class-bandwidth-type mbps class class4 priority medium

set network qos profile default class-bandwidth-type mbps class class5 priority medium

set network qos profile default class-bandwidth-type mbps class class6 priority low

set network qos profile default class-bandwidth-type mbps class class7 priority low

set network qos profile default class-bandwidth-type mbps class class8 priority low

set network virtual-router default protocol bgp enable no

set network virtual-router default protocol bgp dampening-profile default cutoff 1.25

set network virtual-router default protocol bgp dampening-profile default reuse 0.5

set network virtual-router default protocol bgp dampening-profile default max-hold-time 900

set network virtual-router default protocol bgp dampening-profile default decay-half-life-reachable 300

set network virtual-router default protocol bgp dampening-profile default decay-half-life-unreachable 900

set network virtual-router default protocol bgp dampening-profile default enable yes

set network virtual-router RouterAlto ecmp algorithm ip-modulo

set network virtual-router RouterAlto protocol bgp routing-options graceful-restart enable yes

set network virtual-router RouterAlto protocol bgp enable no

set network virtual-router RouterAlto protocol rip enable no

set network virtual-router RouterAlto protocol ospf enable no

set network virtual-router RouterAlto protocol ospfv3 enable no

set network virtual-router RouterAlto routing-table ip static-route RouteAlto nexthop ip-address 192.168.40.1

set network virtual-router RouterAlto routing-table ip static-route RouteAlto path-monitor enable no

set network virtual-router RouterAlto routing-table ip static-route RouteAlto path-monitor failure-condition any

set network virtual-router RouterAlto routing-table ip static-route RouteAlto path-monitor hold-time 2

set network virtual-router RouterAlto routing-table ip static-route RouteAlto interface ethernet1/1

set network virtual-router RouterAlto routing-table ip static-route RouteAlto metric 10

set network virtual-router RouterAlto routing-table ip static-route RouteAlto destination 0.0.0.0/0

set network virtual-router RouterAlto routing-table ip static-route RouteAlto route-table unicast

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" path-monitor enable no

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" path-monitor failure-condition any

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" path-monitor hold-time 2

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" nexthop ip-address 192.168.254.254

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" interface tunnel.666

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" metric 10

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" destination 192.168.20.0/24

set network virtual-router RouterAlto routing-table ip static-route "Tunnel Route" route-table unicast

.666 vlan.666 ]

set network dhcp interface vlan.666 server option dns primary inherited

set network dhcp interface vlan.666 server option dns secondary inherited

set network dhcp interface vlan.666 server option lease timeout 120

set network dhcp interface vlan.666 server option gateway 192.168.10.1

set network dhcp interface vlan.666 server option subnet-mask 255.255.255.0

set network dhcp interface vlan.666 server option inheritance source ethernet1/1

set network dhcp interface vlan.666 server option wins primary inherited

set network dhcp interface vlan.666 server option wins secondary inherited

set network dhcp interface vlan.666 server option nis primary inherited

set network dhcp interface vlan.666 server option nis secondary inherited

set network dhcp interface vlan.666 server option ntp primary inherited

set network dhcp interface vlan.666 server option ntp secondary inherited

set network dhcp interface vlan.666 server option dns-suffix inherited

set network dhcp interface vlan.666 server option pop3-server inherited

set network dhcp interface vlan.666 server option smtp-server inherited

set network dhcp interface vlan.666 server ip-pool 192.168.10.2-192.168.10.254

set network dhcp interface vlan.666 server reserved 192.168.10.10

set network dhcp interface vlan.666 server mode auto

set network tunnel ipsec IPSec\_Tunnel auto-key ike-gateway Tunnel

set network tunnel ipsec IPSec\_Tunnel auto-key ipsec-crypto-profile IPSEC\_Profile

set network tunnel ipsec IPSec\_Tunnel tunnel-monitor enable yes

set network tunnel ipsec IPSec\_Tunnel tunnel-monitor destination-ip 192.168.254.1

set network tunnel ipsec IPSec\_Tunnel tunnel-monitor tunnel-monitor-profile "Tunnel Monitoring"

set network tunnel ipsec IPSec\_Tunnel tunnel-interface tunnel.666

set network tunnel ipsec IPSec\_Tunnel anti-replay yes

set shared application

set shared application-group

set shared service

set shared service-group

set shared botnet configuration http dynamic-dns enabled yes

set shared botnet configuration http dynamic-dns threshold 5

set shared botnet configuration http malware-sites enabled yes

set shared botnet configuration http malware-sites threshold 5

set shared botnet configuration http recent-domains enabled yes

set shared botnet configuration http recent-domains threshold 5

set shared botnet configuration http ip-domains enabled yes

set shared botnet configuration http ip-domains threshold 10

set shared botnet configuration http executables-from-unknown-sites enabled yes

set shared botnet configuration http executables-from-unknown-sites threshold 5

set shared botnet configuration other-applications irc yes

set shared botnet configuration unknown-applications unknown-tcp destinations-per-hour 10

set shared botnet configuration unknown-applications unknown-tcp sessions-per-hour 10

set shared botnet configuration unknown-applications unknown-tcp session-length maximum-bytes 100

set shared botnet configuration unknown-applications unknown-tcp session-length minimum-bytes 50

set shared botnet configuration unknown-applications unknown-udp destinations-per-hour 10

set shared botnet configuration unknown-applications unknown-udp sessions-per-hour 10

set shared botnet configuration unknown-applications unknown-udp session-length maximum-bytes 100

set shared botnet configuration unknown-applications unknown-udp session-length minimum-bytes 50

set shared botnet report topn 100

set shared botnet report scheduled yes

set shared certificate URL-Override-CA subject-hash 00cb6d99

set shared certificate URL-Override-CA issuer-hash 00cb6d99

set shared certificate URL-Override-CA not-valid-before "Oct 18 07:06:51 2022 GMT"

set shared certificate URL-Override-CA issuer "issuer=C = US, ST = WA, CN = 192.168.10.10"

"

set shared certificate URL-Override-CA common-name 192.168.10.10

set shared certificate URL-Override-CA expiry-epoch 1697612811

set shared certificate URL-Override-CA ca yes

set shared certificate URL-Override-CA subject "subject=C = US, ST = WA, CN = 192.168.10.10"

set shared certificate URL-Override-CA public-key "-----BEGIN CERTIFICATE-----

MIIDDzCCAfegAwIBAgIUYNWk2YuVuOELX1xtxfaGsycrmfswDQYJKoZIhvcNAQEL

BQAwMjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAldBMRYwFAYDVQQDDA0xOTIuMTY4

LjEwLjEwMB4XDTIyMTAxODA3MDY1MVoXDTIzMTAxODA3MDY1MVowMjELMAkGA1UE

BhMCVVMxCzAJBgNVBAgMAldBMRYwFAYDVQQDDA0xOTIuMTY4LjEwLjEwMIIBIjAN

BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuBbDYJLISdhM0hguQwDSWFDW2oCK

4jTdsHB2mlwMZTUZZIjXVmCAmkz619JWxpv1S5pm/s4ENirHEZIU+jradp9Rkkma

uQCrtFd60PngcA3OZdP/7I0g5gqoBj8wruesNlaNpc+L8KCT5cZ4qI/e/G5zBIpi

yhWQ5cF3MR+4J4O3luQTitS54osUGvt8jlWSrsPUDz25vjvt77yeag3ZJwWsKc09

HARyvluIP/5Sd8dNFmgdMo49HEAQDMl9TRIbtcDjIPuDSPo8yKVmobI/QpSvz+l9

/3UfdRSPQYG21xsYFzp9tAcuk7FlQ5fHpTN0rjWJfOhcGS2WxaeQzOrsEQIDAQAB

ox0wGzAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwICBDANBgkqhkiG9w0BAQsFAAOC

AQEAYMcy0fNlW2ueyB/ov1CHC7ptGD5tZGmb/Ej9xlu2lNWeBhJlDNQAeTyLn5Pe

1RtlqoxwckP0XE97I8yNSjXURtfYpHvRLlizpytSE5dIjC1q6TCtnFWGJw5sM0E6

YRWTQMkDjRvAwXUXu7IIT+1tMECzX2waKzBBK1jthZIa8jPHJNR21un8AGOmOs33

DMO/9sbM79dP/nu6T0ZbP5ZJnAqnaBnY0qZd/GxoWY7ivcLgAyuX9IQXg1F1bcou

dldJYJbPooZqgjSYU3Hf6M/vN3QMS4pJgoso8usNwMnWWiy6jHbKW/hiVVIwxuDd

a0JrFFWk7WLBMzLMGLslB7FDaQ==

-----END CERTIFICATE-----

"

set shared certificate URL-Override-CA algorithm RSA

set shared certificate URL-Override-CA private-key -AQ==K0QbtGIlanYstwRYI+rkVqtzXZg=



set shared certificate URL-Override-SSL subject-hash 05d32c51

set shared certificate URL-Override-SSL issuer-hash 00cb6d99

set shared certificate URL-Override-SSL not-valid-before "Oct 18 07:07:41 2022 GMT"

set shared certificate URL-Override-SSL issuer "issuer=C = US, ST = WA, CN = 192.168.10.10"

set shared certificate URL-Override-SSL not-valid-after "Oct 18 07:07:41 2023 GMT"

set shared certificate URL-Override-SSL common-name 192.168.10.1

set shared certificate URL-Override-SSL expiry-epoch 1697612861

set shared certificate URL-Override-SSL ca no

92.168.10.1"

set shared certificate URL-Override-SSL public-key "-----BEGIN CERTIFICATE-----

MIIDTzCCAjegAwIBAgIFAOq4Ui0wDQYJKoZIhvcNAQELBQAwMjELMAkGA1UEBhMC

VVMxCzAJBgNVBAgMAldBMRYwFAYDVQQDDA0xOTIuMTY4LjEwLjEwMB4XDTIyMTAx

ODA3MDc0MVoXDTIzMTAxODA3MDc0MVowMTELMAkGA1UEBhMCVVMxCzAJBgNVBAgM

AldBMRUwEwYDVQQDDAwxOTIuMTY4LjEwLjEwggEiMA0GCSqGSIb3DQEBAQUAA4IB

DwAwggEKAoIBAQDNkextLS8N0me0+08mVxP+LCLbMAUIGWOHvhVrQylgjSNb8Qye

XE2AKwVZ7O2X1AsnHyHbMHa/V38YuD17hMk44+aDQcI6cVLVTppHDH+CLmikAcn6

ZBJSWfqd9v4zFQ2F2ieowArpalYOhZ8Xbs+ciiBkkztg7C4jHONv+8R3ONN31fpR

9j4q+o7Pf7XCRaI3ElbYpLq6qgajrffC2ZWbLIDTNGWzauvpDdc1x81JigNgkpeq

PH5yIgV6KBbQd5JqSaQrueP6kXti8JpQq3Z460drYYol6xp3koI6HLDdw9qiZK1V

WE7xpx7OV7UI5J3b13Lz+cbiMIR2pg9MLa6VAgMBAAGjbTBrMAkGA1UdEwQCMAAw

CwYDVR0PBAQDAgO4MCcGA1UdJQQgMB4GCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYB

BQUHAwUwCQYDVR0jBAIwADAdBgNVHQ4EFgQUwcd/tuRC/zYW/6iYOahyCdEXZwow

DQYJKoZIhvcNAQELBQADggEBAIk330HfNOzYWWA1vnpqXbfu2l0jCzAlcb5XDTQ7

JEIeGrqKfzFgwrX1mKmlKaCx+pxxU8fp30oZQFCsp8RPD1Q8V7vdrHa+1e8pGeO6

5jX5kONg+d3CCdiqDDh75hSIo4rToz4BCXPzLiYGYfHwlNqRrMdv8r4Px+2Lw1GP

VHZkg8WKE7ZqPgmVg0217xdrDfwUq50kdiFZ48nzRpHAXZGctL7FSVlbs6bDcxSP

kUD3B4wSN3cZo5fFTBYSAQVYPdiOzxVzq0rQ7/UzKLxHCdqHKRCy9Uku+5paldpK

I6/dB6W+/vMjBdpZofrmIqmgBMsipwh7HrnSWldxieCXFhM=

-----END CERTIFICATE-----

"

set shared certificate URL-Override-SSL algorithm RSA

set shared certificate URL-Override-SSL private-key -AQ==U08Pq7RzH2XlTNowh5JItu+L6UI=

set shared certificate Tunnel-CA subject-hash be30ce7e

set shared certificate Tunnel-CA issuer-hash be30ce7e

set shared certificate Tunnel-CA not-valid-before "Mar 13 19:11:24 2023 GMT"

set shared certificate Tunnel-CA issuer "issuer=C = US, ST = Washington, CN = SSL\_Tunnel"

set shared certificate Tunnel-CA not-valid-after "Mar 12 19:11:24 2024 GMT"

set shared certificate Tunnel-CA common-name SSL\_Tunnel

set shared certificate Tunnel-CA expiry-epoch 1710270684

set shared certificate Tunnel-CA ca yes

set shared certificate Tunnel-CA subject "subject=C = US, ST = Washington, CN = SSL\_Tunnel"

set shared certificate Tunnel-CA public-key "-----BEGIN CERTIFICATE-----

MIIFGTCCAwGgAwIBAgIUTDKsE31mZkfXMZgmNMgB4KE4lgkwDQYJKoZIhvcNAQEN

BQAwNzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCldhc2hpbmd0b24xEzARBgNVBAMM

ClNTTF9UdW5uZWwwHhcNMjMwMzEzMTkxMTI0WhcNMjQwMzEyMTkxMTI0WjA3MQsw

CQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGluZ3RvbjETMBEGA1UEAwwKU1NMX1R1

bm5lbDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALRpfLnAbY4rR8Ha

zpaNerb3D98f68/6P8CJjQnTmgHAPWlWqmns4NL9ETbnsGTmQjh4lVPAK3a90JBx

3D3m/8VoH528Fyw8DT5Ndg+tSf3qVbRi5yS2prZ//ttjrwJ/jGi6JSGkUV5gALMI

XJx4VpxFE5m7v9Mjm+wMhTYLm1GVxgl+IoW4piBmnQr8zClFvhfw4ALmCi7C9UjC

t/RqVdCBKq9vTuThFBws9ZxfIPmE98dOSFwKrKk102L2Uwsezd+vwds6qPeQDV6O

XqhxtQeVtzUZowA+ch7L4UXbnak/62iBz72sLTNYp8/Kzl++FpT5Qrke2t4btoug

wEUJW7Iqti+AFm+//ShLnxbtWd9UFmq+gWY21WHu5ToZgEP6uM2iDuIf5feuJzMJ

v7JZGPPaIwKp1m7B+tywISRjGtGZ69o1PjIfDrXVgNNqgUfIaKmjCdyVjyxc1hFB

tIJCYU4Oy9RCVfgRl1wWybYYC1yWNz7NSeHEepJ0or13c/XMHjCA/ASAcRUR85Jh

ypvG3NplW4du1SJebDEGYz2ZTbnNWUnM62WHPGejY0H+RM/7wzYJv6XfFEZaQuV+

fC7bJ1FqXzGsjJO++0jKrPOoWQqUYc0B8U020oFEZB9jH6CxzZBg9T7JU7x6SRk6

0qXRYZkZvRSefS8Pjsxw758sTzYPAgMBAAGjHTAbMAwGA1UdEwQFMAMBAf8wCwYD

VR0PBAQDAgIEMA0GCSqGSIb3DQEBDQUAA4ICAQCtSjeT/aN1h8V5Afp+bYcDmlDt

DIsLNYQA3OOMu3Cnw+7XXVr/Mi7/JAwMW/bDOBq7s96s9c1YzcZWWcFny72s3CwF

6WNb7r60qBxuADU+ACa7661FOvHT6r4bXES06xwBKR6rxPS5zZ3jZWisJLU9jNtS

s/6BJsFUj7h8t/fJJNsO/y+UIsVgYH+YL0PkTg9Gc8dz55/In1vi/4QArhSV+b1d

ksMsOVSzeKFCHZAOaL0ynu/aJclW0ZK22zeXm94yYDEY+OtwYEapALRAg8Z/5TFB

41+hqXGCyLKcu1OMesdKpmLMuPy5YFvqyE7+pmOs/mG5GCUFiLmr61zhAhV0mts2

RaMlEgyL+BTnUcIV88/BgrMPN3jzDEnU4sk9n5bks3WklTcE7oSjnOfro92cKjPT

xWfNpG/nHw/mDW4YC0LTbhk+ILRBq6JnOI5mX8aq4bmZ8xVWdSzbZaNc09dHmvQf

5ax53FTNv700hPwbkPPOJ47vv2ij8ACrEfzQLaWETUl8IcI19Sry/TsvFQ+TOv7A

Lm7+J3TKzqTIxr335MDVmFadn4FxwEcPnEqOz3SbcLjnFLcPUVuXi/QioBluaAxn

tc35UUGFinMjZwmJp9LsoLn9JkVj60mM2k4n4qARS1CKOdHC5e1hjAd8qwslHGih

ePz4yW7g6elqUiinvA==

-----END CERTIFICATE-----

"

set shared certificate Tunnel-CA algorithm RSA

set shared certificate Tunnel-CA private-key -AQ==9lTjtP2r9URDkt9P/JZr1eScHrc=

9+9Mxi1Z3uBHS8Tj+QCBNN6oDXff77Zlp6rzQg0FFqNa0Umh92yA3bDyyxrQTEMots69amXTZOaqRXRDnkNZU1g+3CpX1lEXE8gP+EYXusejMY4sv/g4/QlYcQ6ehRZua8LAPjIZAU12+Rzx51xcfIRh0jHJdsadSNqgmFY8Qf7k0OfOdAjOJtUMNAWDWjzGczQQohfQjjzJn/Nwg4Ub76ENcreJbP8LNYZyRPMmUHZORdIc7TD5zC9zseVVD0U5GulQtDhYyQ8Vp020VUpJIK0M/OzzrN5KNJNbVU36rp5CJazFlUpVOdHFjiYeDUWyL68kNvkXc=

set shared certificate Tunnel-Peer-2 subject-hash b89f5401

set shared certificate Tunnel-Peer-2 issuer-hash be30ce7e

set shared certificate Tunnel-Peer-2 not-valid-before "Mar 15 02:43:19 2023 GMT"

set shared certificate Tunnel-Peer-2 issuer "issuer=C = US, ST = Washington, CN = SSL\_Tunnel"

set shared certificate Tunnel-Peer-2 not-valid-after "Mar 14 02:43:19 2024 GMT"

set shared certificate Tunnel-Peer-2 common-name Tunnel\_P2

set shared certificate Tunnel-Peer-2 expiry-epoch 1710384199

set shared certificate Tunnel-Peer-2 ca no

set shared certificate Tunnel-Peer-2 subject "subject=C = US, ST = Washington, CN = Tunnel\_P2"

set shared certificate Tunnel-Peer-2 public-key "-----BEGIN CERTIFICATE-----

MIIFWTCCA0GgAwIBAgIFAOq4UjIwDQYJKoZIhvcNAQENBQAwNzELMAkGA1UEBhMC

VVMxEzARBgNVBAgMCldhc2hpbmd0b24xEzARBgNVBAMMClNTTF9UdW5uZWwwHhcN

MjMwMzE1MDI0MzE5WhcNMjQwMzE0MDI0MzE5WjA2MQswCQYDVQQGEwJVUzETMBEG

A1UECAwKV2FzaGluZ3RvbjESMBAGA1UEAwwJVHVubmVsX1AyMIICIjANBgkqhkiG

9w0BAQEFAAOCAg8AMIICCgKCAgEAp/PG3bMHVR0Elqf6lMh6XQjz1s8yW91UJAWM

2LM9S6KXoQJMFFWDtpJgSNUSm1dCMNg7ibCSGgeOhtQSdhRxWEhGyxO2wV+sBUz+

yk7A40aCnAxcEKk9H1YHglRFF5NGR8EAuQ+EhZ0Dm163S4kY6u0IazDNEXvfq7iJ

H0GX3OAPOi0shVqyGaiN2MWvrIlonBHv5/aqx3Z8NwvLwYL6ovP84DN1H5n1aCl1

CoqpQYutjIG9WQ9yRo88W5uSgSx3sQmKNqlVR4/p5K9fqDqWZVIAEabRUTeW4mRQ

13NV/ufyiAcJ34RqsRbo5o6Hq+s+ZS12VQltaTyLCeYp6shwqWX5IdNpxYSSMVsz

ytwdIGOf9G1Z1d9H67Ndbrs+BtSJqxkWa/nD0V4A2p43tislt45zDyOra3Gslqe+

nkxc4cGqAoN+GhBplcK4nk9bzZiaqz/gh2UcrpjeyJ6T0DCGI1k7Gsx2LjxMWWjS

0Rfk4EFVwemiQja9Q0Ur7JVqQMOoIj7dih4EuKeOGzB6pZ787ZG6xosihxxbNhs7

rfCaXtYXTWnnjgmrZnoYv0MHUVM2JCSC6CyPM0Xb/Cjx7v6u6gWmkVJ8J/fczuyU

p5PqdcB9Ru+A48K0yJCxccqb36198gdsVfQZIgagMUwbxFBtAzh1WByhnyfprTi6

demOrw8CAwEAAaNtMGswCQYDVR0TBAIwADALBgNVHQ8EBAMCA7gwJwYDVR0lBCAw

HgYIKwYBBQUHAwEGCCsGAQUFBwMCBggrBgEFBQcDBTAJBgNVHSMEAjAAMB0GA1Ud

DgQWBBQL+Bt6Gfh1fOXc/4lCzE7c/Ci2nDANBgkqhkiG9w0BAQ0FAAOCAgEAALM7

v9oVVn7QThqlezkUq/rW4itXgipDDcL+LmS28ihZKO56GpNDACXNxtYpxgyVJX7l

fL5cG7pxUDvZ2kGH4l2Zt2Hzj2jLazAo7cIYWBezruyUVG3X/Kt4aRWaV1UyrG1/

wg+HiBL2WX3aGBdAw0M7PVNhfMTB+IlixZ3gxu8Q6iqFoIgZ7pcQndYcW1yHzehC

rMB/4bGH9n9db8WG5xtT21rEWeRwoM5ewyABMq6cphk5PL315Wudg2jb6sqFqmaB

dXYXGz7mvqbz2UziDZuCMl7eu0TwvjSeYdhUnOtV/zQUitAYiWfsLtGnCFzClmv1

owt8BnMB66922sGxzIcd02r5UHjfjHK6nObU0FCQlF9wvTVt46aLDwU4kX+CsAV6

2gIRCGy5adeHmvgIRNlAXBh62cLw9j2LmerZyN1MSaOah+7IiNckPwT8PeTq64Dz

FTmqEwHXgIjWPIFHDN6M7kafL33E5PsqMJN8uEDdxXz4SECJPlWaox5gCWxkefZY

/YWIAoNWB/6bq91SqQvKmeo+l+mfwTKG2nYmkNgrMzmqU0eMYX76D/8xLv6fjgB8

uQICPxyLT0g0lQVJtwQ5uqH+CvKNp4NKjUwTHLM1vI+fcKRuBXOHUAXjftLNoj/l

MOXuz0jyyw+8ZYZOuIIXdv8S95yWS1wj+Z2ao9c=

-----END CERTIFICATE-----

"

set shared certificate Tunnel-Peer-2 algorithm RSA

set shared certificate Tunnel-Peer-2 private-key -AQ==7KeU8b9xoA9OQ9irbwwOzIyh/bY=





+fPADHmAij7rWSag6aVLNOgThVOVyyCPyGpuq/ThR0jGGF6FEOPnGYa4tGRGKrY4UbdvyyguLlsyF3CQ+zrnTlydDZzTq5aQiHrlm2VNLEQ32kkxIWq8Meuzj578ukg63TKSRzeRA73YSnSza/JyZWHcYFcvuQpjCyS75Yr7EWqWgOGFr89FfZ8MHWF7qDo0DOlDZaSODVMyBo0L2Gb1peyTH7L31n6YgVsBoqx/O+MCtIKQ

CkT4SZyMeexknjAg5ttt/SZF5TZTtdQNLhCiLEO0bixlTonNRZFXZ1lzyfq7Uhiu5H0RNvzZIJMJ+QQe9EXdwZOXE0y3smw5q+7qJQxVyyTHneu2yaFqkZfs2H97B9L2qNfy2KmGi+OKSPzSpivedYvZXfKCCZTKMPLAQ07DKeIIfECPaiH4mMJY2rSj9yjWaTIzHW7jvLPrnC7SfONvCc3SvsRw5pUMWvM9hKD+bHoikaCMTUiUbfXk3P/kbKK4OY+4zQ1BoAtkApuYNoZO3VOQSs7Nd2ZF3leh04TBxwqnjbDZDd6cY+56ImRkQLcxJejkeCzBySP8hOrcZr4CARTs0yjrjRtGBPmAp6Tr85zCwYIVY/B4FvPT8ObPzaKvklt98HD0J42fRFzNm8yPqkOWIX1mmrjD9yFw8O1maUhm/YuEh/1T3eAaT11iGWgvO/723e2HjWMhXT4+xg3hSPMgzDuLDgUc

fxlRpMPIRRJeFsZQArdowKcThxJcqWZBgcH0pEgZX3JKGQGzYFQi2TtA4eTcJCqlJ44V0Khfx8rxUv/kjcOad4jeLkUZi4thPXNTREU5dXX0HcW/r43YIpVsjctYK82C1c2zV5TjD4WRkWoUM6Xvgv5BOVy8F5ndEH9dGihszWImSk50+FdSJ6N/nNZXdNu5FsQeHdfv8XxZGy/hD9blrUSYyKyzEvWHOwg/3im/T7eD/u7TH+1UQTK/ss8fs=

s1-2

set shared ssl-tls-service-profile Override-SSL protocol-settings max-version max

set shared ssl-tls-service-profile Override-SSL certificate URL-Override-SSL

set shared ssl-decrypt forward-trust-certificate

set shared certificate-profile STS-Profile CA Tunnel-CA

set zone trust network virtual-wire

set zone untrust network virtual-wire

set zone Untrust-L3 network layer3 ethernet1/1

set zone Trust-L3 network layer3 [ vlan.666 ethernet1/8 ]

set zone Trust-L2 network layer2 [ ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5 ethernet1/6 ethernet1/7 ]

set zone VPN\_Tunnel network layer3 tunnel.666

set url-admin-override password -AQ==nnyXgBy0zOh7bAL5gpGmQg5kAK0=jTL19hVHwgXqztQi4TdDIA==

set url-admin-override mode transparent

set url-admin-override ssl-tls-service-profile Override-SSL

set service-group

set service

set schedule

set rulebase security rules rule1 from trust

set rulebase security rules rule1 to untrust

set rulebase security rules rule1 source any

set rulebase security rules rule1 destination any

set rulebase security rules rule1 service any

set rulebase security rules rule1 application any

set rulebase security rules rule1 action allow

set rulebase security rules rule1 log-end yes

set rulebase security rules "Internet Outgoing" profile-setting group Internet

set rulebase security rules "Internet Outgoing" to Untrust-L3

set rulebase security rules "Internet Outgoing" from Trust-L3

set rulebase security rules "Internet Outgoing" source any

set rulebase security rules "Internet Outgoing" destination any

set rulebase security rules "Internet Outgoing" source-user any

set rulebase security rules "Internet Outgoing" category any

set rulebase security rules "Internet Outgoing" application any

set rulebase security rules "Internet Outgoing" service application-default

set rulebase security rules "Internet Outgoing" source-hip any

set rulebase security rules "Internet Outgoing" destination-hip any

set rulebase security rules "Internet Outgoing" action allow

set rulebase security rules "Internet Outgoing" description "Traffic going to the interntet"

set rulebase security rules "VPN Tunnel" to [ Trust-L3 Untrust-L3 VPN\_Tunnel ]

set rulebase security rules "VPN Tunnel" from [ Trust-L3 Untrust-L3 VPN\_Tunnel ]

set rulebase security rules "VPN Tunnel" source any

set rulebase security rules "VPN Tunnel" destination any

set rulebase security rules "VPN Tunnel" source-user any

set rulebase security rules "VPN Tunnel" category any

set rulebase security rules "VPN Tunnel" application any

set rulebase security rules "VPN Tunnel" service application-default

set rulebase security rules "VPN Tunnel" source-hip any

set rulebase security rules "VPN Tunnel" destination-hip any

set rulebase security rules "VPN Tunnel" action allow

set rulebase security rules "VPN Tunnel" description "Allows VPN Tunnel traffic"

set rulebase nat rules "Internet Outgoing" source-translation dynamic-ip-and-port interface-address interface ethernet1/1

set rulebase nat rules "Internet Outgoing" to Untrust-L3

set rulebase nat rules "Internet Outgoing" from Trust-L3

set rulebase nat rules "Internet Outgoing" source any

set rulebase nat rules "Internet Outgoing" destination any

set rulebase nat rules "Internet Outgoing" service any

set rulebase nat rules "Internet Outgoing" description "Traffic going to the internet"

set rulebase nat rules "Internet Outgoing" to-interface ethernet1/1

set profiles url-filtering "Internet Filtering" credential-enforcement mode disabled

set profiles url-filtering "Internet Filtering" credential-enforcement log-severity medium

bortion abused-drugs adult alcohol-and-tobacco auctions gambling grayware malware nudity phishing ransomware ]

set profiles url-filtering "Internet Filtering" credential-enforcement continue [ business-and-economy cryptocurrency dating extremism financial-services hacking high-risk home-and-garden job-search legal military motor-vehicles newly-registered-domain news real-estate religion sex-education social-networking stock-advice-and-tools swimsuits-and-intimate-apparel translation travel weapons ]

set profiles url-filtering "Internet Filtering" description "URL Filtering in Palo Alto"

set profiles url-filtering "Internet Filtering" log-http-hdr-user-agent no

set profiles url-filtering "Internet Filtering" alert not-resolved

set profiles url-filtering "Internet Filtering" block [ abortion abused-drugs adult alcohol-and-tobacco auctions gambling grayware malware nudity phishing ransomware ]

set profiles url-filtering "Internet Filtering" continue high-risk

set profiles url-filtering "Internet Filtering" override [ business-and-economy cryptocurrency dating extremism financial-services hacking job-search legal military motor-vehicles newly-registered-domain news real-estate religion sex-education social-networking stock-advice-and-tools swimsuits-and-intimate-apparel translation travel weapons ]

set profile-group Internet virus default

set profile-group Internet spyware strict

set profile-group Internet vulnerability strict

set profile-group Internet url-filtering "Internet Filtering"

set import network interface [ ethernet1/1 vlan.666 ethernet1/2 ethernet1/3 ethernet1/4 ethernet1/5 ethernet1/6 ethernet1/7 ethernet1/8 tunnel.666 tunnel ]

set application-group

set application

set mgt-config users admin phash $5$xxhcudql$vUshiLFpLwtEkiIFxc7dLI.hwFjf62EBAPYJ6QgdSH8

set mgt-config users admin permissions role-based superuser yes

set mgt-config password-complexity enabled yes

set mgt-config password-complexity minimum-length 8

Screenshots/Steps

Configuring Layer 3 interface for VPN Connections (Peer 1):

**Graphical user interface, text, application, email

Description automatically generated**

Configuring Layer 3 interface for VPN Connections (Peer 2):

Graphical user interface, text, application, email

Description automatically generated

Configuring Tunnel Interface for VPN Tunnel Connections (Peer 1):

Graphical user interface, text, application, email

Description automatically generated

Configuring Tunnel Interface for VPN Tunnel Connections (Peer 2):

Graphical user interface, text, application, email

Description automatically generated

Configuring Security zone for the VPN Tunnel (Peer 1 and 2):

Graphical user interface, text, application, email

Description automatically generated

Configuring Security Policy rule for the Layer 3 security zones (Peer 1 and 2):

Graphical user interface, text, application, email

Description automatically generated

Configuring a static route to redirect traffic to the peer’s subnet (Peer 1):

Graphical user interface, text, application

Description automatically generated

Configuring a static route to redirect traffic to the peer’s subnet (Peer 2):

Graphical user interface, text, application, email

Description automatically generated

Configuring IPSec Crypto profile (Peer 1 and 2):

Graphical user interface, text, application, email

Description automatically generated

Configuring IKE Crypto Profile (Peer 1 and 2):

Graphical user interface, text, application, email

Description automatically generated

Configuring IKE Gateway (Peer 1):

Graphical user interface, text, application

Description automatically generated

Configuring IKE Gateway (Peer 2):

Graphical user interface, text, application

Description automatically generated

Configuring IPSec Tunnel (Peer 1):

Graphical user interface, text, application, email

Description automatically generated

Configuring IPSec Tunnel (Peer 2):

Graphical user interface, text, application, email

Description automatically generated

Problems

We did not encounter any major problems while configuring the lab. But we did encounter some small mistakes that stopped our progress. First, we found that there was an issue with the VPN peers not being able to reach each other. This was fixed through looking at the static IP addresses on a separate Layer 3 interface, configuring security profiles, the destination subnets in the static routes, and then setting the same pre-shared keys again on both peer 1 and peer 2. After the configuring the peers were able to reach and ping to each other. A Second issue we encountered when trying to setup the VPN is that once both peers show that it failed to negotiate a new key, when the tunnels stop working and when looking in the log when logging into the web console. This issue was fixed by adding more encryption algorithms, entering the pre-shared keys again and changing the IP authentication to the correct IP addresses. With that fix both peers were able to negotiate a new key and the site-to-site VPN was able to work again.

Conclusion

The objective of the lab was to be able to set up or create a We were able to set up a site-to-site VPN on two different Palo Alto fire walls. During this prosses of configuring the site-to-site VPN allowed us to practice and allowed us to familiarize ourselves with Palo Alto Firewall management console and configuring VPN. During the lab we encountered some small troubles that we learned from, but we were finally able to create a Palo Alto Site to Site VPN with Shared Secret keys that can ping the remote devices on another subnet.